Advances in Science, Technology and Engineering Systems Journal Vol. 5, No. 3, 361-370 (2020)

www.astesj.com

ASTESJ

ISSN: 2415-6698

A Survey on Image Forgery Detection Using Different Forensic Approaches

Akram Hatem Saber[1,*], Mohd Ayyub Khan[1], Basim Galeb Mejbel[2]

[1]Department of Electronics Engineering, Aligarh Muslim University, 202002, India

[2]Department of Computer Technician Engineering, AL-Esraa University, 10069, Iraq

ARTICLE INFO

Article history:
Received: 18 February, 2020
Accepted: 13 May, 2020
Online: 11 June, 2020

Keywords:
Forgery Detection
Active Forensic Approaches
Passive Forensic Approaches
Tampering Identification
Copy-Move
Digital Watermarking
Digital Signature
Image Cloning
Image Splicing

ABSTRACT

Recently, digital image forgery detection is an emergent and important area of image processing. Digital image plays a vital role in providing evidence for any unusual incident. However, the image forgery my hide evidence and prevents the detection of such criminal cases due to advancement in image processing and availability of sophisticated software tamper of an image can be easily performed. In this paper, we provide a comprehensive review of the work done on various image forgeries and forensic technology. Many techniques have been proposed to detect image forgery in the literature such as digital watermarking, digital signature, copy-move, image retouching, and splicing. The investigation done in this paper may help the researcher to understand the advantage and handles of the available image forensic technology to develop more efficient algorithms of image forgery detection. Moreover, the comparative study surveys the existing forgery detection mechanisms include deep learning and convolution neural networks concerning it is on benefits and demerits.

1. Introduction

Digital images are the major information source in recent days, due to its availability and sophistication [1]. Also, it is widely used in different fields, detection of digital image forgery is utilized in numerous applications that are linked to media, publication, law, military, medical image science applications, satellite image, and world wide web publications. Because it is very easy to manipulate and edit [2]. For this reason, different types of cameras and the user-friendly software are used to create and edit the digital images [3]. Digital images are frequently used to support the important decision for many situations. Moreover, the digital images are a popular source of information and the reliability of digital image and it becomes an important issue.

For image forensics, the techniques are classified into two, such as the active approach and passive approach. In the case of active approach: in this method, the digital image entails the various types of preprocessing like watermark embedded or signature are added in the original image. Digital watermarking and signature are two different active protection techniques. If the image has tampered, special information is not extracted from the obtained image. Watermarking is one of the methods of active tampering detection and security structure is embedded into the image but most of the image processing tools are not contained any watermarking or signature module[4].

In recent days different methods are developed for made image reliable and secure that is analogous to watermarking like message authentication code, image checksum, image hash, and image shielding. Passive image forensics is a challenging task in image processing techniques[5]. It is not a particular method for all cases but different methods each can detect the special forgery. The stream of passive tempering detection is to deal with analyzing raw image based on different statistics and semantics of an image content to localize tampering of image[6].

There are several types of image forgery that include image retouching, image splicing, copy and move attack. Image retouching is considered a minimum harmful type of digital image forgery. An original image does not significantly change, but they reduced some features of the original image. This technique is used to edit the image for a popular magazine. This type of image forgery is located in all magazine covers and also it used to improve the specific features of an image[7]. On the other hand, Image splicing or photo montage refers to make a forgery image and it is more aggressive than image

[*] Akram Hatem Saber, Aligarh, +919515584268, alasmr.2a@gmail.com

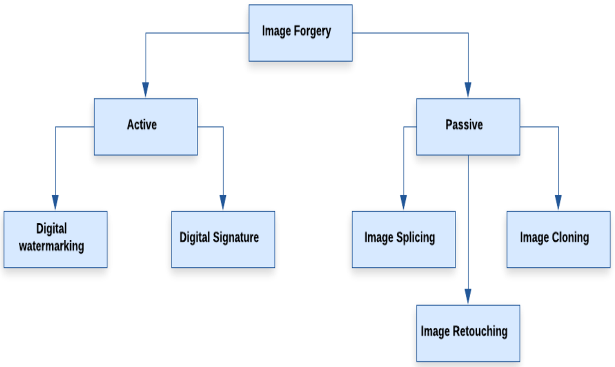
https://dx.doi.org/10.25046/aj050347

retouching. Image splicing is an easy process and it pastes the regions from isolated sources. This method is referred to as paste-up formed by sticking together the image by using digital tools like photoshop. This technique is a group of two or more images that are combined to generate fake images[8]. However, copy and move attack is also one of the popular and difficult images tampering technique. It required the cover part of a similar image to add or remove the information. Copy and move attack, the aim is to hide some information in the original image. The detection of the forged image from the original one is very hard. The naked eye is not able to identify the tampered region from a forged image. The image tampering is a general manipulation of digital images. Traditional block-based forgery detection methodologies are categorized as the input images into overlapping and regular image blocks and also tampered regions are identified by matching blocks of pixel or transform coefficient[9].

Normally, the image forgery detection is performed by using the following techniques: JPEG quantization tables, Chromatic Aberration, Lighting, Camera Response Function (CRF), Bi-coherence and higher-order statistics, and Robust matching. The digital cameras encode the images based on JPEG compression [10], which configures the devices at various compression level. Then, the sign of image tampering is evaluated by analyzing the inconsistency of lateral chromatic aberration [11]. In which, the average angular between the local and global parameters is computed for every pixel in the image. If the average value exceeds the threshold, it is stated that the deviation is unpredictable in the image due to the forgery of the image. Then, for each object in the image, the inconsistencies and the illuminating light source is detected to identify the forgery [12]. Typically, different measurements such as infinite, local and multiple are considered for determining the error rate. Then, the CRF is mainly used to expose the image splicing instituted on the geometry invariant of the image. In which, the suspected boundary is identified within each region of the image, and it is validated for identifying the inconsistencies [13]. The bi-coherence features [14] are widely used for detecting the splicing on images that estimate the mean of magnitude and phase entropy for augmenting the images. Moreover, it extracts the features for the authentic counterpart and incorporates it to capture the characteristics of various object interfaces. Finally, the exact replicas are identified by matching the features concerning the block size, which is done by the use of robust matching [15]. But, it requires the human intervention for interpreting the output of replicas detection [16]. Generally, the region duplication is performed on the image based on the geometrical and illumination adjustments. It is a very simple operation in which a continuous portion of pixels is copied and pasted on some other location in the image. This paper is fully focused on the detailed investigation of the image forgery detection mechanisms. The remaining sectors present in the study are arranged as follows: Section II investigates some of the image forgery detection mechanisms used in digital image processing. Section III surveys the forensic approaches and its working procedure for image forgery detection. Section IV presents a detailed investigation of the existing methodologies used for image forgery detection with its advantages and disadvantages. The overall conclusion of the paper is presented in Section V.

