IJIE

http://penerbit.uthm.edu.my/ojs/index.php/ijie
ISSN : 2229-838X e-ISSN : 2600-7916

The International Journal of Integrated Engineering

Comparative Analysis of Techniques Used to Detect Copy-Move Tampering for Real-World Electronic Images

Esha Tripathi[1,2*], Upendra Kumar[1], Surya Prakash Tripathi[3]

[1]Institute of Engineering & Technology, AKTU Lucknow, 226021, INDIA

[2]Department of Information Technology,
Pranveer Singh Institute of Technology, Kanpur, 209305, INDIA

[3]R R Institute of Modern Technology, AKTU Lucknow, 226201, INDIA

*Corresponding Author

DOI: https://doi.org/10.30880/ijie.2023.15.04.018
Received 22 February 2022; Accepted 3 August 2023; Available online 28 August 2023

Abstract: Evolution of high computational powerful computers, easy availability of several innovative editing software package and high-definition quality-based image capturing tools follows to effortless result in producing image forgery. Though, threats for security and misinterpretation of digital images and scenes have been observed to be happened since a long period and also a lot of research has been established in developing diverse techniques to authenticate the digital images. On the contrary, the research in this region is not limited to checking the validity of digital photos but also to exploring the specific signs of distortion or forgery. This analysis would not require additional prior information of intrinsic content of corresponding digital image or prior embedding of watermarks. In this paper, recent growth in the area of copy-move tampering identification have been discussed along with benchmarking study. In this study, three combination of methods like discrete cosine transform with Fast K-Means, discrete wavelet transform with Fast K-Means and discrete cosine transform with Fuzzy-C means can efficiently locate duplicated regions with quantitative parameter i.e. 92%, 83% and 92% respectively. With variety of methodologies and concepts, different applications of forgery detection have been discussed with corresponding outcomes especially using machine and deep learning methods in order to develop efficient automated forgery detection system. The future applications and development of advanced soft-computing based techniques in digital image forgery tampering has been discussed.

Keywords: Copy-move tampering, image forensic, discrete cosine transform, clustering, Fuzzy C means, copy-move forgery detection

1. Introduction

Nowadays, Image data is crucial in every field like healthcare sectors [113], Plant Disease identification [112] and cryptography [114]. Image processing is expected to be viewed as extremely sensitive area. Unfortunately, modern image-processing techniques allow for quite sophisticated malicious content manipulation that has constructive aspect and sometimes destructive also in terms of digital content security. The term Digital Image Forensics refers to the field that involves acquisition, preservation, examination, analysis, authentication [115] and retrieval of electronic data originated through various digital equipment like cameras, video recorders or computers. Although electronic photographs and digital videos act like a primary resource for evidence towards crime activity and it is also used in broadcasting and media fields. These fields are essential domain for digital image forensics. Presently there is a vast availability of a low-priced image processing methods, tools and software, which have resulted in many unique features

*Corresponding author: tripathi.esha@gmail.com

and the capacity to tamper with multimedia data without leaving any visible traces. It is utilized in the court for justice or for broadcast and media industries. All the possibilities of unauthorized manipulation of electronic data serve as a challenge to their legal integrity which serve as legal evidence in court [1-5]. Additionally, digital images are widely shared on internet using various social website, it can be easily tempered or misinterpret their significance with malicious purpose. The key objectives of this paper are:

- to provide knowledge about several aspects of identification of image tampering;
- to review some of the existing and recent methodologies used for image tampering;
- to examine a comparable analysis with its advantages and disadvantages of several existing methods.

Currently, there are several novel methodologies exists for identification of copy-move tampering. Although Warif [97] discussed the efficiency of common feature extraction methods for copy-moving manipulation and discuss the future challenges of copy-move forgery. Meanwhile, Hegazi [99] suggested an improved methodology for keypoint-based copy-move tampering. This suggested methodology focuses primarily on clustering based on density and elimination algorithm with guaranteed outlier. Whereas Du [98] introduced a new approach for forgery detection called Locality-aware Auto Encoder (LAE), to improve the accuracy of the generalization by making predictions based on correct evidence of tampering. Whereas several techniques exist for identification of digital image splicing. As Tripathi [125] discussed the multifractal dimension using Differential Box Counting (DBC) [124] method with twin support vector machine.

Through this article, the entire process of copy-move tampering detection is written in a comprehensive manner and describes different methods of extraction of features and associates many techniques for matching. Also, we outline the various datasets of copy-move tampering and with this we also implement discrete cosine transformation and discrete wavelet transformation with Fuzzy C-Means clustering or Fast K-Means clustering on Columbia Dataset and display our results by categorizing copied regions and detected areas found in copy-move tampering detection.

The remaining article is arranged as in following points. Point 2, outlines the specification of an image forgery identification. Further, copy-move methodology are classified in block and keypoint-based strategies depicted in points 3 and 4 respectively. Afterwards point 5 describes the data sets and authentications for the copy-move forgery process. Next Point 6 shows the common workflow of existing copy-move forgery techniques. The Performance matrices used for evaluation of our result is elaborated in Point 7. Finally, Point 8 provides conclusion and future direction are presented.

2. Image Forgery Detection

The current situation highlights the need for the creation of methods to confirm the integrity of the electronic image. Different methods have been developed for ensuring authentic photos. This technique is categorized into two types of methods: active method (intrusive method), passive method (non-intrusive method). in an intrusive approach, the electronic image needs to pre-embed information like a digital watermarking or electronic signature during generation of image that limits their practical applications [6]. A safeguard is made for the images to protect them from being tempered. In intrusive method, prior knowledge of the digital image is essential for authentication phase. Digital Signature [2] and watermarking [7] embed some authentic information in digital media that have objective of determining the legitimacy and uniqueness of digital data. This form of invisible information present in the image is made robust and imperceptible against all the intentionally and unintentionally attacks i.e. compression, histogram equalization, rotation, filtering, additional noise etc. But, the major drawback of active methodology is it needs alteration of the original image after capturing or storage. Additionally, images demand for especially well-formed capturing devices, the prerequisite of producing the digital watermark or signature before storing an image arises. Therefore, the use of digital signatures and watermarking techniques is not widely used by image forensic tools [3]. Although, on the internet there are many images that have no digital watermarking, signature. Therefore, to find the authenticity of digital image, intrinsic method cannot be helpful.

Though, passive approach can identify digital image tampering without prior information. This method identifies tampering through extraction of intrinsic features within the image and identification of source machine. Further detection method may be divided into two sections i.e. dependent and independent tampering. Dependent method basically covers copy-move manipulation and Image Splicing tampering. copy-move is just act of photocopying and paste an image's portion inside the same digital image and Splicing forgery refers copy one region from one image and paste on another image. Further manipulation in image like compression, re-touching and inconsistencies etc. are considered as independent forgery. On the other hand, source device identification is an action of identifying the origin of digital image capturing device based on optical and sensor regularities [1-5]. An outline of the categories of image tampering detection is depicted in Fig. 1.

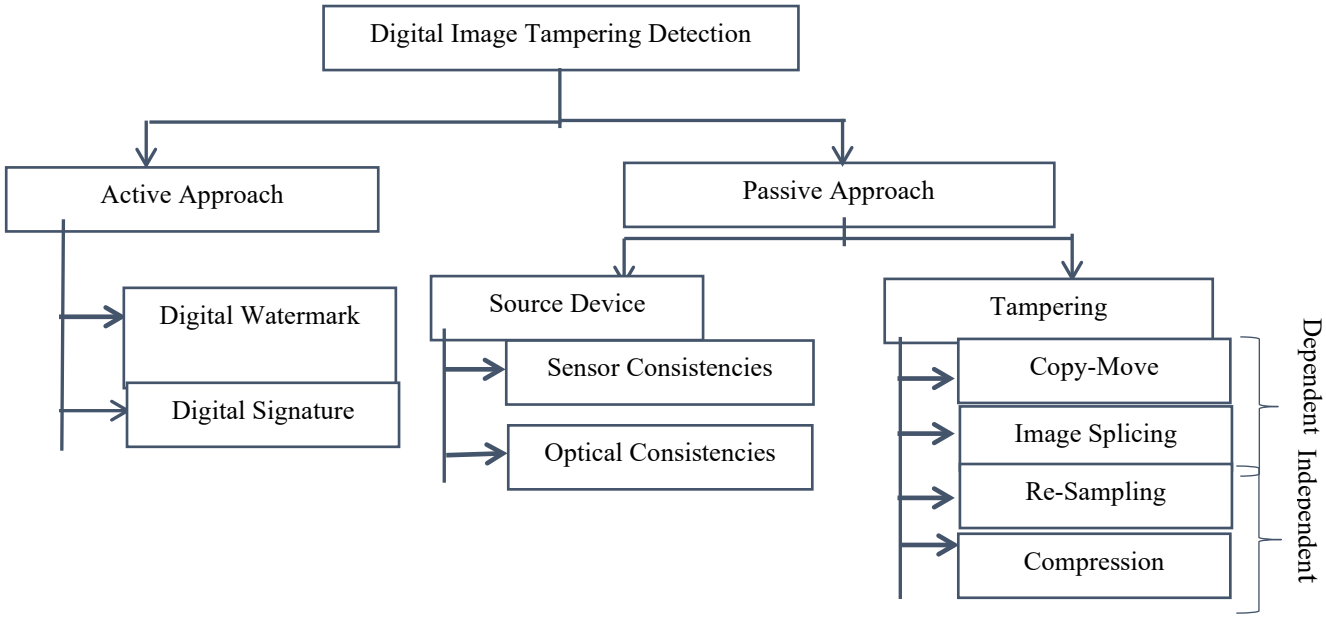

Fig. 1 - Various methods for identifying forgery in electronic images

3. Copy-Move Tampering Detection

Copy-move has seen significant interest in image tampering in past few years, in which a specific portion of photo is copied and pasted onto other position within the similar photo. As a copied portion takes from the same picture, various properties like color palette, noise components etc. will be fully compatible with remaining electronic image. Hence, identifying copy-move tampering in image data is a quit difficult task. Mostly to make the tampering unseen, few operations like image scaling, rotation, noise imposing, filtering are implemented either on the copied portion or on the whole forged image before pasting it on another image. Here we consider the papers published from 2003 to 2023 on copy-move, compiled by ScienceDirect displays in Fig. 2.

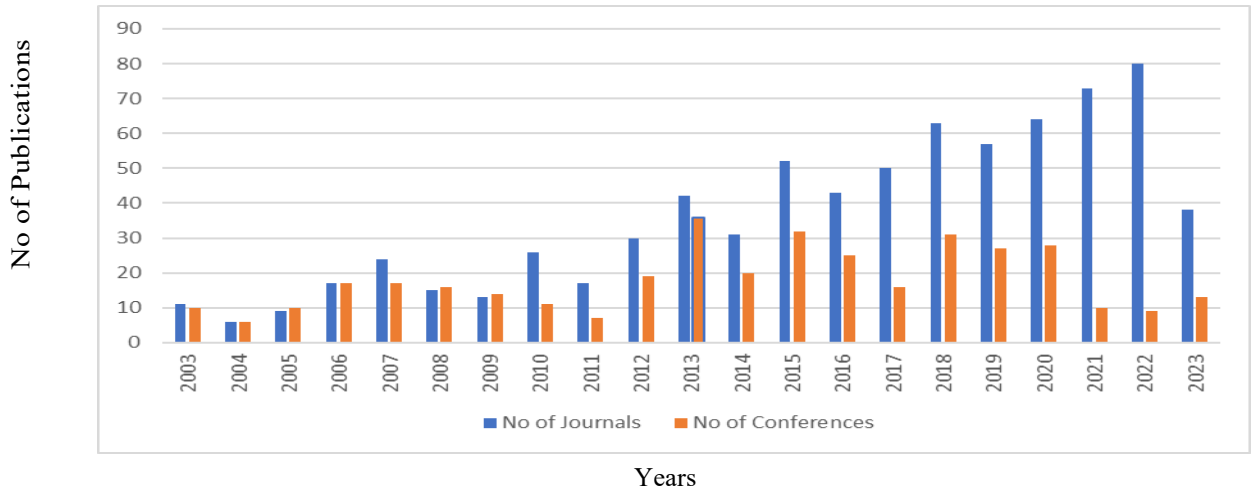

Fig. 2 - The Number of published papers in the "Science Direct" for various techniques used for copy-move tampering detection from year 2003 to 2023. Statistics are collected with the query "Copy-Move Forgery Detection" from "http:/www.sciencedirect.com."