2. Digital Image Forgery Detection Methods

Typically, the methodologies used for forgery detection are classified into two types such as active forensics and passive forensics, in which digital watermarking and digital signature are the types of active techniques. Then, the splicing, image retouching, image cloning, and copy-move techniques are the categories of the passive technique [17]. The description of these techniques are investigated in the following sub-sections.



2.1. Digital Watermarking

In this type of image forgery, a digital watermark is added on the photo, which is more or less visible. Then, the appended information is more or less transparent, so it is very difficult to notice the watermark. *Ferrara, et al.* [18] suggested a new forensic tool for analyzing the original image and forged regions based on the interpolation process. The image splicing can be detected by the use of the conditional Co-occurrence Probability Matrix (CCPM) [19], which uses the third-order statistical features during the forgery detection. Normally, the watermarking schemes are categorized as reversible and irreversible. In which, the image irreversible distortions are avoided based on the original features of the image by using the reversible watermarking techniques. The watermarking can be mainly used to indicate the source or authorized consumer of the image. It is a pattern of bits that is inserted into a digital media for identifying the creator [20]. The watermarking techniques are semi-fragile, fragile, and content based, which are mainly used for image authentication application.

Li, et al. [21] implemented a new method for detecting the copy move forgery, where the Local Binary Pattern (LBP) was utilized to extract the circular blocks. The stages involved in this system are preprocessing, feature extraction, feature matching, and post processing. Here, it is stated that when the region is rotated at different angles, it is highly difficult to detect the forgeries. *Hussain, et al.* [22] suggested a multi-resolution Weber Local Descriptors (WLD) for detecting the image forgeries based on the features obtained from the chrominance components. Here, the WLD histogram components are calculated and the Support Vector Machine (SVM) classifier is utilized to detect the forgery. In this paper, two different types of forgeries such as splice and copy-move are detected by using the multi-resolution WLD approach.

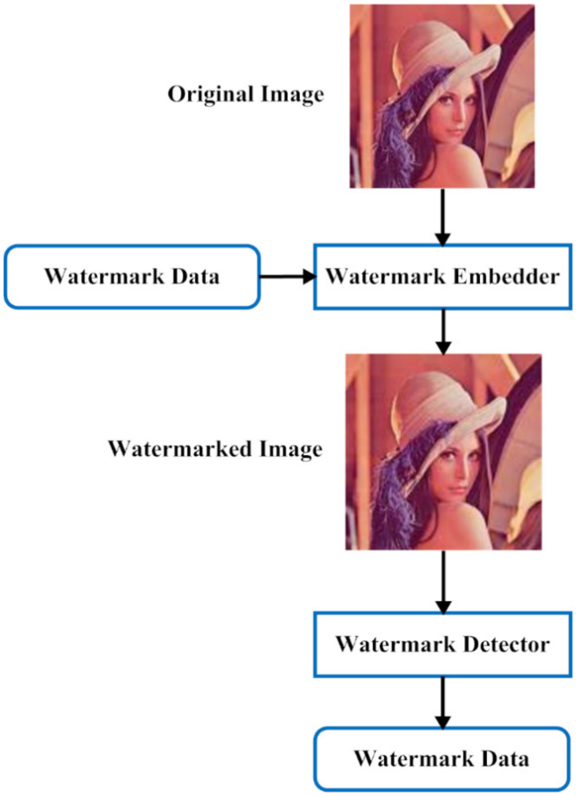


Figure 2. Digital watermarking [18]

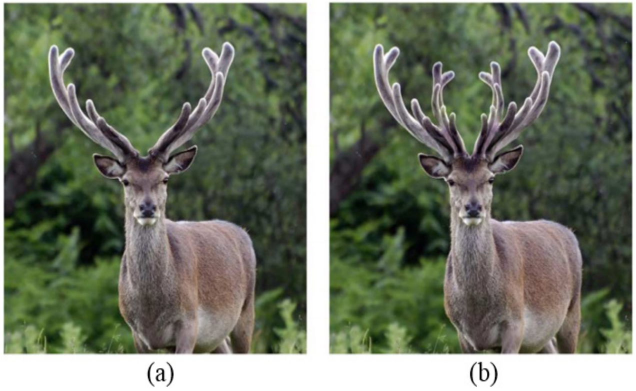
2.2. Digital Signature

Normally, the authenticity of the digital messages is validated based on the digital signature. Because, based on the valid signature, the recipient can believe that the message is formed by the recognized sender. Thus, the digital signature is widely used in the fields of financial transactions, contract management software, and software distribution [20]. Normally, the digital signature embeds some secondary information, which is obtained from the image. In this method [23], the distinct features are extracted from the image during the initial stage, based on these, the image authenticity is validated. Typically, the digital signature has the following properties:

- Only the sender can sign the image and the receiver can validate the signature
- Unauthenticated users cannot able to forge the signature
- It provides an integrity
- Also, it achieves non-reputation

2.3. Splicing Method

Image splicing is a kind of forgery detection method, in which a single image is created based on the combination of two or more images [24]. It is also termed as image composition, in which various image manipulation operations are performed. Typically, many inconsistencies may be created in the image features due to the splicing operation. In this technique, the composition between the two images is estimated and incorporated for creating a fake image. Based on the image block content, the difference between the illumination and reference illuminate color is estimated. In this digital image forgery, it is very difficult to extract the exact shape of the image. Typically, the image splicing method [25] is categorized into two types such as boundary-based and region-based. *Alahmadi, et al* [26] suggested a passive splicing forgery detection mechanism for verifying the authenticity of digital images. Here, the features are extracted from the chromatic channel for capturing the tampering artifacts. *Kakar, et al* [27] utilized a forgery detection approach for detecting the splicing in the digital images. Here, the small inconsistencies in the motion blur are detected by analyzing the special characteristics of image gradients [28]. The stages involved in this detection are image subdivision, motion blur estimation, smoothing, blur computation, interpolation and segmentation [29]. The authors of this paper [30] employed a machine learning algorithm for detecting the image splices. The illumination analysis is highly effective for the detection of image splicing [31]. To increase the effect of photorealism, an image splicing operation is performed with the operations of color and brightness adjustment. In this paper [32] the radial distortion from various portions of the image is estimated for the detection of image splicing.



2.4. Image Retouching

Among the other image forgeries, image retouching is considered as the less harmful forgery technique, in which some enhancement can be performed on the image. Also, it is popular in photo editing applications and magazines. *Muhammad, et al* [33] suggested an un-decimated dyadic wavelet transformation technique for detecting the copy-move forgery. Typically, more sophisticated tools are available for making this type of forgery by applying the soft touch on the edges. So, it is very difficult to differentiate the color and texture of the stimulated part with the unoriginal part. Moreover, it makes the forgery detection as highly complicated, because of two or more identical objects in the same image. So, the authors of this paper utilized similarity measurements for detecting this forgery, in which the noisy inconsistency is analyzed between the copied and moved parts. Here, it is stated that the transformation methods such as FMT, Scale Invariant Feature Transform (SIFT), and Discrete Wavelet Transform (DWT) can detect the forgery in a highly compressed image. *Ghorbani, et al* [34] recommended a Discrete Cosine Transform Quantization Coefficients Decomposition (DCT-QCD) for detecting the copy-move forgery. The integrity and authenticity verification of digital images is a very difficult process, specifically the images used for news items, medical records, and court law. Because the copy-move forgery may be created for those types of images.

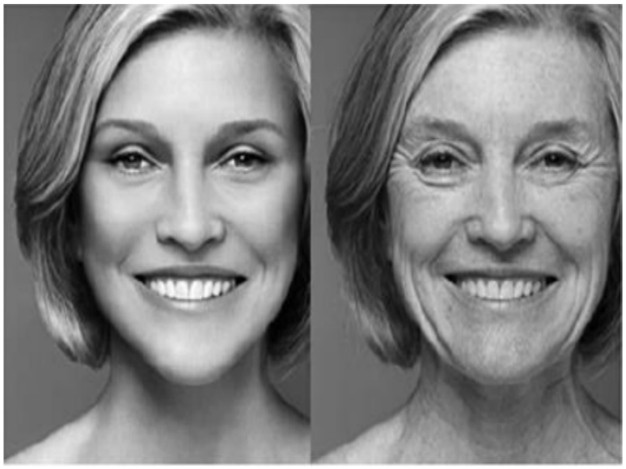

(a) (b)

Figure 4 (a). Forged image and (b). Real image [33]

2.5. Copy-Move Method

Among the other forgery methods, the copy-move method an extensively used type of image tampering, where the specific portion is copied and pasted on some other region [35]. The main motive of this method is to hide a significant element or highlight a precise object. *Bayram, et al* [36] implemented a proficient method for detecting the copy-move forgery. The authors stated that the block matching procedure is used to detect this type of forgery by separating the image into overlapping chunks. Also, it identifies the duplicated connected image blocks by finding the distance between the neighbor blocks [37]. For taking the forgery decision, only the duplicate blocks detection is not enough, because the natural images have many similar blocks [38]. Moreover, the Fourier Mellin Transform (FMT) is used to perform the operations like scaling, translation, and rotation for image forgery detection [39].

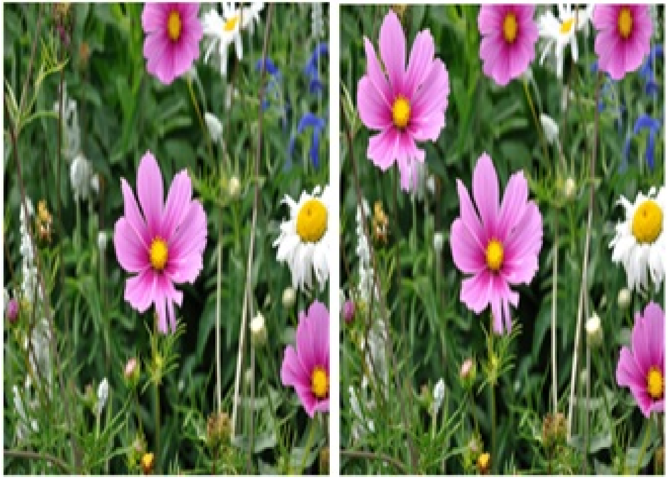

(a) (b)

Figure 5 (a). Original image and (b). Tampered image [36].

As shown in figure above copy move image forgery (a) original image and (b) is tampered image *Mahdian, et al* [40] utilized a detection method for identifying the copy-move forgery based on the blur moment invariants. This detection methodology can detect blur degradation, noise, and some other arbitrary changes in the duplicate image regions like noise addition and gamma correction gamma is a non-linear adjustment to individual pixel values. The steps involved in this method are image tiling with overlapping, representation blur moment invariants, transformation, similarity analysis, and map creation for duplication region detection. Moreover, the dimensionality of blocks was reduced by using the principle component transformation. *Muhammad, et al* [41] employed a Dyadic undecorated Wavelet Transformation (Dew) technique for detecting blind copy-move image forgery detection. This transformation technique aimed to extract the low frequency and high-frequency components by estimating the similarity between the blocks [42]. Moreover, the Euclidean distance is computed between every pair of blocks in the image. Then, the match is identified by computing the threshold value between the sorted lists [43]. In the wavelet transformation, the downsampling process is not involved, and the coefficients are not shrunk between the scales. *Lynch, et al* [44] aimed to detect the copy-move forgery by the use of expanding block algorithms. Also, it intended to identify the duplicated regions in the image by estimating the size and shape [45]. In this paper [46], it is stated that the copy-move forgery is performed for hiding the region of the image by wrapper it with a duplicate image. Still, recognizing the forged region is extremely intricate due to the precise copy of another region [47]. This detection mechanism contains the stages of feature extraction, comparison, and similarity estimation for taking copy decisions [48]. As shown in figure below the procedure of copy move technique first step the input image preprocessed, second step block division, third step feature extracted, last step the blocks which carry same feature triggered and mapped as a forgery.