Copy-move tampering identification techniques have been mostly categorized into two kinds of method i.e. block and key-point based method. While key-point based strategies has not followed a subdivision of digital image. and detection is totally relied on keypoint found in an image. Though, all keypoint are the high entropy regions. The major differences between both the methods of copy-move tampering are only feature-extraction

step, the remaining procedure is same. Key-point approaches are invariant to geometric transformation i.e. scaling and rotation [65].

(i) (ii)

Fig. 3 - Images shown copy-move tampering (i) real photo; (ii) tampered photo. Gravel and leaves are used to manipulate the photo with the purpose of showing Lamp light

Therefore, copy-move forgery can be unnoticeable by naked eyes. The grass, gravel, foliage, fabric with irregular patterns etc. are the very common textured region which is found in manipulated image [10]. Due to similarities in the color and texture, copied regions are simply mixed with background of digital image. Here, picture shows forgery by copy-move using leaves and gravel as a tampered region is as depicted in Fig. 3.

Table 1 - Review of publications on copy-move tampering from 2003 to 2023

Paper Title	Methodology Used	Description	Year of Publication
Detection of copy-move forgery in digital image [10]	Discrete Cosine Transformation Technique (DCT)	It will not perform for noisy images.	Fridrich et al., 2003
Exposing digital forgeries by detecting duplicated image regions [11]	Principal Component Analysis Technique (PCT)	Time complexity will be high.	Popescu et al.,2004
Robust detection of region duplication in digital image [12]	Similarity Match Technique	Time complexity will be reduced.	Luo et al.,2006
A sorted neighborhood approach for detecting duplicate reason based on DWT and SVD [13]	Discrete Wavelet Transformation (DWT) with Singular Value Decomposition (SVD) Technique	Time complexity will be less as compared from other algorithms.	Li et al., 2007
Identifying tampered regions, using singular value decomposition in Digital image forensics [16]	SVD Technique	It will not be performed for compressed and highly noisy image	Kang et al.,2008
A new approach for detecting copy-move forgery detection in digital image [14]	Discrete Wavelet Transformation Technique	It will perform well for compressed and noisy image.	Zang et al.,2008
Detection of copy-move forgery in digital images using SIFT algorithm [15]	Scale-Invariant Feature Transform Algorithm (SIFT)	It will be detected false match also.	Huang et al.,2008
Fast copy-move forgery detection [17]	Improved PCA Technique	It will be performed good for compressed and noisy image	Lin et al., 2009
Fast, automatic and fine-grained tempered JPEG image detection via DCT coefficient analysis [18]	Double Quantization Discrete Cosine Technique	It will be works well only for JPEG Image Format	Lin et al.,2009
Exploring duplicated regions in natural images, [20]	Kernel-based principal component analysis (KPCA) Technique	Identify extra noise, lossy JPEG conversation etc.	Hashmi et al.,2010

		Average precision is less than wavelet-based methods precision.	
Copy-move forgery detection in digital image [19]	Singular Value Decomposition Technique (SVD)	It will not be performed well for noisy image	Kang et al.,2010
Detecting copy-paste forgeries using transform-invariant features [24]	Transform-Invariant Feature Extraction Method	Detection will hard when image is blurred	Kakar et al.,2011
Blind copy move image forgery detection Using dyadic undecimated wavelet transform [21]	Dyadic undecimated wavelet transformation Technique	It will not perform for noisy image	Muhammad et al.,2011
Copy-move forgery detection using dyadic wavelet transform [22]	Dyadic wavelet transformation Technique	Image segmentation process and similarity identification	Muhammad et al.,2011
Detecting copy-move forgery using non-negative matrix factorization [23]	Non-negative matrix factorization Approach	Few geometric distortions like reflection, rotation will invalidate the methodology	Yao et al.,2011
Detection of copy-create image forgery using Luminance level techniques [25]	Luminance Level techniques	Time consuming and less accurate	Murali et al.,2011
Image copy-move forgery detection Based on crossing shadow division [26]	DWT with cross shadow division Method	Low complexity for computation	Hou et al.,2011
A fast image copy-move forgery detection method using phase correlation [27]	Correlation based on Phase Method	It is accurate for detecting the Duplicate image region and is very reliable to add noise and blurring	Xu et al.,2012
Detection of copy-move forgery in digital images Using radon transformation and phase correlation [33]	Phase correlation and Radon transformation Method	Identify exact tampering when tampered images will undergoing processing operation i.e. gaussian noise addition and rotation	Nguyen et al.,2012
An evaluation of popular copy-move Forgery detection approaches [28]	DCT, PCA, DWT and KPCA hybrid Technique	Low processing cost and good functioning	Christlein et al.,2012
Copy-Move Forgery Detection In Digital Images Based on Local Dimension Estimation [30]	Dimension Estimation Locally	Less Computational Efficiency	Quan et al.,2012
Copy-move image forgery detection using multi-resolution weber Descriptors [31]	Multi-resolution weber Descriptors Method (WLD)	WLD used for extraction of features from components of chrominance and reliable texture Descriptor extends to various scales, high precision	Hussain et al.,2012
Detection of copy move Forgery Image using gabor Descriptor [32]	Gabor Feature Descriptor Method	Highly Accurate and Reliable	Hsu et al.,2012
Copy-move forgery detection based on PHT [29]	Polar-Harmonic Transformation Technique	Method will not accurate for scaling, bending locally for images	Li et al.,2012
A robust image copy-move forgery detection Based on mixed moments [34]	Mixed moment, gaussian pyramid transformation	Improved accuracy and processing time with some drawbacks for smaller manipulated	Zhong et al.,2013

		region.	
Copy move image forgery detection using mutual Information [38]	Mutual statistics of different region of image	Less accurate	Chakraborty et al.,2013
A fast DCT based method for copy move forgery Detection [35]	Fast DCT Technique	It will not be performed for noisy image	Kumar et al.,2013
Copy move forgery detection using DWT and SIFT features [36]	DWT with SIFT hybrid Technique	Defects false results also	Hashmi et al.,2013
Copy move image forgery detection method using Steerable pyramid transform and texture descriptor [37]	Steerable pyramid transformation with the help of descriptor	High Accuracy comparatively	Muhammad et al.,2013
Copy-move forgery detection in images via 2D-fourier transform [39]	Two-Dimensional Fourier transformation Technique	It Identifies various copy move tampering, reliable to several attacks like jpeg compression	Ketenci et al.,2013
Copy-move image forgery detection using local binary pattern and Neighborhood clustering [40]	neighbourhood cluster Technique associated with Local Binary Pattern (LBP)	Highly accurate	AlSawadi et al.,2013
Detection of copy-move forgery using wavelet Decomposition [41]	Used method of Wavelet Decomposition	Accuracy is high	Kashyap et al.,2013
Detection of copy-move forgery using krawtchouk moment [42]	Moment used like Krawtchouk	It will perform well when noisy or blurred image used	Imamoglu et al.,2013
Video copy-move forgery detection and Localization based on tamura texture features [43]	Tamura based texture feature Extraction	Highly accurate	Liao et al.,2013
A copy-move image forgery detection based on Speeded up robust feature transform and wavelet Transforms [44]	SURF i.e. Speeded up robust feature transform with wavelet Transformation Technique	Performs good for copy-move tampering	Hashmi et al.,2014
A scheme for copy-move forgery detection in Digital images based on 2D-DWT [45]	Two-Dimension DWT Technique	Performs well for compressed and noisy image	Fattah et al.,2014
Adaptive Matching for Copy- Move Forgery Detection [46]	Adaptive Threshold for the Matching Stage to overcome tampering issue	Less Accuracy	Zandi et al.,2014
Copy-move forgery detection based on patch match [47]	Randomized algorithm for nearest- neighbour search Method	High Accuracy	Cozzolino et al.,2014
Copy-move image forgery detection Based on sift descriptors and SVD-matching [48]	Scale-Invariant Feature Transform based descriptors with Singular Value Decomposition Matching Technique	Less efficient in noisy image	Chihaoui et al.,2014
Copy-rotate-move forgery detection based on Spatial domain [49]	Used Spatial domain Technique	Highly efficient	Chihaoui et al., 2014
Copy-rotation-move forgery detection using the Mrogh descriptor [50]	Mrogh descriptor Method	Highly efficient	Yu et al.,2014
Jpeg copy paste forgery detection using bag Optimized for complex images [51]	Used Bag Optimization method	Highly efficient	Ayalneh et al.,2014
Shape based copy move forgery detection using level set approach [52]	Levels rely on various shapes	Time complexity is minimum	Sudhakar et al.,2014
Speeding-up sift based copy move forgery Detection using level set approach [53]	Keypoint method i.e. SIFT with Level set Method	Less efficient	Sudhakar et al.,2014
Video frame copy-move forgery detection based on cellular automata	Cellular automation with LBP Method	Highly efficient	Tralic et al. ,2014

and local binary patterns [55]			
Robustness of copy-move forgery detection under high JPEG compression artifacts [57]	Fast Fourier transformation, Principal Component Analysis and SVD	Fully threshold-free and high accuracy	Huang et al.,2015
Multi-Level Dense Descriptor and Hierarchical Feature Matching for Copy–Move Forgery Detection [54]	Hierarchical Clustering Technique for performing Matching and Multi-Level Dense Descriptor	Robust against various attacks	Xiuli, et al.,2016
Covert copy-move forgery detection based on color LBP [56]	Gray level co-occurrence matrix (GLCM) and K-d tree; Euclidean distance	Eliminate the false matched blocks using morphological operation then identify the regions contains copy-move tampering	Zhu et al.,2017
Copy-move forgery detection based on hybrid features [58]	KAZE, SIFT both methods used for fetching features	Robust interest point detector Precisely locate tampered regions having rotation, JPEG compression, scaling and adding noise distortion.	Yang et al.,2017
Hybridized Technique for Copy-Move Forgery Detection Using Discrete Cosine Transform and Speeded-Up Robust Feature Techniques [101]	Combining block-based method i.e. DCT and a keypoint-based method i.e. SURF	Effectively detect multiple copy-move attacks and also detect scaling, rotation, and mixture of scaling and rotation, blur, noisy, compressive attacks.	Ojeniyi et al.,2018
An Image Copy-Move Forgery Detection Scheme Based on A-KAZE and SURF Features [102]	Accelerated-KAZE with speeded-up robust features Transformation	Fast feature extraction and robustness to identify tampered areas	Wang et al.,2018
An improved copy-move forgery detection based on density-based clustering and guaranteed outlier removal [99]	Guaranteed Outlier Removal algorithm and Density-based clustering	High Accuracy with tampered region detected effectively	Hegazi et al., 2019
Towards Generalizable Forgery Detection with Locality-aware AutoEncoder [98]	Locality aware AutoEncoder (LAE) Technique	Boost the generalization accuracy	Du et al., 2019
Tampering detection using hybrid local and global features in wavelet-transformed space with digital images [116]	Local binary pattern variance technique with Histogram of oriented gradients (HOG) descriptor	Accurate for tampered region	Jothi et al.,2020
A passive forensic scheme for copy-move forgery based on superpixel segmentation and K-means clustering [117]	Apply SIFT features for complex regions and for smooth regions apply sector mask feature with RGB color feature	Improve the detection accuracy	Liu et al.,2020
Image splicing detection using mask-RCNN [118]	ResNet-convolutional network with Recurrent CNN	Initial feature map made more efficient	Ahmed et al.,2020
Image copy-move forgery passive detection based on improved PCNN and self-selected sub-images [119]	Self-selected sub-images with Improved Pulse coupled neural network	High robustness rating and accuracy score	Zhou et al.,2022
An enhanced copy-move forgery detection using machine learning based hybrid optimization model [120]	Prewitt mm′ Filter with Generalized Action Selection based Hybrid Artificial Bee Colony African Buffalo Optimization	Good results for image contain rotation and scaling	Rao et al.,2022
Accurate and robust image copy-move forgery detection using adaptive	Adaptive keypoint feature extraction and domain features	High-precision	Wang et al.,2023

keypoints and FQGPCET-GLCM feature [121]	extract through texture features through GLCM and Fast Quaternion Generic Polar Complex Exponential Transform (FQGPCET)