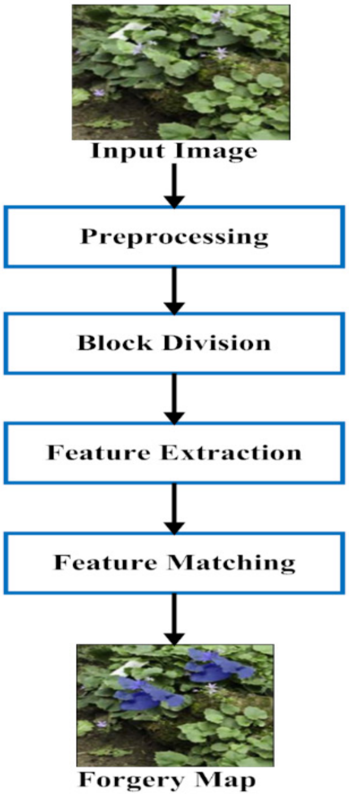


Figure 6. Procedure of Copy Move technique [48]

3. Forensic Approaches

In this section, some of the forensic approaches used for digital image forgery detection are surveyed with its working stages. *Omen, et al* [49] utilized a fractal dimension and Support Vector Decomposition (SVD) techniques to detect and isolate the duplicated regions in the image. In this scheme, the image is classified into various groups based on its fractal dimension, which is used to identify the variations. Then, the copied and pasted regions are identified by using an efficient texture-based classification technique. Here, it is stated that the SVD is one of the widely used robust and reliable matrix factorization methods, which offers algebraic and geometric invariant features for classification. Also, the SVD technique provides maximum energy packaging for exhibiting good stability from distortion. It helps to locate the duplicated regions by adding noise and avoiding the blurred edges. *Chierchia, et al* [50] implemented a Bayesian Markov Random Field (MRF) technique to identify the image forgeries based on the sensor pattern noise. Here, the observed statistics and prior knowledge were balanced by the use of a Bayesian approach. Also, the reliability of forgery detection is improved by using the global optimization algorithm. *Bianchi and Piva* [51] developed a new forensic algorithm for discriminating against the original and forged regions in the image. Here, the effects of cumulation between various DCT coefficients are extracted with the simplified map by using the unified statistical model. *Murali, et al* [52] investigated various image forgery detection mechanisms for identifying the forged regions in the forged image. In this paper, it is stated that the copy-move and copy create types are the two kinds of image forgeries, which are implemented at earlier stages. It is detected by using the JPEG compression analysis and filtering algorithms. Here, the algorithms are evaluated based on the factors of image formation, time complexity, multiple forgery detection, and image transformation. *Piva* [53] provided a comprehensive overview of image forensics for determining whether the image content is authenticated or not. The methods investigated in this paper were acquisition-based, coding-based methods, and editing based methods. *Pan, et al* [54] suggested a feature matching technique for identifying the duplicated regions in the digital image.

4. Comparative Study

This section surveys the existing forgery detection mechanisms with respect to its own benefits and demerits. This study is mainly focused on the detection of image forgery by using various forensic approaches. The methods that have been investigated in this analysis are digital signature verification, digital image watermarking, cosine transformation, authentication watermarking, SURF, wavelet transformation, binary pattern extraction, deep learning, block matching, and blind image forgery detection.

Table 1. Comparative analysis of various image forensic approaches

S.No	*Paper Title*	*Methods Used*	*Tampering Detection Type*	*Pros/Cons*	*Publication Year*
1.	Research issues and challenges for multiple digital signatures	Digital Signature Verification Schemes [55]	The validity of multiple digital signatures are verified.	Advantage: 1. It provides the clear overview of various signature verification schemes with its specific limitations. Disadvantage: 1. However, it failed to state an efficient and robust signature verification scheme	2005
2.	ROI based tamper detection and recovery for medical images using reversible watermarking technique	Digital image watermarking [56]	It is used to detect the locations of the tampered portion inside the Region of Interest (ROI).	Advantages: 1. Good performance in terms of hiding capacity and visual quality 2. High embedding capacity Disadvantages: 1. Lack of reversibility 2. Limited hiding capacity Induced distortions inside the regions	2010
3.	A comparison study on copy-cover image forgery detection.	Discrete Cosine Transformation (DCT and Principle Component Analysis [57]	It detected a copy-move image forgery.	Advantages: 1. Energy compaction property 2. Reduced time complexity 3. Increased accuracy Disadvantages: 1. It required to locate the possible inconsistency 2. Increased false positive rate	2010
4.	A chaotic system based fragile watermarking scheme for image tamper detection	Authentication watermarking scheme [58].	It locates the tampered regions for image authentication.	Advantages: 1. High security 2. Superior tamper detection and localization Disadvantages: 1. Increased computational complexity 2. Required to improve the performance	2011
5.	DWT-DCT (QCD) based copy-move image forgery detection	Discrete Wavelet Transformation (DWT) and Discrete	It detected a copy-move image forgery in an accurate manner.	Advantages: 1. Better accuracy 2. Reduced dimensionality of features Disadvantages:	2011