3.1 Block-Based Approach

In block-based theory division of entire digital photo into several overlapped or non-overlapped blocks. Later, comparison between each block decides how many blocks are matching. Then portion of an image enclosed by matched blocks are the sections that have been copied and forged as shown in Fig. 4

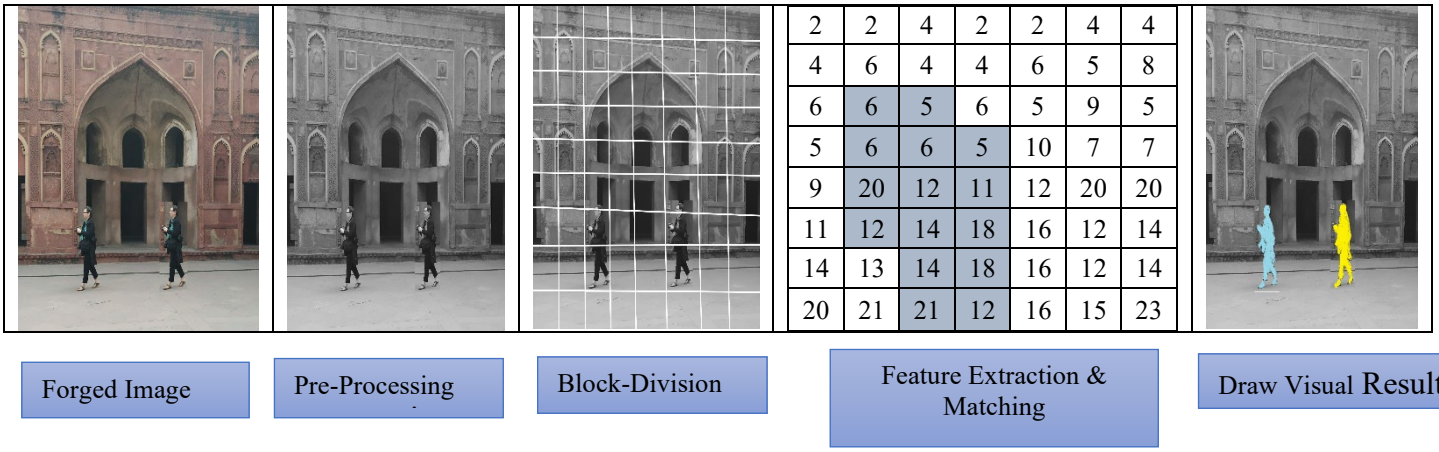

Fig. 4 - The Copy-move process via block-based strategy

In past decades, mostly block-based is a common technique implemented by researchers, possibly its compatibility nature with several extraction approaches and higher matching efficiency.

■ Feature Extraction Techniques followed by Block-Based Approach

Commonly, there are several feature extraction methods used in block-based approach which works in digital image forensic i.e. intensity and texture based method, log polar transformation method, moment invariant method, dimensionality reduction method, frequency based method etc. Table 2 provides a description of the methods for extraction.

3.1.1 Frequency Based

Frequency transformation is one of the earliest approaches employed by block-based approaches. Firstly, Fridrich et al. [10] delivered a methodology of Discrete Cosine Transform (DCT), using an idea of overlapping block. After compared this strategy against several other block-based methodologies, it has been observed to be more efficient, but this method is prone to the changes due to additive noise in copied regions. Afterwards, Cao et al. [59] recommended that Discrete Cosine Transform coefficient has been modified by reduced the frequency containing higher coefficient which results in a functional dimension reduction and this is also effective for jpeg compressed image, blurring and distortion of Additive White Gaussian Noise (AWGN). Later Bashar et al. [60] found methodology to identify duplication through two or more reliable features which rely on Discrete Wavelet Transform (DWT) and Kernel Principal Component Analysis (KPCA). Projected vectors that depended on KPCA and the blocks of respective image with multi-resolution wavelet coefficients are organized in matrix form for performing lexicographic sorting. Rotation of an image is also rectified with the help of geometric transformation. This technique eliminates the threshold of offset frequency that itself to be manually altered as analogous to other detection approaches. Afterwards Bayram et al. [61] recommended Fourier Mellin Transformation (FMT) scheme which used filter (counting bloom) to save computational cost in place of lexicographic sorting.

3.1.2 Intensity and Texture Based

Texture is present in realistic scenes and image attributes like smoothness, roughness, regularity (reflect the content of texture) [37]. Therefore, it should be utilized to recognize similarities in manipulated images produced by copy move tampering. The need for k-dimension tree allows matching techniques to search blocks having same intensity patterns introduced by Langille et al. [62] and kd-tree also decreases the difficulty of the computations.

Although, Lynch et al. [63] built expanding block technique for the identification of manipulated portion. This process involves that an electronic image is first partitioned into overlapped blocks. After comparing dominant feature for each block, there is a formulation of connection matrix. Formed connection matrix includes row having zeros, it means blocks contained certain row are not linked with another block in the bucket. It is a better method for defining the shape and location of distorted regions, and it is possible to perform comparison between blocks.

Luo et al. [64] used statistical study of several pixel of small overlapping image blocks to build an algorithm for extracting digital image characteristics, then comparing similarity between blocks. At that moment, find forged area with the support of intensity-based features. This methodology is vulnerable for blurring, noise contamination, lossy compression with the accuracy of 96%. Whereas Ardizzone et al. [65] proposed the study of bit-plane to categorize various texture of gray scale in content present in the picture. Although, bit plane study is quite weak for detection of JPEG electronic images based on changes intensity level in compression.

Table 2 - Methodology used by feature extraction method followed by block-based techniques

	Feature-Extraction Techniques	Author & Year	Methodology used	Feature-Length
Block-Based Feature Extraction Techniques	Frequency Based	Fridrich et al., 2003 [10]	DCT	64
		Cao et al., 2012 [59]	Circular block DCT with Lexicographic Sorting	4
		Bashar et al., 2010 [60]	DWT and KPCA with Lexicographical sorting	256
		Bayram et al., 2009 [61]	Fourier-Mellin Transform with Lexicographic Sorting & Counting Bloom Filter	45
	Intensity & Texture Based	Lynch et al., 2013 [63]	Enhanced expanding block algorithm	-
		Langille et al., 2006 [62]	intensity patterns of blocks with Kd-sorting	-
		Luo et al., 2006 [64]	Statistical study of pixels with overlapping blocks with Lexicographical sorting	-
		Ardizzone et al., 2010 [65]	Texture descriptors with Lexicographical sorting	-
	Moments Invariant	Mahdian et al., 2007 [67]	Blur Moment with KD-tree	24
		Ryu et al., 2010 [69]	Zernike Moment	12
		Hu et al., 2014 [70]	Exponential Moment	5
	Log-Polar Transformation	Li et al., 2012 [42]	Polar Harmonic Transform	-
		Bravo-Solorio et al., 2013 [103]	Log Polar Coordinates	-
		Li et al., 2013 [41]	Polar Cosine Transform	-
		Li et al., 2014 [43]	Polar Sin Transform	-
	Dimensionality Reduction	Popescu et al., 2004 [23]	Principal Component Analysis with Duplication map	32
		Bashar et al., 2010 [4]	Kernel Principal Component Analysis (Non-linear)	192
		Kang et al., 2008 [13]	Singular Value Decomposition	-
		Zhao et al., 2010 [44]	Locally Linear Embedding	-

3.1.3 Moments Invariant

Moment invariants are features which are invariant in an image for the translation, rotation and scale of related regions. These are beneficial as these describe a simple a set of regional attributes that could be used to classify various shapes and identify the component. Firstly, usage of moment invariants was suggested by Hu et. al in 1962, for character recognition(2-Dimension), numerous modifications have introduced based on the orthogonal polynomial series and the distribution of probabilities. And the various modification like central moment, exponential moment, Zernike moment and Krawtchouk's moment have been recommended for solving several problems related to regular moments. Although regular moments which are computationally costly because of redundancy present in data, position dependency and it is showing global features in place of local feature.

Mahdian et al. [67] initially used the blur moments invariant for copy-move forgery detection. Basically, blur moment refers by arithmetic function that contains centralize moment and it can be quite sensitive towards additive noise, alterations in blur loss, random contrast etc. Extracting features from dataset having a large size digital images can increase difficulty of the computation. With the combination of DWT and blur moment,

computation complexity can be much reduced [41]. Moreover, Bilgehan et al.[68] suggested that a most reliable moment is Krawtchouk moment for various operations like post-processing, performing Gaussian Blurring and detecting tampering of all types of shaped areas. As according to Hu et al.,1962, Zernike is comparatively robust moment for rotation invariant. Whereas it is not strong against manipulation based on an affine transformation and scaling according to Ryu et al. [69]. Moreover, Hu et al. [70] presents the exponential moment that enhances the efficiency of Zernike moments.

At last, moment invariant is a global feature which is inherently depends on location. Hence, this technique is not suitable for object recognition. There are several means to ensure invariance of the location must be adopted.

3.1.4 Log-Polar Transform

Log-polar transformation method for extraction of features invariant for scaling, translation, rotation etc. This method functions when projection mapping taken from points (x, y) over Cartesian plane to the log-polar points (x, h). Firstly, Li et al. [73] proposed log-polar transformations method i.e. Log Polar Fourier Transform (LPFT) for copy-move tampering identification. Further, among other CMFD (Copy-move Forgery Detection) approaches, the Polar Harmonic Transform (PHT) method analyzes circular blocks instead of regular square blocks [71]. Such techniques are typically resilient for various post-processing functions i.e. apply Additive white Gaussian noise (AWGN), apply Gaussian blurring, perform lossy compression. Moreover, Li et al.,2013[72] proposed that Polar Cosine Transform is efficient compared to the Zernike moment against noise with minimum computational time and according to Li et al. [74] survey, polar sine transform (PST) has the highest invariance for geometric distortions.

3.1.5 Dimensionality Reduction

Dimensionality reduction methods with domain features are widely used to minimized the dimension of electronic images and to maximize complexity inappropriately. However, there is two common technique used as dimension reduction i.e. Singular Value Decomposition (SVD) with the help of Locally Linear Embedding (LLE) technique. In general, SVD technique is efficient, scalable, generates invariance of rotation either for an arithmetic or geometric characteristic. Ting et al. [75] implements SVD which generally decreases computation complexity and is reliable especially for scaling, Gaussian noise, filtering and rotation operations. But, SVD results in a lack of image data and poor performance for JPEG compression. Moreover, LLE can be applied in high-dimensional dataset to decrease the dimension of digital images [76]. LLE defines topological relationship between nonlinear data set and maps large sized image data type to small sized image data type with no alteration of relative positions. As compared to PCA implemented by Popescu et al. [11], LLE is capable of detecting fused edges which is hidden in the manipulated image, whereas PCA has recommended minimum time for computation. But SVD performs well in terms of efficiency for various operations.

3.2 Matching Performed in Block-Based Strategies

Matching is a method of finding similarities among two or more features in an electronic image. Then matching procedure may have accomplished afterwards each and every feature of electronic image are firstly evaluated and then extracted to show the tampered portion. There is various method of matching features of an image for block-based method as summarized in Table 3.

Table 3 - Description of various sorting techniques

Sorting Techniques	Description
Lexicographical Sorting	Generalized form of feature value based on the alphabetical order.
K-dimensional Tree	Space partitioning for arranging points in a K-Dimensional space.
Radix Sorting	Sorting algorithm have non-comparative nature which prevents from comparison by constructing and distributing data items into various buckets corresponding to their radix.

4. Keypoint Based Strategies

Keypoint based strategies do not rely on method of block division refer to Fig. 8. In this strategy, features are basically extracting the local features distinctively like edges, image's corners, image's blobs. Each feature of keypoint based strategies is represented as a collection of descriptors generated within a particular region around the keypoint features.

Fig. 5 - The Copy-move process via keypoint based strategies

The descriptor facilitates the affine transformation to enhance the consistency of the features. Afterwards, digital image features and descriptors are classified and matched for finding the manipulated areas found in the copy-move tampering.

4.1 Feature Extraction Methods Used for Keypoint Based Strategies

In keypoint based strategies there are various techniques for feature extraction used like Harris corner detector, SIFT (Scale invariant feature transform), SURF (Speed up robust features). Various extraction method used for keypoint based strategies is listed in Table 4.

4.1.1 Harris Corner Detector

Firstly, Harris corner detector concept was given by Harris and Stephens in 1988 which implements keypoint techniques are accompanied by SIFT. This detector extracts edges and corners from particular areas that rely on local auto correlation function.

Chen et al. [77] suggested a copy-move tampering identification scheme which depend on the Harris corner points then move sector statistics for tampering detection, afterwards best-bin-first approach is utilized to search tampered area. Zhao et al. [78] presented a strategy for finding area duplication in electronic images through merging Harris corner points and local binary pattern.

4.1.2 Scale Invariant Feature Transformation

SIFT feature extraction technique is the widespread and very reliable methodology, perhaps due to its robust nature against geometrical transformation (rotation, scaling etc.). Firstly, SIFT is developed by David G. Lowe (1999) for object recognition community. SIFT detects salient and stable feature points in scale-space representation at different scales by using Difference of Gaussian (DoG) method. Difference of Gaussians means approximation of LoG (Laplacian of Gaussian) which acts like blob detector that finds blobs of various sizes due to variation in scaling parameter. DoG is cheaper compare to LoG and is used during the extraction phase to boost the computing speed in digital photo. Thereafter, Huang et al. [80] and Ardizzone et al. [65] extracted feature as SIFT descriptor [80], and the search method best-bin-first is used to suit for same type of features. Li et al. [81] used the algorithm of expectation maximization and Dense Scale-Invariant Feature Transform (DSIFT) to evaluate the transformation matrix whereas Karsh et al. [82] uses Affine-Scale-Invariant Feature Transform (ASIFT) that identifies copy-move tampering. Typical keypoint-based strategies are SIFT, ASIFT, DSIFT, MIFT i.e. Mirror reflection Invariant Feature Transform [83], MROGH i.e. Multi-support Region Order-based Gradient Histogram [84].

Table 4 - Methodology used by feature extraction method followed by keypoint-based techniques

Key-point Feature Extraction Technique	Feature-Extraction Techniques	Author & Year	Methodology used	Feature-Length
	Harris Corner	Chen et al., 2013 [77]	Harris corner detection points	72
		Zhao et al., 2013 [78]	Harris corner points with Local Binary Pattern	-
	Scale Invariant Feature Transformation	Huang et al., 2008 [80]	SIFT Feature Extraction Method	128
		Li et al., 2015 [81]	DSIFT	-
		Karsh et al., 2016 [82]	ASIFT	-
		Jaberi et al., 2014 [83]	MIFT (Mirror reflection Invariant Feature Transform)	-
		Yu et al., 2016 [84]	MROGH (Multi-support Region Order-based Gradient Histogram)	-
		Yang et al., 2017 [58]	KAZE with SIFT	-
	Speed Up Robust Features	Bo et al., 2010 [85]	SURF Features Extraction Method	128
		Mishra et al., 2013 [87]	SURF and Hierarchical Agglomerative Clustering	maybe 64

4.1.3 Speed Up Robust Features

SURF basically utilized to minimize processing time and also try to reduce dimension of the feature. Bay et al. [86] initially proposed SURF technique for enhancing SIFT efficiency. Bo et al. [85] introduces the SURF-based methodology, where they expanded the Bay techniques and length of feature becomes 128. Although it can reduce the chances of false matches specifically for images having high-resolution and being reliable for various post-processing operation and for transformation. Yet, this is not identifying a small area inside image which has been copied. Further, Mishra et al. [87] was shown that SURF and Hierarchical Agglomerative Clustering (HAC) technique minimizes the efficiency although this enhances computation cost in copy-move tampering identification.

4.2 Matching Techniques Applies in Keypoint Based Strategies

It is possible to identify similarities between several feature point inside a digital image using the method of finding the nearest neighbor which is an active research subject. Though, due to high computational complexity very hard to identify a manipulation in digital image.

In this segment, various nearest neighbor approaches apply on keypoint based strategies which are categorized into four or many parts i.e. best-bin first, two nearest neighbourhood, generalized two nearest neighbourhood and clustering. Respective literature is listed in Table 5.

Table 5 - Description of matching methods applies in keypoint based methods

Matching Methods	Description
Best Bin First	The Best Bin First (BBF) approach is a fast way to discover the nearest neighbour among a large number of high-dimensional feature descriptors. The approach begins with the construction of a balanced k-d tree, which is then searched using the best-bin-first strategy.
2NN (Two Nearest Neighbourhood)	Examine the distance proportion for the main points between the 1st nearest neighbour and 2nd nearest neighbour called Two Nearest Neighbourhood (2NN) a well-known matching process for keypoints.
g2NN (Generalized Two Nearest Neighbourhood)	Consider the ratio for distance of the nearest neighbour [n] to nearest neighbour's [n+1] and g2NN metric with $d_n/d_{(n+1)}$ ratio and here d_n is Euclidean distance of nearest neighbour [n] where $1 \leq n \leq N$. When the ratio is less than given threshold, the matching between two key points will be shown.
Clustering	K-Nearest Neighbours is the most effective clustering technique that can tried to categorize various points rely on known categorization of another points. “k” in K-Nearest Neighbours is the number of neighbours it checks.

5. Publicly Available Datasets

Since datasets are an essential component for research of modern computer vision. For the significant progress in the research field, datasets are the main reasons. Copy-move forgery detection has some benchmarking datasets which is publicly accessible to do some effective study. Although several datasets work differently for various type of aspects. Ideally these type of datasets offers a variety of electronic images with genuine manipulation activities for copy-move. Available datasets used for copy-move tampering shown in below Table 6.

The open accessed existing dataset can't be adequate to fulfil the necessity of researchers. Moreover, some databases contain original and tampered images both which is used to find accuracy of the system used for forgery detection. These are maintained for research work in the electronic image analysis field, digital image processing, machine vision The images present in datasets be utilized to apply the copy-move tampering with assistance of several editing tools like Adobe Photoshop, Photoscape, Paint Shop, PhotoPlus, GIMP and Pixelmator.

Recently, there are seven datasets accessible on the internet: Image Manipulation Dataset [28], MICC [88], Copy-Move Hard (CMH) [91], CoMoFoD [89], CMFDdb_grip [90], Copy-Move Forgery Dataset [65] and COVERAGE [92].

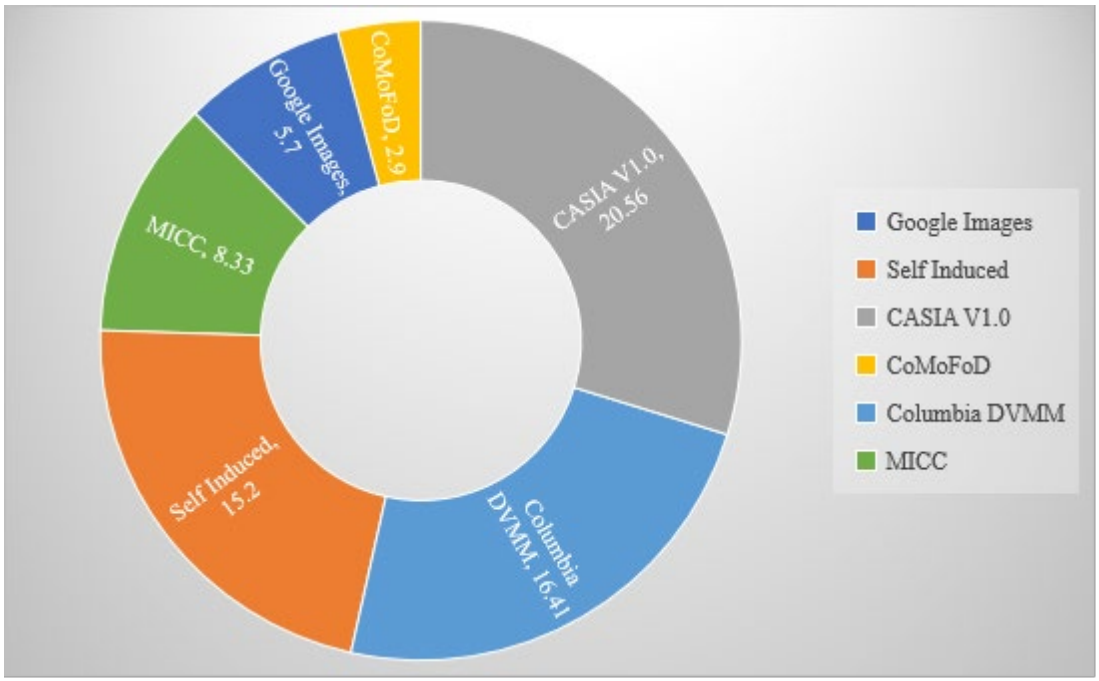

Fig. 6 - Usage of datasets of images in percentage for forgery detection in the different publications

Fig. 6 depicts the different image forensic datasets utilized by the researchers to validate their methodologies; it is shown that CASIA and Columbia dataset has been used by the most of the researchers. Whereas some of the researcher used self-clicked images also.

Table 6 - Existing datasets for copy-move forgery with description and applications

Dataset name	Size of Images	Total image	Short description and application of dataset
Columbia University [105]	128 × 128	1845	■ Image splicing and copy-move tampering ■ Real images and tampered images ■ Separated into 2 groups (Textured vs. Smooth, Straight boundary vs. Random object boundary)
Korus [108]	1920 × 1080	220	■ copy-move and Image splicing ■ TIF format
CASIA v1.0 [106]	374 × 256	1725	■ Image cloning and splicing ■ Real and tampered image ■ JPEG format ■ Division in various classes like scene, plant, animal, character,

			architecture, article, texture, and nature etc.
CASIA v2.0 [106]	240 × 160 to 900 × 600	12614	■ Image splicing and copy-move tampering ■ Real and tampered image ■ JPEG compressed and uncompressed image
Image manipulation [110]	420 × 300 to 3888 × 2592	48	■ Used for Copy-move tampering ■ Real images and tampered images ■ Employed with lossy compression i.e. jpeg, rotation and scaling function done in images
MICC-F220 [8]	722 × 480 to 800 × 600	220	■ Real and tampered image ■ Employed with scaling (symmetric/asymmetric), translation, rotation or combination of these operations
MICC-F600 [8]	800 × 533 to 3888 × 259	600	■ Real and tampered image ■ Taken from SATs- 130 and MICC-F2000 datasets arbitrary
MICC-F2000 [8]	2048 × 1536	2000	■ Real and tampered image ■ Employed with scaling (symmetric/asymmetric), translation, rotation, or combination of these operations
CoMoFoD [107]	512 × 512 to 3000 × 200	260	■ Real and tampered image ■ Employed with scaling, rotation translation, distortion, and a grouping of these operations
SATs-130 [109]	Variable size	120	■ Real images and tampered images, used for copy-move ■ JPG format

6. Workflow of Proposed Methodology

Generally, CMFD methodology follows four phases that is pre-processing, extraction of features, matching, and visual result drawn that is refer in Fig. 7. Every phase will be explored here in following points.

6.1 Conversion from Colored Digital Image to Gray Image

Grayscale pictures are commonly used to perform image processing procedures. Gray-scale pictures need fewer mathematical operations to identify an item than color photos. In detecting image manipulation as we are interested to find out which places have been distorted in digital images. It can be found that classification using gray images results in greater accuracy compared to color images [93]. As a result, every recommended technique initially attempts to convert a color image to a gray-scaled electrical image, i.e. RGB values, 24 bits, into grey values, 8 bits. If the input picture is in RGB format, the RGB values are then converted to Gray-scale values using given equation below: Grayscale-Image = 0.288*Red Pixels + 0.587*Green Pixels + 0.114*Blue Pixels

6.2 Division of Gray Images into Overlapping Blocks

Divide the R x C image into small overlapped blocks of (b x b) pixels which results in N blocks and N = (R-b+1) x (C-b+1). When entire image is examined with the sliding of block from very top left corner to bottom right corner then it results as blocks.