		Cosine Transformation (DCT) [34]		1. Heavy compression 2. It required to remove the position of pasted areas 3. Increased complexity	
6.	Detection of region duplication forgery in digital images using SURF	Speeded Up Robust Features (SURF) [59]	A copy move forgery is detected with better detection performance.	Advantages: 1. Better detection rate 2. It evaluated the image with different angles Disadvantages: 1. Required to reduce the false match rate 2. Also, it failed to identify the small copied regions.	2011
7.	Passive copy move image forgery detection using undecimated dyadic wavelet transform	Undecimated dyadic wavelet transformation [33]	A copy move image forgery is detected efficiently.	Advantages: 1. It estimated the methods based on three case studies 2. Better performance results Disadvantages: 1. Noise estimation is not robust 2. It is not translation invariant	2012
8.	A novel video inter-frame forgery model detection scheme based on optical flow consistency	Inter-frame forgery model detection mechanism [60]	It detected the frame insertion and deletion forgery.	Advantages: 1. It provides the good performance by efficiently identifying the frame insertion and deletion Disadvantages: 1. Reduced precision 2. Increased false detection rate	2013
9.	Digital image tamper detection techniques-a comprehensive study	Fragile watermark detection technique [61]	Authentication based tampering detection is performed.	Advantages: 1. Robust watermark 2. It accurately pinpoint the forgeries Disadvantages: 1. It required a digital signature on the images 2. Not highly efficient	2013
10.	Survey on blind image forgery detection	Blind image forgery detection [62]	It detects the copy-move, splicing, and retouching image forgeries.	Advantages: 1. It evaluated different number of matches for forgery identification 2. It efficiently identified the duplicated blocks Disadvantages: 1. It required to analyze the quality of image 2. Increased time consumption	2013
11.	Splicing image forgery detection based on DCT and Local Binary Pattern	Local Binary Pattern (LBP) and Discrete Cosine Transformation (DCT) [26]	Here, an image splicing forgery is detected accurately.	Advantages: 1. Better detection performance 2. Increased accuracy Disadvantages: 1. Increased complexity 2. Not highly efficient	2013
12.	A Forensic Method for Detecting Image Forgery Using Codebook	SIFT based feature extraction and codebook generation [63]	Dissimilar types of image tampering are concentrated in this paper that includes enhancing, composting and copy move.	Advantages: 1. Highly efficient 2. Better accuracy Disadvantages: 1. Requires more time for detection 2. It distorts the content 3. Inconclusive results	2013
13.	Region Duplication Forgery Detection using Hybrid Wavelet Transforms	Hybrid wavelet transformation technique [64]	It detected a copy move image forgery and region duplication forgery.	Advantages 1. Effective compression 2. It detected the duplicated regions with increased accuracy Disadvantages 1. It failed to detect the duplicated regions, when the copied region is rotated or scaled 2. Not highly efficient	2014
14.	Digital image forgeries and passive image authentication techniques: A survey	Passive image authentication techniques [20]	A copy move image forgery is detected in an efficient way.	Advantages: 1. Reduced computational complexity 2. Increased robustness Disadvantages: 1. Sharp edge disturbances after splicing 2. Not reliable feature extraction	2014

15.	Image Forgery Detection using Speed up Robust Feature Transform, Wavelet Transform, Steerable Pyramid Transform and Local Binary Pattern	Discrete Wavelet Transformation (DWT) and dyadic wavelet transformation techniques [65]	Copy move image forgery is detected with better accuracy.	Advantages: 1. Good efficiency 2. Reliable Disadvantages: 1. Not more suitable for noisy image 2. Time complexity is high	2016
16.	An Evaluation of Digital Image Forgery Detection Approaches	Pixel based image forgery detection [19]	Image splicing, copy-move and image resampling forgeries are detected.	Advantages: 1. Better accuracy 2. High reliability Disadvantages: 1. Will not work in the noisy image 2. Time consuming	2017
17.	A Review Paper on Digital Image Forgery Detection Techniques	Brute force, block based and key point based techniques [66]	A generalized schema is developed for detecting a copy move image forgery.	Advantages: 1. Reduced complexity 2. Quit robust Disadvantages: 1. Not efficient for complicated background and texture 2. Less accurate	2017
18.	Boosting Image Forgery Detection using Resampling Features and Copy-move Analysis	Deep learning mechanism [67]	The copy move image features are identified for detecting the forgery.	Advantages: 1. Reduced false positive 2. Highly efficient Disadvantages: 1. Not highly robust 2. Less accurate	2018
19.	Accurate and Efficient Image Forgery Detection Using Lateral Chromatic Aberration	Lateral Chromatic Aberration (LCA) and block matching algorithm [68]	Image forgery is detected by analyzing the hypothesis testing problem.	Advantages: 1. Increased efficiency 2. Reduced complexity Disadvantages: 1. Increased estimation error 2. Not suitable for noisy images	2018
20.	Recent Advances in Passive Digital Image Security Forensics: A Brief Review	Passive digital image forensic approaches [69]	It detected the image forgeries based on the artifacts.	Advantages: 1. Better generalization ability 2. Minimized time consumption Disadvantages: 1. Handling difficulty in most forgery cases 2. Performance degradation	2018
21	Image Splicing Detection using Deep Residual Network	this approach three classifiers Multiclass Model using SVM Learner, K-NN and Naïve Bayes are used to train the classifier model[70]	Spliced image forgery detection using image as input for CNN and processed through various layers	Advantages: 1- Increase the accuracy 2- Localization of spliced forged image efficiently Disadvantages: 1- Not suitable for copy-move forgery detection 2- Required highly performance system to implement the algorithms	2019
22	Image splicing forgery detection combining coarse to refined convolutional neural network and adaptive clustering	paper proposes detection method with two parts: Coarse-to- refined convolutional neural network (C2RNet) and diluted adaptive Clustering, replace patch-level CNN in C2RNet.[71]	Spliced image forgery detection with two parts (C2RNet) and diluted adaptive Clustering.	Advantages: 1- Decrease the computational complexity. 2- Tremendous decrease in the time. Disadvantages: 1- Slightly Poorer in visual performance. 2- Poorer in Recall than that of several of comparison methods.	2019
23	Image Forgery Detection: A Low Computational-Cost and Effective Data-Driven Model	low computational-cost and effective data-driven model as a Modified deep learning-based model [72]	Daubechies wavelet transform is utilized, representing YCrCb patches inside the image, neural network used to classify forged patches.	Advantages: 1- Reduce computational cost. 2- Increase accuracy. Disadvantages: 1- Not highly robust 2- Time complexity is high	2019