6.3 Apply Dimension Reduction with Feature Extraction Techniques

Discrete Cosine Transform (DCT) is basically utilized for extraction of features in several fields like image tampering detection, image compression techniques and brain signal classification. DCT is firstly used by Ahmad et al. [94] in 1974 to use the conversion of signals from spatial to frequency transform. Discrete Cosine Transform transformation is imposed on every block in this stage. Assuming block size is of (b x b) and elements are present in matrix. Since According to DCT nature however not all elements of image are equally essential. In order to simplify reduction of feature length process, DCT coefficients have been re-shaped in zigzag manner and forms row vector which is depicted as Fig. 3. Then coefficients with indices have been removed which is bigger than threshold value which helps in reduction of dimension of feature vector and minimize the computation cost.
skip this block to the next one.

Following Eq. 1 evaluates DCT coefficient for only one entry i.e. (p, q)th entry of transformed pixel value contained image and r(x, y) refers to x, yth data element of an image denoted through a 2-D matrix 'r', where 'N' refers to the size of each block on which DCT technique is implemented.

$$D(p,q) = \frac{1}{\sqrt{2N}} C(p)C(q) \sum_{x=0}^{N-1}\sum_{y=0}^{N-1} r(x,y).\cos\frac{(2x+1)i\pi}{2N}\cos\frac{(2y+1)i\pi}{2N} \quad (1)$$

$$C(U) = \begin{cases} \frac{1}{\sqrt{2}} & if\ U = 0 \\ 1 & if\ U > 0 \end{cases}$$

Then for standard block i.e. 8 x 8 that is generally used for JPEG compression then the value of N equals to 8 and the range of x, y taken as 0,1,2, 3, …,7. Therefore, now equation for DCT coefficient D (p, q) becomes as Eq 2.

$$D(p,q) = \frac{1}{4} C(p)C(q) \sum_{x=0}^{7}\sum_{y=0}^{7} r(x,y).\cos\frac{(2x+1)i\pi}{16}\cos\frac{(2y+1)i\pi}{16} \quad (2)$$

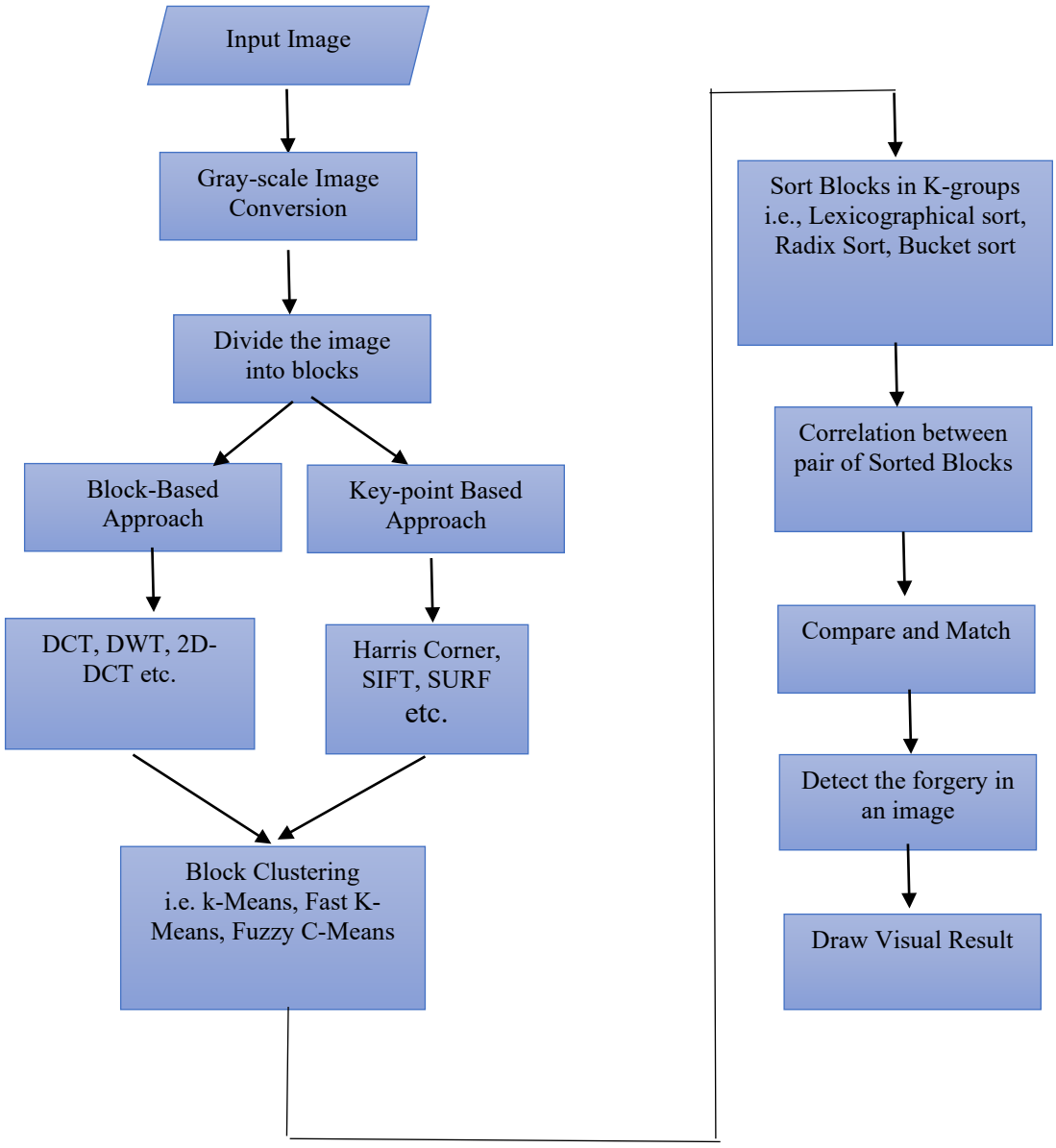

Fig. 7 - General workflow of copy-move tampering identification techniques

6.4 Reduce Blocks Using Clustering Algorithms

The goal of the clustering is splitting input data in a variety of clusters according to similarity basis. Data points put in one cluster which having similarity compare to other points and so on. There are several algorithms for clustering used for copy-move forgery i.e. Fuzzy C-Means, Fast K-means, K-means, K-Nearest Neighbour (KNN) and two-pass KNN algorithm etc. Although k-means technique makes number of groups having similarity between objects rely on features, hence k denotes positive number. In k-means, groups are formed by minimizing sum of squares of distance between input data and respective centroid of a cluster. Afterwards, Fast K-Means clustering methodology suggested by researcher C. Elkan [95], which prevents from distance calculation by using triangle inequality. The difficulty is that the upper bounds will be provided by triangle inequalities, but it requires lower bound for minimizing the calculation. Assume 'x' be an input datapoint, (b, c) are center points then we require to understand these conditions for triangle inequalities:

i) if d (b, c) ≥ 2d (x, b) then d (x, c) ≥ d (x, b)
ii) d (x, c) ≥ max {0, d (x, b)-d (b, c)}

6.5 Sort the Clustered Block

To identify forged regions, block feature vectors have been sorted through several sorting methods i.e. Radix sort, Bucket Sort, lexicographical sort etc. Although Radix sorting with the most significant digit is utilized to sort the clustered blocks vectors in ascending order. Whereas in lexicographically sorting, similar values are sorted in left to right manner to obtain new series of vectors allowing for comparison with each neighbouring vector (Bashar et al.,2010) [60]. Here Fig. 8 shows how the blocks are sorted after applying clustering.

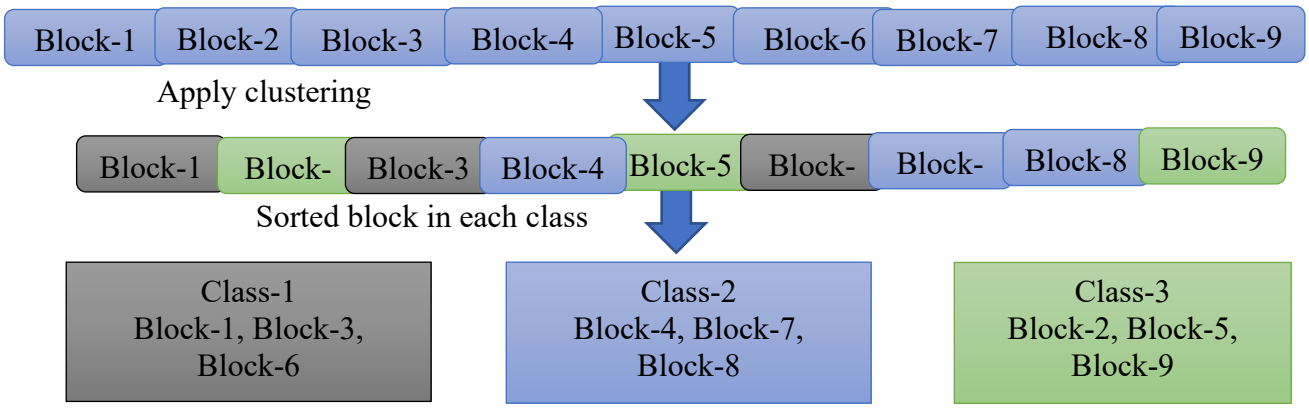

Fig. 8 - Blocks arranged in clusters and sorted according to class

6.6 Evaluating Correlation

Correlation is evaluated among two similar blocks by the given equation (Eq. 3)

$$Correlation = \frac{\sum_{i=1}^{N}(m-m').(n-n')}{\sqrt{\sum_{i=1}^{N}(m-m')^2 \sum_{i=1}^{n}(n-n')^2}} \quad (3)$$

here m, n is block coefficients using DCT and m', n' are the respective mean of coefficient, N refers count of block coefficients. Whenever the correlation value exceeds the specified threshold value, then similarity between two blocks are shown. Moreover, distance should be found between similar blocks for eliminating the false positives, otherwise, The distance between two similar blocks could be given by following equation (Eq. 4):

$$Distance = \sqrt{(M_i^m - M_{i+1}^m) + (M_i^n - M_{i+1}^n)} \quad (4)$$

Where (M_i^m, M_i^n), (M_{i+1}^m, M_{i+1}^n) are location of $(i)^{th}$, $(i+1)^{th}$ block respectively.

Find distance between same type of blocks if Distance has a larger value than threshold distance (D), Where S=16, then there is a presence of forgery in an image then point out the tampered blocks.

7. Performance Measure

Moreover, a classification model assessment always operates on common principles; every data has actual and predicted output. Though the predicted output is observed as a result of detection, the real outcome of copy-move manipulation is ground truth. Thus, for each dataset, output can be allocated to one of four statistics: True Positive (TP), False Positive (FP), True Negative (TN), False Negative (FN), as depicted in Table 7 in confusion matrix.

Table 7 - Confusion Matrix

Actual	Predicted Spliced Image	Predicted Authenticated Image
Spliced Image	True Positive (TP)	False Negative (FN)
Authentic Image	False Positive (FP)	True Negative (TN)

Numerous researchers presented many criteria to assess the efficiency of their proposed algorithms. Hence, they used a variety of groupings, like True Positive Rate (TPR) and True Negative Rate (TNR), TPR and False Positive Rate (FPR), ACC and FPR, P and R and P, R and F1 which is written in Table 8.