24	Morphological Filter Detector for Image Forensics Applications	Mathematical morphological filter detector (considered Gaussian low pass and Median filtering)[73]	operates on grayscale images, propose a non-trivial extension of a deterministic approach originally detecting erosion and dilation of binary images	Advantages: 1- Robust to image compression 2- Very high accuracy Disadvantages 1- Mathematical complexity 2- Time complexity	2020
25	Constrained Image Splicing Detection and Localization With Attention-Aware Encoder-Decoder and Atrous Convolution	Newly methods used AttentionDM for CISDL[74]	Splice forgery detection, and detects whether one image has forged regions pasted from the other	Advantages: 1- Performance improved 2- Computational improved Disadvantages: 1- Equal error rate and detection rate reduced 2- Slightly slower than DMAC	2020
26	Deep Learning Local Descriptor for Image Splicing Detection and Localization	Deep convolution neural network CNN, a two branch CNN used with automatically learn hierarchical [75]	Image splice detection and localization scheme	Advantages: 1- Robustness against JPEG compression 2- Highly detection accuracy Disadvantages: 1- Huge complexity while used 30 linear high pass filter 2- Future fusion is complex	2020

5. Conclusion and Future Work

This paper surveyed various image forensics approaches for identifying the forgeries performed on the digital images. The techniques investigated in this paper are digital signature, digital watermarking, copy-move, image splicing, and image cloning. Most of the authors stated that image forgery detection is a highly complicated process due to the advent of various manipulation and editing tools. The feature is also playing an essential role in forgery detection because the features are highly sensitive to some forgery operations. Moreover, different image processing techniques such as preprocessing, feature extraction, feature selection, and classification are highly useful for detecting the forgeries in an exact manner. The passive methods are highly suitable for forgery detection compared to the active approaches. Because it analyzes the pixel variations and estimates the geometrical illuminations in an efficient manner. Among the other passive methods, the copy-move and image splicing are widely used by many researchers due to its benefits of reduced complexity and increased accuracy.

References

[1] B. Mahdian and S. Saic, "A bibliography on blind methods for identifying image forgery," *Signal Processing: Image Communication,* vol. 25, pp. 389-399, 2010.

[2] J. Li, X. Li, B. Yang, and X. Sun, "Segmentation-based image copy-move forgery detection scheme," *IEEE Transactions on Information Forensics and Security,* vol. 10, pp. 507-518, 2015.

[3] H.-D. Yuan, "Blind forensics of median filtering in digital images," *IEEE Transactions on Information Forensics and Security,* vol. 6, pp. 1335-1345, 2011.

[4] C. Chen, J. Ni, and J. Huang, "Blind detection of median filtering in digital images: A difference domain based approach," *IEEE Transactions on Image Processing,* vol. 22, pp. 4699-4710, 2013.

[5] X. Lin, J.-H. Li, S.-L. Wang, A.-W.-C. Liew, F. Cheng, and X.-S. Huang, "Recent Advances in Passive Digital Image Security Forensics: A Brief Review," *Engineering,* 2018/02/17/ 2018.

[6] M. D. Ansari, S. P. Ghrera, and V. Tyagi, "Pixel-based image forgery detection: A review," *IETE journal of education,* vol. 55, pp. 40-46, 2014.

[7] C.-M. Pun, X.-C. Yuan, and X.-L. Bi, "Image forgery detection using adaptive oversegmentation and feature point matching," *IEEE Transactions on Information Forensics and Security,* vol. 10, pp. 1705-1716, 2015.

[8] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra, "Geometric tampering estimation by means of a SIFT-based forensic analysis," in *Acoustics Speech and Signal Processing (ICASSP), 2010 IEEE International Conference on*, 2010, pp. 1702-1705.

[9] W. Li and N. Yu, "Rotation robust detection of copy-move forgery," in *Image Processing (ICIP), 2010 17th IEEE International Conference on*, 2010, pp. 2113-2116.

[10] M. C. Stamm, S. K. Tjoa, W. S. Lin, and K. R. Liu, "Undetectable image tampering through JPEG compression anti-forensics," in *Image Processing (ICIP), 2010 17th IEEE International Conference on*, 2010, pp. 2109-2112.

[11] V. Christlein, C. Riess, and E. Angelopoulou, "On rotation invariance in copy-move forgery detection," in *Information Forensics and Security (WIFS), 2010 IEEE International Workshop on*, 2010, pp. 1-6.

[12] E. Kee and H. Farid, "Exposing digital forgeries from 3-D lighting environments," in *Information Forensics and Security (WIFS), 2010 IEEE International Workshop on*, 2010, pp. 1-6.

[13] M. Kobayashi, T. Okabe, and Y. Sato, "Detecting forgery from static-scene video based on inconsistency in noise level functions," *IEEE Transactions on Information Forensics and Security,* vol. 5, pp. 883-892, 2010.

[14] Z. He, W. Sun, W. Lu, and H. Lu, "Digital image splicing detection based on approximate run length," *Pattern Recognition Letters,* vol. 32, pp. 1591-1597, 2011.

[15] M. Jaberi, G. Bebis, M. Hussain, and G. Muhammad, "Accurate and robust localization of duplicated region in copy–move image forgery," *Machine vision and applications,* vol. 25, pp. 451-475, 2014.

[16] D. Cozzolino, D. Gragnaniello, and L. Verdoliva, "Image forgery detection through residual-based local descriptors and block-matching," in *Image Processing (ICIP), 2014 IEEE International Conference on*, 2014, pp. 5297-5301.

[17] G. Muhammad, "Multi-scale local texture descriptor for image forgery detection," in *Industrial Technology (ICIT), 2013 IEEE International Conference on*, 2013, pp. 1146-1151.

[18] 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, pp. 1566-1577, 2012.

[19] A. Kashyap, R. S. Parmar, M. Agrawal, and H. Gupta, "An Evaluation of Digital Image Forgery Detection Approaches," *arXiv preprint arXiv:1703.09968,* 2017.

[20] S. Mushtaq and A. H. Mir, "Digital image forgeries and passive image authentication techniques: A survey," *International Journal of Advanced Science and Technology,* vol. 73, pp. 15-32, 2014.

[21] L. Li, S. Li, H. Zhu, S.-C. Chu, J. F. Roddick, and J.-S. Pan, "An efficient scheme for detecting copy-move forged images by local binary patterns,"

Journal of Information Hiding and Multimedia Signal Processing, vol. 4, pp. 46-56, 2013.