Table 8 - Classification metrics with various parameters

Metrics	Equation	Description
True Positive Rate (TPR) or Recall (R)	$TPR = \frac{TP}{TP + FN}$	It estimates proportion of positives which are identified correctly.
False Positive Rate (FPR)	$FPR = \frac{FP}{FP + TN}$	It estimates proportion of negatives wrongly detected as positive.
True Negative Rate (TNR) or Specificity	$TNR = \frac{TN}{FP + TN} = 1 - FPR$	It estimates proportion of negatives detected correctly.
False Negative Rate (FNR)	$FNR = \frac{FN}{TP + FN} = 1 - TPR$	It estimates proportion of positive components that are mistakenly classified as negatives.
Precision (P)	$P = \frac{TP}{TP + FP}$	It estimates the degree of probability for which identified area is precise.
Accuracy (Acc.)	$Acc = \frac{TP + TN}{TP + TN + FP + FN}$	It estimates proportion of total number of predictions which were correct.
F_1-Measure	$F1 = \frac{2.P.R}{P + R} = \frac{2.TP}{2.TP + FN + FP}$	It estimates harmonic mean of Recall value and Precision value.
Mean Square Error	$MSE = \frac{1}{xy}\sum_{i=0}^{x-1}\sum_{j=0}^{y-1}[A(i,j) - B(i,j)]^2$	A is real result and B is the result expected by methodology employed and x, y denotes row and column of the images respectively.
Peak Signal to Noise Ratio	$PSNR = 10\log_{10}(\frac{MAX_I^2}{MSE})$	Here MAX_I denotes the over-all pixel in the images.
Jaccard Index	$JI = \frac{\lvert A \cup B \rvert}{\lvert A \cap B \rvert}$	Jaccard Index should have pixel similarity between ground truth (A) and segmented result (B). When the Jaccard Index is higher than result 's accuracy.
Dice Similarity Coefficient	$DSC = \frac{2.\lvert A \cup B \rvert}{\lvert A \rvert + \lvert B \rvert}$	Dice Similarity Coefficient (DSC) provides pixel similarity between ground truth (A) and segmented result (B).

Last three metrics of Table 8 together with ACC and F1-measure are therefore sufficiently to assess performance if it can identify certain pixels that correspond to altered areas of copy-move forgeries. Although accuracy is measured statistically by the proportion of true positive to true negative results as well as the overall number of cases examined [72]. While accuracy has historically been a poor measurement when there is a probability that the picture dataset may be significantly out of balance. Unbalanced dataset often refers to when the copy-move area in a manipulated picture is very tiny in comparison to the whole image size. As a result, with an imbalanced dataset, measures like as accuracy and recall are commonly utilized. Though pixel count in copy-move and authentic class have been unequal, thereafter both classes have not been likely significant [73] then the parameters are preferred i.e. recall and precision. Most systems provide a desirable balance among both the metrices precision and recall, which must be taken after joining them in a

matrix known as F1-measure. F1-measure, recall and precision, these parameters commonly utilized in area of information retrieval [75]. Although Mean Square Error (MSE), Jaccard Index, Peak Signal to Noise Ratio (PSNR), Dice Similarity Coefficient or Dice-overlap-index (DOI) also used as an evaluation standard for performance.

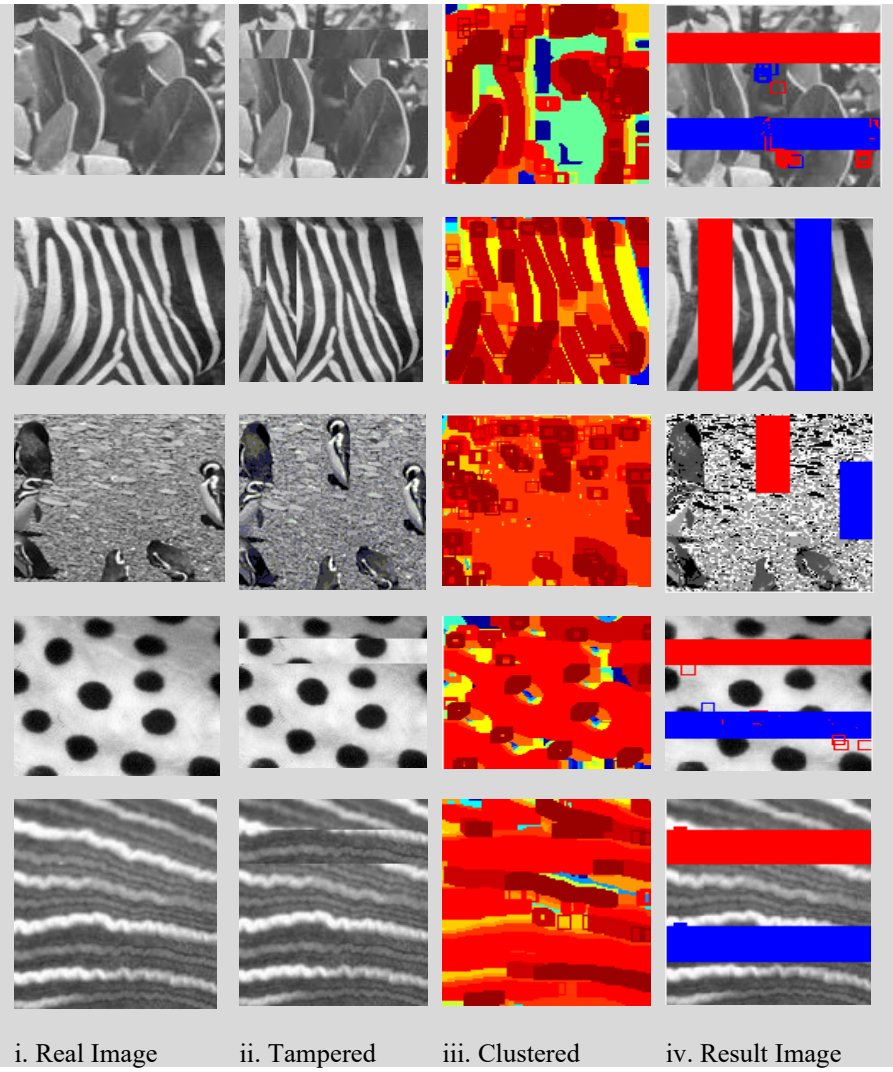

Fig. 9 - Here blue region shows actual images and red region shows detected region which are identifying as a results for tampered images

Though, we must define image with a collection of various local patches (blocks or keypoints) in conventional CMFD frameworks and then pass CMFD to a comparison problem between those local patches. When the count of patches is very large, then comparison process can be time consuming, i.e. various block-based methods [12], [61], [69] generally require a large amount of time to identify a digital image. Therefore, this is beneficial to minimize count of patches for comparison. In this reference, the keypoint based methodologies are robust and faster compare to block-based methods, since the number of keypoints in an image is lower than that of the block division.

Instead, Keypoint-based method still has two major issues. First issue is determining the shortest gap between two equivalent keypoints is tedious, since keypoints lie spatially very close to each other must not be compared because they may be inherently similar. Second issue is that it is difficult to precisely locate and differentiate the source region for copying and the target region for pasting [81]. To tackle this issue, Amerini et al. [88] proposed a method focused on clustering perform for matched keypoints, that was also incorporated by the framework of the CMFD evaluation. Therefore, the new clustering-based Copy-Move Tampering system greatly improves the precision of localization of Copy-move regions.

Table 9 - Various parameter for copy-move forgery using DCT with Fast-K-means clustering

Image No.	True Positive Rate	True Negative Rate	False Positive Rate	False Negative Rate	Precision	Recall	Accuracy
i.	1	0.998833	0.00116686	0	99.4048	99.8833	85.8942
ii.	1	0.902025	0.0979749	0	66.3834	90.2025	78.9863
iii.	1	0.994383	0.00561675	0	97.2020	99.4383	85.5606
iv.	1	0.997448	0.00255195	0	98.7056	99.7448	85.808
v.	1	0.998251	0.00174927	0	99.1071	99.8251	85.8883
				Average	**92.16**	**97.82**	**84.43**

In this context, we propose a methodology having discrete cosine transformation with Fast K-Means clustering. I have also checked the results of Discrete Wavelet transform with same clustering. Thus, outcome is expressed by image level detection errors with false positive rate and false negative rate. At next level, we estimated our proposed CMFD system by pixel-level precision and accuracy which is shown in Fig. 9. The estimation of the effects of detection is determined according to equation given in Table 8 equations and provided in Table 9. These experiments are performed on MATLAB R2019b platform and the Columbia dataset is used as an image dataset.

Table 10 - Various parameter for copy-move forgery using DWT with Fast-K-means clustering

Image No.	True Positive Rate	True Negative Rate	False Positive Rate	False Negative Rate	Precision	Recall	Accuracy
i.	1	0.996208	0.0037923	0	98.091	99.6208	85.7053
ii.	1	0.810096	0.189904	0	50.4655	81.0096	72.3582
iii.	1	0.986213	0.013786	0	93.4008	98.6213	84.973
iv.	1	0.9607	0.0393	0	83.1983	96.07	83.1628
v.	1	0.976493	1.0235071	0	89.2952	97.6493	84.2265
		Average			**82.89**	**94.59**	**82.09**

Here Table 9,10 and Table 11 shows our experiment in which we found result in the terms various parameters of confusion matrix for copy-move forgery where various feature extraction methods are applied like DCT, DWT and various clustering techniques like Fast K-Means, Fuzzy C-Means [104] are applied for performing matching among similar blocks.

Table 11 - Various parameter for Copy-move forgery using DCT with Fuzzy C-means clustering

Image No.	True Positive Rate	True Negative Rate	False Positive Rate	False Negative Rate	Precision	Recall	Accuracy
i.	1	0.998833	0.00116686	0	99.4048	99.8833	85.8942
ii.	1	0.902025	0.0979749	0	66.3834	90.2025	78.9863
iii.	1	0.994383	0.00561675	0	97.2020	99.4383	85.5606
iv.	1	0.997448	0.00255195	0	98.7056	99.7448	85.808
v.	1	0.998251	0.00174927	0	99.1071	99.8251	85.8883
		Average			**92.16**	**97.82**	**84.43**

We try to improve the results from existing algorithm that is depicted in Table 12. Here Fig. 9 depicts the comparative study of clustering techniques based on accuracy and precision apply with feature-extraction method.

Table 12 - Comparison between existing and proposed methodology

Existing Algorithm	Precision	Recall	Accuracy
Alkawaz et al. [122]	64.529	96.58	79.51
Hayat et al. [123]	72.50	96.30	81.80
Proposed Methodology:			
DCT + Fast K-Means	92.16	97.82	84.43
DWT + Fast K-Means	82.89	94.59	82.09
DCT + Fuzzy C Means	92.16	97.82	84.43

Moreover, we point out that our proposed method has a low computational cost for a small dataset but for other geometric transformation that requires our further research to improve it.

Fig. 10 - Graph showing variation of precision and accuracy of (DWT with Fast K-Means), (DCT with Fuzzy C-Means) techniques

8. Conclusion

In this article, a variety of research papers of duration 2003-2023, majorly covering detection of copy-move forgery from the suspicious digital images, have been used for literature review and benchmarking study. In this review it has been observed that the study on copy-move forgery has emerged as highly interesting research area to investigate critical scenario form static images as well as video streams-based scenes. A comprehensive analysis of existing copy-move tampering identification methods has been discussed in this article which is based on variety of methodologies with different outcomes. The proposed models have variety of feature extractions methods and also different types of classifiers, correspondingly they perform well for different kinds of real time problems. The variety of techniques used in both strategies has been discussed with their performances with relevant CMFD activities including several datasets. Thereafter, classifications of copied regions (ROI of forgery detection) were discussed to determine their importance to current real time applications used for CMFD. Although, additional work should be done to address various competing difficulties, there is a strong requirement to additional research and apply several diverse deep learning techniques in addressing the copy-move detection problem. Recently, in digital forensics, deep learning CMFD techniques like Multi-domain CNN, Convolutional Neural Network (CNN), Convolutional Long Short-Term Memory (Conv-LSTM) and Buster-Net, extract image characteristics employing layers with extensive training and validation methods to reach optimal scenario. Though use of deep learning systems has gained most of attention of the researchers. But these techniques involve big GPU systems containing millions of data for providing training for getting better and efficient results. Despite of complexity issue of deep learning, in upcoming days it considered as a standard device.

Acknowledgment

The authors fully acknowledged the Institute of Engineering & Technology, Pranveer Singh Institute of Technology and R R Institute of Modern Technology for supporting this work.

References

[1] Cheddad A (2012) Doctored Image Detection: A Brief Introduction to Digital Image Forensics. Inspire magazine, July 2012.

[2] Qazi T, Hayat K, Khan SU, Madani SA, Khan IA, Kołodziej J, Li H, Lin WYKC, Xu CZ (2013) Survey on Blind Image Forgery Detection. IET Image Processing; 7(7), 1–11.

[3] Guojuan Z and Dianji L (2011) An Overview of Digital Watermarking in Image Forensics. In: Proc. of 4th IEEE International Joint Conference on Computational Sciences and Optimization, pp 332-335.

[4] Swaminathan A, Wu M and Liu KJR (2008) Digital Image Forensics via Intrinsic Fingerprints. IEEE Trans on Information Forensics and Security, 3(1), 101-117.

[5] Weiqi L, Zhenhua Q, Feng P and Jiwu H (2007) A Survey of Passive Technology for Digital Image Forensics. Review article, Front. Comput. China.
[6] Gomase PG, Wankhade NR (2014) Advanced Digital Image Forgery Detection-A Review. Iosr Journal of Computer Science (Iosr-Jce) E-Issn: 2278-0661, P-Issn: 2278-8727 Pp 80-83.
[7] Zhang J, Feng Z, Su, Y (2008) A new approach for detecting copy-move forgery in digital images, in: 11th IEEE Singapore International Conference on Communication Systems, ICCS. pp. 362–366. http://dx.doi.org/10.1109/ICCS.2008. 4737205.
[8] Qazi T, Hayat K, Khan SU, Madani SA, Khan IA, Kołodziej J, Li H, Lin WYKC, Xu CZ (2013) Survey on Blind Image Forgery Detection. IET Image Processing; 7(7), 1–11.
[9] Zhang, J., Feng, Z., Su, Y (2008) A new approach for detecting copy-move forgery in digital images, in: 11th IEEE Singapore International Conference on Communication Systems, ICCS 2008. pp. 362–366. http://dx.doi.org/10.1109/ICCS.2008. 4737205.
[10] Fridrich J, Soukal D, Lukas J (2003) Detection of copy move forgery in digital images," Proceedings of the Digital Forensic Research Workshop, pp. 5-8, Aug. 2003.
[11] Popescu AC, Farid H (2004) Exposing digital forgeries by detecting duplicated image regions.Dept. Comput. Sci., Dartmouth College, Tech. Rep., TR2004-515, 2004.
[12] Luo WQ, Huang JW, Qiu GP (2006) Robust detection of region duplication forgery in digital image," 18th International Conference on Pattern Recognition (ICPR), Vol. 4, pp. 746-749.
[13] Li GH, Wu, Tu D, Sun SJ (2007) A sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWT and SVD. Proceedings of IEEE International Conference on Multimedia and Expo, Beijing, Jul. 2007, pp. 1750-1753.
[14] Zhang J, Feng Z, Su Y (2008) A new approach for detecting copy-move forgery in digital images," IEEE International Conference on Communication Systems, China, pp. 362-366.
[15] Huang H, Guo W, Zhang Y (2008) Detection of copy-move forgery in digital images using SIFT algorithm. Pacific-Asia Workshop on Computational Intelligence and Industrial Application, Vol. 2, pp. 272-6.
[16] Kang X, Wei S (2008) Identifying tampered regions using singular value decomposition in digital image forensics. International Conference on Computer Science and Software Engineering, Vol. 3, pp. 926-930.
[17] Lin HJ, Wang CW, Kao YT (2009) Fast copy-move forgery detection. WSEAS Transaction on Signal Processing, pp. 188-197, 2009.
[18] Lin Z et al (2009) Fast, automatic and fine-grained tampered JPEG image detection via DCT coefficient analysis. Pattern Recogn.,Vol. 42, pp. 2492-2250.
[19] Kang L, Cheng XP (2010) Copy-move forgery detection in digital image. 3rd IEEE International Congress on Image and Signal Processing (CISP 2010), pp. 2419-2421.
[20] Hashmi MF, Hambarde AR, Keskar AG (2013) Copy move forgery detection using DWT and SIFT features. 13th International Conference on Intellient Systems Design and Applications, Bangi, pp. 188-193.
[21] Muhammad G, Hussain M, Khawaji K, Bebis G (2011) Blind copy move image forgery detection using dyadic undecimated wavelet transform. 17th International Conference on Digital Signal Processing (DSP), Corfu, pp. 1-6.
[22] Muhammad N, Hussain M, Muhammad G, Bebis G (2011) Copy-Move Forgery Detection Using Dyadic Wavelet Transform. Eighth International Conference on Computer Graphics, Imaging and Visualization (CGIV), Singapore, pp. 103-108.
[23] Yao H, Qiao T, Tang Z, Zhao Y, Mao H (2011) Detecting Copy-Move Forgery Using Non-Negative Matrix Factorization. Third International Conference on Multimedia Information Networking and Security, Shanghai, pp. 591-594.
[24] Kakar P, Sudha N (2011) Detecting copy-paste forgeries using transform invariant features. IEEE 15th International Symposium on Consumer Electronics (ISCE), Singapore, pp. 58-61.
[25] Murali S, Anami BS, Chittapur GB (2011) Detection of Copy-Create Image Forgery Using Luminance Level Techniques. Third National Conference on Computer Vision, Pattern Recognition, Image Processing and Graphics (NCVPRIPG), Hubli, Karnataka, pp. 215-218.
[26] Hou D, Bai Z, Liu S (2011) Image copy-move forgery detection based on crossing shadow division. International Conference on Electric Information and Control Engineering (ICEICE), Wuhan, 2011, pp. 1416-1419.
[27] Xu B, Liu G, Dai Y (2012) A Fast Image Copy-Move Forgery Detection Method Using Phase Correlation. Fourth International Conference on Multimedia Information Networking and Security, Nanjing, pp. 319-322.
[28] Christlein V, Riess C, Jordan J, Riess C, Angelopoulou E (2012) An Evaluation of Popular Copy-Move Forgery Detection Approaches. IEEE Transactions on Information Forensics and Security, vol. 7, no. 6, pp.1841-1854.
[29] Li L, Li S, Wang J (2012) Copy-move forgery detection based on PHT. World Congress on Information and Communication Technologies (WICT), pp. 1061-1065, Trivandrum.

[30] Quan X, Zhang H (2012) Copy-move forgery detection in digital images based on local dimension estimation. International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), Kuala Lumpur, pp. 180-185.
[31] Hussain M, Muhammad G, Saleh SQ, Mirza AM, Bebis G (2012) Copy-Move Image Forgery Detection Using Multi-Resolution Weber Descriptors. Eighth International Conference on Signal Image Technology and Internet Based Systems (SITIS), Naples, pp. 395-401.
[32] Hsu HC, Wang MS (2012) Detection of copy-move forgery image using Gabor descriptor. Anti-counterfeiting, Security, and Identification, pp. 1-4, Taipei.
[33] Nguyen HC, Katzenbeisser S (2012) Detection of Copy-move Forgery in Digital Images Using Radon Transformation and Phase Correlation. Eighth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), Piraeus, pp. 134-137.
[34] Zhong L, Xu W (2013) A robust image copy-move forgery detection based on mixed moments. 4th IEEE International Conference on Software Engineering and Service Science (ICSESS), Beijing, pp.381-384.
[35] Kumar S, Desai J,Mukherjee S (2013) A fast DCT based method for copy move forgery detection. IEEE Second International Conference on Image Information Processing (ICIIP), Shimla, pp. 649-654.
[36] Hashmi MF, Hambarde AR, Keskar AG (2013) Copy move forgery detection using DWT and SIFT features. 13th International Conference on Intellient Systems Design and Applications, Bangi, pp. 188-193.
[37] Muhammad G, Al-Hammadi MH, Hussain M, Mirza AM, Bebis G (2013) Copy move image forgery detection method using steerable pyramid transform and texture descriptor. IEEE EUROCON, Zagreb, pp. 1586-1592.
[38] Chakraborty S (2013) Copy move image forgery detection using mutual information. Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT), Tiruchengode, pp.1-4.
[39] Ketenci S, Ulutas G (2013) Copy-move forgery detection in images via 2D-Fourier Transform. 36th International Conference on Telecommunications and Signal Processing (TSP), 2013, Rome, pp. 813-816.
[40] AlSawadi M, Muhammad G, Hussain M, Bebis G (2013) Copy-Move Image Forgery Detection Using Local Binary Pattern and Neighborhood Clustering. Modelling Symposium (EMS), pp. 249-254, European, Manchester.
[41] Kashyap A, Joshi SD (2013) Detection of copy-move forgery using wavelet decomposition. International Conference on Signal Processing and Communication (ICSC), Noida, pp. 396-400.
[42] Imamoglu MB, Ulutas G, Ulutas M (2013) Detection of copy-move forgery using Krawtchouk moment. 8th International Conference on Electrical and Electronics Engineering (ELECO), Bursa, pp.311-314.
[43] Liao SY, Huang TQ (2013) Video copy-move forgery detection and localization based on Tamura texture features. 6th International Congress on Image and Signal Processing (CISP), Hangzhou, pp. 864-868.
[44] Hashmi MF, Anand V, Keskar AG (2014) A copy-move image forgery detection based on speeded up robust feature transform and Wavelet Transforms. International Conference on Computer and Communication Technology (ICCCT), Allahabad, pp. 147-152.
[45] Fattah SA, Ullah MMI, Ahmed M, Ahmmed I, Shahnaz C (2014) A scheme for copy-move forgery detection in digital images based on 2D-DWT. IEEE 57th International Midwest Symposium on Circuits and Systems (MWSCAS), College Station, TX, pp. 801-804.
[46] Zandi M, Mahmoudi-Aznaveh, Mansouri A (2014) Adaptive matching for copy-move Forgery detection. IEEE International Workshop on Information Forensics and Security (WIFS), Atlanta, GA, pp. 119-124.
[47] Cozzolino D, Poggi G, Verdoliva L (2014) Copy-move forgery detection based on PatchMatch," IEEE International Conference on Image Processing (ICIP), Paris, pp. 5312-5316.
[48] Chihaoui T, Bourouis S, Hamrouni K (2014) Copy-move image forgery detection based on SIFT descriptors and SVD-matching. 1st International Conference on Advanced Technologies for Signal and Image Processing (ATSIP), Sousse, pp. 125-129.
[49] Fadl SM, Semary NA, Hadhoud MM (2014) Copy-rotate-move forgery detection based on spatial domain. 9th International Conference on Computer Engineering and Systems (ICCES), Cairo, pp. 136-141.
[50] Yu L, Han Q, Niu X (2014) Copy-Rotation-Move Forgery Detection Using the MROGH Descriptor. IEEE International Conference on Cloud Engineering (IC2E), 2014, Boston, MA, pp. 510-513.
[51] Ayalneh DA, Kim HJ, Choi YS (2014) Jpeg copy paste forgery detection using bag Optimized for complex images. 16th International Conference on Advanced Communication Technology, Pyeongchang, pp. 181-185.
[52] Sudhakar K, Sandeep VM, Kulkarni S (2014) Shape Based Copy Move Forgery Detection Using Level Set Approach. Fifth International Conference on Signal and Image Processing (ICSIP), Jeju Island, 2014, pp. 213-217.
[53] Sudhakar K, Sandeep VM, Kulkarni S (2014) Speeding-up SIFT based copy move forgery detection using level set approach. International Conference on Advances in Electronics, Computers and Communications (ICAECC), Bangalore, pp. 1-6.

[54] Bi X, Pun CM , Yuan XC (2016) Multi-Level Dense Descriptor and Hierarchical Feature Matching for Copy–Move Forgery Detection. Information Sciences Volume 345, Pages 226-242

[55] Tralic D, Grgic S, Zovko-Cihlar B (2014) Video frame copy-move forgery detection based on Cellular Automata and Local Binary Patterns. 10th International Symposium on Telecommunications (BIHTEL), 2014, Sarajevo, pp. 1-4.

[56] Zhu Y, Shen XJ, Chen HP (2017) Covert copy-move forgery detection based on color LBP. Acta Automatica Sinica, 2017, vol. 43, no. 3, pp. 390-397.

[57] Huang DY, Huang CN, Hu WC, Chou CH (2015) Robustness of copy-move forgery detection under high JPEG compression artifacts. Multimedia Tools and Applications, vol. 76, no. 1, pp. 1509-1530.

[58] Yang F, Li J, Lu W, Weng J (2017) Copy-move forgery detection based on hybrid features. Engineering Applications of Artificial Intelligence, 2017, vol. 59, pp. 73-83.