[22] M. Hussain, G. Muhammad, S. Q. Saleh, A. M. Mirza, and G. Bebis, "Image forgery detection using multi-resolution Weber local descriptors," in *2013 IEEE EUROCON,* , 2013, pp. 1570-1577.

[23] T. Mahmood, T. Nawaz, R. Ashraf, M. Shah, Z. Khan, A. Irtaza*, et al.*, "A survey on block based copy move image forgery detection techniques," in *Emerging Technologies (ICET), 2015 International Conference on*, 2015, pp. 1-6.

[24] D. Chauhan, D. Kasat, S. Jain, and V. Thakare, "Survey on Keypoint Based Copy-move Forgery Detection Methods on Image," *Procedia Computer Science,* vol. 85, pp. 206-212, 2016/01/01/ 2016.

[25] T. Huynh-Kha, T. Le-Tien, S. Ha-Viet-Uyen, K. Huynh-Van, and M. Luong, "A Robust Algorithm of Forgery Detection in Copy-Move and Spliced Images," *International Journal of advanced Computer SCience and Applications,* vol. 7, pp. 1-8, 2016.

[26] A. A. Alahmadi, M. Hussain, H. Aboalsamh, G. Muhammad, and G. Bebis, "Splicing image forgery detection based on DCT and Local Binary Pattern," in *Global Conference on Signal and Information Processing (GlobalSIP), 2013 IEEE*, 2013, pp. 253-256.

[27] P. Kakar, N. Sudha, and W. Ser, "Exposing digital image forgeries by detecting discrepancies in motion blur," *IEEE Transactions on multimedia,* vol. 13, pp. 443-452, 2011.

[28] A. C. Gallagher and T. Chen, "Image authentication by detecting traces of demosaicing," in *Computer Vision and Pattern Recognition Workshops, 2008. CVPRW'08. IEEE Computer Society Conference on*, 2008, pp. 1-8.

[29] J. G. Han, T. H. Park, Y. H. Moon, and I. K. Eom, "Efficient Markov feature extraction method for image splicing detection using maximization and threshold expansion," *Journal of Electronic Imaging,* vol. 25, p. 023031, 2016.

[30] T. J. De Carvalho, C. Riess, E. Angelopoulou, H. Pedrini, and A. de Rezende Rocha, "Exposing digital image forgeries by illumination color classification," *IEEE Transactions on Information Forensics and Security,* vol. 8, pp. 1182-1194, 2013.

[31] F. Hakimi and I. M. H. Zanjan, "Image-Splicing Forgery Detection Based On Improved LBP and K-Nearest Neighbors Algorithm," *International Journal Of Electronics Information & Planning,* 2015.

[32] H. R. Chennamma and L. Rangarajan, "Image splicing detection using inherent lens radial distortion," *arXiv preprint arXiv:1105.4712,* 2011.

[33] G. Muhammad, M. Hussain, and G. Bebis, "Passive copy move image forgery detection using undecimated dyadic wavelet transform," *Digital Investigation,* vol. 9, pp. 49-57, 2012.

[34] M. Ghorbani, M. Firouzmand, and A. Faraahi, "DWT-DCT (QCD) based copy-move image forgery detection," in *Systems, Signals and Image Processing (IWSSIP), 2011 18th International Conference on*, 2011, pp. 1-4.

[35] Z. Mohamadian and A. A. Pouyan, "Detection of duplication forgery in digital images in uniform and non-uniform regions," in *Computer Modelling and Simulation (UKSim), 2013 UKSim 15th International Conference on*, 2013, pp. 455-460.

[36] S. Bayram, H. T. Sencar, and N. Memon, "An efficient and robust method for detecting copy-move forgery," in *Acoustics, Speech and Signal Processing, 2009. ICASSP 2009. IEEE International Conference on*, 2009, pp. 1053-1056.

[37] M. Jaberi, G. Bebis, M. Hussain, and G. Muhammad, "Improving the detection and localization of duplicated regions in copy-move image forgery," in *Digital Signal Processing (DSP), 2013 18th International Conference on*, 2013, pp. 1-6.

[38] N. B. A. Warif, A. W. A. Wahab, M. Y. I. Idris, R. Ramli, R. Salleh, S. Shamshirband, *et al.*, "Copy-move forgery detection: Survey, challenges and future directions," *Journal of Network and Computer Applications,* vol. 75, pp. 259-278, 2016.

[39] J. ZHENG, W. HAO, and W. ZHU, "Detection of Copy-move Forgery Based on Keypoints' Positional Relationship," *JOURNAL OF INFORMATION &COMPUTATIONAL SCIENCE,* vol. 9, pp. 4729-4735, 2012.

[40] B. Mahdian and S. Saic, "Detection of copy–move forgery using a method based on blur moment invariants," *Forensic science international,* vol. 171, pp. 180-189, 2007.

[41] G. Muhammad, M. Hussain, K. Khawaji, and G. Bebis, "Blind copy move image forgery detection using dyadic undecimated wavelet transform," in *Digital Signal Processing (DSP), 2011 17th International Conference on*, 2011, pp. 1-6.

[42] K. Asghar, Z. Habib, and M. Hussain, "Copy-move and splicing image forgery detection and localization techniques: a review," *Australian Journal of Forensic Sciences,* vol. 49, pp. 281-307, 2017.

[43] N. Chaitawittanun, "Detection of copy-move forgery by clustering technique," *International Proceedings of Computer Science & Information Technology,* vol. 50, 2012.

[44] G. Lynch, F. Y. Shih, and H.-Y. M. Liao, "An efficient expanding block algorithm for image copy-move forgery detection," *Information Sciences,* vol. 239, pp. 253-265, 2013.

[45] L. Chen, W. Lu, and J. Ni, "An image region description method based on step sector statistics and its application in image copy-rotate/flip-move forgery detection," *International Journal of Digital Crime and Forensics (IJDCF),* vol. 4, pp. 49-62, 2012.

[46] A. Kaur and R. Sharma, "Optimization of copy-move forgery detection technique," *Computer Engineering and Applications Journal,* vol. 2, 2013.

[47] M. Sridevi, C. Mala, S. Sandeep, and N. Meghanathan, "Copy–move image forgery detection in a parallel environment," *SIPM, FCST, ITCA, WSE, ACSIT, CS and IT,* vol. 6, pp. 19-29, 2012.

[48] B. Liu, C.-M. Pun, and X.-C. Yuan, "Digital image forgery detection using JPEG features and local noise discrepancies," *The Scientific World Journal,* vol. 2014, 2014.

[49] R. S. Oommen, M. Jayamohan, and S. Sruthy, "Using Fractal Dimension and Singular Values for Image Forgery Detection and Localization," *Procedia Technology,* vol. 24, pp. 1452-1459, 2016/01/01/ 2016.

[50] G. Chierchia, G. Poggi, C. Sansone, and L. Verdoliva, "A Bayesian-MRF approach for PRNU-based image forgery detection," *IEEE Transactions on Information Forensics and Security,* vol. 9, pp. 554-567, 2014.

[51] T. Bianchi and A. Piva, "Image forgery localization via block-grained analysis of JPEG artifacts," *IEEE Transactions on Information Forensics and Security,* vol. 7, pp. 1003-1017, 2012.

[52] S. Murali, G. B. Chittapur, and B. S. Anami, "Comparision and analysis of photo image forgery detection techniques," *arXiv preprint arXiv:1302.3119,* 2013.

[53] A. Piva, "An overview on image forensics," *ISRN Signal Processing,* vol. 2013, 2013.

[54] X. Pan and S. Lyu, "Region duplication detection using image feature matching," IEEE Transactions on Information Forensics and Security, vol. 5, pp. 857-867, 2010.

[55] M.-S. Hwang and C.-C. Lee, "Research Issues and Challenges for Multiple Digital Signatures," *IJ Network Security,* vol. 1, pp. 1-7, 2005.

[56] O. M. Al-Qershi and B. E. Khoo, "ROI-based tamper detection and recovery for medical images using reversible watermarking technique," in *Information Theory and Information Security (ICITIS), 2010 IEEE International Conference on*, 2010, pp. 151-155.

[57] F. Y. Shih and Y. Yuan, "16 A Comparison Study on Copy–Cover Image Forgery Detection," *Multimedia Security: Watermarking, Steganography, and Forensics,* p. 297, 2017.

[58] S. Rawat and B. Raman, "A chaotic system based fragile watermarking scheme for image tamper detection," *AEU-International Journal of Electronics and Communications,* vol. 65, pp. 840-847, 2011.

[59] B. Shivakumar and L. Baboo, "Detection of region duplication forgery in digital images using SURF," *IJCSI International Journal of Computer Science Issues,* vol. 8, 2011.

[60] J. Chao, X. Jiang, and T. Sun, "A novel video inter-frame forgery model detection scheme based on optical flow consistency," in *The International Workshop on Digital Forensics and Watermarking 2012*, 2013, pp. 267-281.

[61] M. Mishra and F. Adhikary, "Digital image tamper detection techniques-a comprehensive study," *arXiv preprint arXiv:1306.6737,* 2013.

[62] T. Qazi, K. Hayat, S. U. Khan, S. A. Madani, I. A. Khan, J. Kołodziej, *et al.*, "Survey on blind image forgery detection," *IET Image Processing,* vol. 7, pp. 660-670, 2013.

[63] E. Agnes, S. D. Mahalakshmi, and D. K. Vijayalakshmi, "A Forensic Method for Detecting Image Forgery Using Codebook," *International Journal of Advanced Research in Computer Science and Software Engineering,* vol. 3, 2013.

[64] T. K. Sarode and N. Vaswani, "Region Duplication Forgery Detection using Hybrid Wavelet Transforms," *International Journal of Computer Applications,* vol. 90, 2014.

[65] R. Kaur and T. Sharma, "Image Forgery Detection using Speed up Robust Feature Transform, Wavelet Transform, Steerable Pyramid Transform and Local Binary Pattern," *International Journal of Modern Computer Science and Applications (IJMCSA),* vol. 4, 2016.

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

[67] T. M. Mohammed, J. Bunk, L. Nataraj, J. H. Bappy, A. Flenner, B. Manjunath*, et al.*, "Boosting Image Forgery Detection using Resampling Detection and Copy-move analysis," *arXiv preprint arXiv:1802.03154,* 2018.

[68] O. Mayer and M. C. Stamm, "Accurate and Efficient Image Forgery Detection Using Lateral Chromatic Aberration," *IEEE Transactions on Information Forensics and Security,* 2018.

[69] X. Lin, J.-H. Li, S.-L. Wang, F. Cheng, and X.-S. Huang, "Recent Advances in Passive Digital Image Security Forensics: A Brief Review," *Engineering,* 2018.

[70] Ankit Kumar Jaiswal and Rajeev Srivastava, "Image Splicing Detection using Deep Residual Network," 2nd International Conference on Advanced Computing and Software Engineering (ICACSE-2019).

[71] Bin Xiao, Yang Wei, Xiuli Bi, Weisheng Li, andJianfeng Ma, "Image splicing forgery detection combining coarse to refined convolutional neural network and adaptive clustering " *Elsevier Information Sciences, 2019*.

[72] Thuong Le-Tien, Hanh Phan-Xuan, Thuy Nguyen-Chinh, and Thien Do-Tieu, " Image Forgery Detection: A Low Computational-Cost and Effective Data-Driven Model " *International Journal of Machine Learning and Computing, Vol. 9, No. 2, April 2019.*

[73] Giulia Boato, Duc-Tien Dang-Nguyen, and Francesco G. B. Denatale, " Morphological Filter Detector for Image Forensics Applications" *IEEE Access 2020.*

[74] Yaqi Liu, and Xianfeng Zhao, "Constrained Image Splicing Detection and Localization With Attention-Aware Encoder-Decoder and Atrous Convolution" *IEEE Access2020.*

[75] Yuan Rao, Jiangqun Ni, and Huimin Zhao, "Deep Learning Local Descriptor for Image Splicing Detection and Localization" *IEEE Access2020.*