[59] Cao Y, Gao T, Fan L, Yang Q (2012) A robust detection algorithm for copy-move forgery in digital images. Forensic science international, Vol. 214, No. 1, pp.33–43.

[60] Bashar M, Noda K, Ohnishi N, Mori K (2010) Exploring duplicated regions in natural images. IEEE transactions on image processing, p.1, 2010.

[61] Bayram S, Sencar HT, Memon N(2009) An Efficient And Robust Method For Detecting Copy-Move Forgery. In: IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). pp. 1053–1056.

[62] Langille A, Gong M (2006) An efficient match-based duplication detection algorithm. Proc. of the 3rd Canadian conference on computer and robot vision, pp. 64.

[63] Lynch G, Shih YN, Liao HYN (2013) An efficient expanding block algorithm for image copy-move forgery detection. Information Sciences, vol. 239, pp. 253-265.

[64] Luo W, Huang J, Qiu G (2006) Robust detection of region-duplication forgery in digital image. In 18th international conference on pattern recognition, (ICPR); Hong Kong, pp. 746-749.

[65] Ardizzone E, Bruno A, Mazzola G (2010) Copy-move forgery detection via texture description. In Proceedings of the 2nd ACM workshop on Multimedia in forensics, security and intelligence, ACM, pp. 59-64.

[66] Hu MK (1962) Visual Pattern Recognition by. Moment Invariants. IRE Transaction on Information Theory 2, 179–187.

[67] Mahdian B, Saic S (2007) Detection of Copy-Move Forgery using a Method Based on Blur Moment Invariants. Forensic Science International, vol. 171, no. 2, pp. 180–189, Dec. 2007.

[68] Bilgehan M, Uluta M (2013) Detection of Copy-Move Forgery Using Krawtchouk Moment. In: 8th International Conference on Electrical and Electronics Engineering (ELECO), pp. 311–314.

[69] Ryu S, Lee M, Lee H (2010) Detection of Copy-Rotate-Move Forgery using Zernike Moments. In Information Hiding Conference, pp. 51–65.

[70] Hu H, Zhang Y, Shao C, Ju Q (2014) Orthogonal moments based on exponent functions: exponent-Fourier moments. Pattern Recognition. 47, 2596–2606.

[71] Li L, Li S, Wang J (2012) Copy-move forgery detection based on PHT. Proceeding 2012 World Congr. Inf. Commun. Technology WICT, pp. 1061–1065. http://dx.doi. org/10.1109/WICT.2012.6409232.

[72] Li Y (2013) Image copy-move forgery detection based on polar cosine transform and approximate nearest neighbor searching. Forensic Sci. Int. 224, 59–67. http://dx.doi.org/10.1016/j.forsciint.2012.10.031.

[73] Li L, Li S, Zhu H, Wu X (2014) Detecting copy-move forgery under affine transforms for image forensics. Comput. Electr. Engineering. 40, 1951–1962. http://dx.doi.org/10.1016/j.compeleceng.2013.11.034.

[74] Li W, Yu N (2010) Rotation robust detection of copy-move forgery, in: Proceedings- International Conference on Image Processing, ICIP. pp. 2113–2116. doi:10.1109/ICIP.2010.5652519.

[75] Ting Z, Rang-Ding W (2009) Copy-move forgery detection based on SVD in digital image, in: 2nd International Congress on Image and Signal Processing, CISP'09. pp. 0–4. http://dx.doi.org/10.1109/CISP.2009.5301325.

[76] Zhao J (2010) Detection of copy-move forgery based on one improved LLE method. 2nd IEEE Int. Conf. Adv. Comput. Control 4, 547–550. http://dx.doi.org/10.1109/ ICACC.2010.5486861

[77] Chen L, Lu W, Ni J, Sun W, Huang J (2013) Region duplication detection based on Harris corner points and step sector statistics. Journal of Visual Communication and Image Representation, vol. 24, no. 3, pp. 244-254.

[78] Zhao J, Zhao W (2013) Passive forensics for region duplication image forgery based on Harris feature points and local binary patterns. Mathematical Problems in Engineering article no. 619564, 2013, vol. 2013, no. article 619564.

[79] Lowe DG (2004) Distinctive Image Features from Scale-Invariant Keypoints. International Journal of Computer Vision, volume 60, pp. 91–110.
[80] Huang H, Guo W, Zhang Y (2008) Detection of copy-move forgery in digital images using SIFT algorithm. In Proceedings of the IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application, pp. 272-276.
[81] Li J, Li X, Yang B, Sun X (2015) Segmentation-based image copy-move forgery detection scheme. IEEE Transactions on Information Forensics and Security, vol. 10, no. 3, pp. 507-518.
[82] Karsh RK, Das A, Swetha GL, Medhi A, Laskar RH, Arya U, Agarwal RK (2016) Copy-move forgery detection using A SIFT. In Proceedings of the 1st India International Conference on Information Processing, Delhi, India, pp. 1-5.
[83] Jaberi M, Bebis G, Hussain M, Muhammad G (2014) Accurate and robust localization of duplicated region in copy–move image forgery. Machine Vision and Applications, vol. 25, no. 2, pp. 451-475.
[84] Yu L, Han Q, Niu X (2016) Feature point-based copy-move forgery detection: covering the non-textured areas. Multimedia Tools and Applications, vol. 75, no. 2, pp. 1159-1176.
[85] Bo X, Junwen W, Guangjie L, Yuewei D (2010) Image Copy-Move Forgery Detection Based on SURF. In Multimedia Information Networking and Security, pp. 889–892.
[86] Bay H, Ess A (2008) Speeded-Up Robust Features (SURF). Computer Vision Image Understanding 110, 346–359. http://dx.doi.org/10.1016/j.cviu.2007.09.014
[87] Mishra P, Mishra N, Sharma S, Patel R (2013) Region duplication forgery detection technique based on SURF And HAC. Sci. World J.
[88] Amerini I, Ballan L, Caldelli R, Del Bimbo A, Serra G (2011) A SIFT-based forensic method for copy-move attack detection and transformation recovery. IEEE Trans. Inf. Forensics Secur., vol. 6, no. 3, pp. 1099–1110.
[89] Tralic D, Zupancic I, Grgic S, Grgic M (2013) CoMoFoD - New Database for Copy-Move Forgery Detection. In Proceedings of 55th International Symposium ELMAR, 2013, pp. 49–54.
[90] Cozzolino D, Poggi G, Verdoliva L (2014) Copy-move forgery detection based on patchmatch. In the International Conference on Image Processing (ICIP), pp. 5247–5251.
[91] Silva E, Carvalho T, Ferreira A, Rocha A (2015) Going deeper into copy-move forgery detection: Exploring image telltales via multi-scale analysis and voting processes. J. Vis. Commun. Image Represent., vol. 29, pp. 16–32.
[92] Wen B, Ye Z, T.-T. Ng RS, Shen X, Winkler S (2016) COVERAGE – A Novel Database for Copy-Move Forgery Detection. In Proceedings of the IEEE International Conference on Image Processing (ICIP), pp. 161–165.
[93] Kanan C, Cottrell G.W (2012) Color-to-grayscale: does the method matter in image recognition. PLoS ONE 7(1), 1–7.
[94] Ahmed N, Natarajan T, Rao K (1974) Discrete Cosine Transform. IEEE Transactions on Computers, Vol. 23, No. 1, pp. 90-93.
[95] Elkan C (2003) Using the triangle inequality to accelerate k-means. ICML. pp. 147-153.
[96] Al-Qershi OM, Khoo BE (2018) Evaluation of Copy-Move Forgery Detection: Datasets and Evaluation Metrics. Multimedia Tools and Applications, DOI: 10.1007/s11042-018-6201-4
[97] Warif NBA, Wahab AWA, Idris MYI, Roziana Ramli, Salleh R, Band SS, Choo K-KR (2016) Copy-move forgery detection: Survey, challenges and future directions. Journal of Network and Computer Applications, Volume 75, pp. 259-278
[98] Du M, Pentyala S, Li Y, Hu Y (2019) Towards Generalizable Forgery Detection with Locality-aware AutoEncoder. arXiv:1909.05999v1 [cs.CV].
[99] Hegazi A , Taha A, Selim MM (2019) An improved copy-move forgery detection based on density-based clustering and guaranteed outlier removal. Journal of King Saud University –Computer and Information Sciences, https://doi.org/10.1016/j.jksuci.2019.07.007.
[100] Ng TT, Hsu J, Chang SF. Columbia Image Splicing Detection Evaluation Dataset. Available: http://www.ee.columbia.edu/ln/dvmm/downloads/AuthSplicedDataSet/AuthSplicedDataSet/
[101] Ojeniyi JA, Adedayo BO, Ismaila I, Shafi'i AM (2018) Hybridized Technique for Copy-Move Forgery Detection Using Discrete Cosine Transform and Speeded-Up Robust Feature Techniques. I.J. Image, Graphics and Signal Processing, 4, 22-30.DOI: 10.5815/ijigsp.2018.04.03
[102] Wang C, Zhang Z, Zhou X (2018) An Image Copy-Move Forgery Detection Scheme Based on A-KAZE and SURF Features. Symmetry 2018, 10, 706; doi:10.3390/sym10120706
[103] Bravo-Solorio S, Nandi A (2011) Exposing duplicated regions affected by reflection, rotation and scaling. In: IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp.1880–1883. http://dx.doi.org/10.1016/j.sigpro. 2011.01.022.
[104] Tripathi E, Kumar U, Tripathi SP, Yadav S (2019) Automated Image Splicing Detection using Texture based Feature Criterion and Fuzzy Support Vector Machine based Classifier. International Conference on

Cutting-edge Technologies in Engineering (ICon-CuTE), pp. 81-86, doi: 10.1109/ICon-CuTE47290.2019.8991470.
[105] Various. Columbia image splicing detection evaluation dataset,(2004). http://www.ee.columbia.edu/ln/dvmm/downloads/AuthSplicedDataSet/AuthSplicedDataSet.htm. Accessed 16 Mar 2021.
[106] Dong J, Wang W, Tan T (2013) Casia image tampering detection evaluation database. In: 2013 IEEE China summit and international conference on signal and information processing, pp 422–426. https://doi.org/10.1109/ChinaSIP.2013.6625374.
[107] Tralic D, Zupancic I, Grgic S, Grgic M (2013) Comofod — new database for copy-move forgery detection. In: Proceedings ELMAR-2013, pp 49–54.
[108] Korus P, Huang J (2016) Evaluation of random field models in multi-modal unsupervised tampering localization. In: 2016 IEEE international workshop on information forensics and security (WIFS), pp 1–6. https://doi.org/10.1109/WIFS.2016.7823898
[109] Christlein V, Riess C, Angelopoulou E (2010) On rotation invariance in copy-move forgery detection. In: 2010 IEEE international workshop on information forensics and security, pp 1–6. https://doi.org/10.1109/WIFS.2010.5711472
[110] Dataset used for Image Manipulation-https://www5.cs.fau.de/research/data/image-manipulation/
[111] Roček, A., Javorník, M., Slavíček, K. et al. Zero Watermarking: Critical Analysis of Its Role in Current Medical Imaging. J Digit Imaging 34, 204–211 (2021). https://doi.org/10.1007/s10278-020-00396-0
[112] Sharma, K., Gupta, A., Sharma, B., & Tripathi, S.L. (Eds.). (2021). Intelligent Communication and Automation Systems (1st ed.). CRC Press. https://doi.org/10.1201/9781003104599
[113] Pathak, J., Tripathi, S.L. (2021). Column shifting algorithm to compute iteration bound of finite impulse response systems having inline delays, International Journal of Embedded Systems 2021 14:5, 443-450
[114] Pathak, J., Tripathi, S.L. (2021). A Novel Model for Resisting Side Channel Attack by Masking of Gates, Journal of Engg. Research, ICMET, https://doi.org/10.36909/jer.ICMET.17165
[115] Pathak J., Tripathi, S.L. (2022). Novel Architecture for Authentication-based Reliable Hardware Security Model. In: Tiwari, S., Trivedi, M.C., Kolhe, M.L., Mishra, K., Singh, B.K. (eds) Advances in Data and Information Sciences. Lecture Notes in Networks and Systems, vol 318. Springer, Singapore. https://doi.org/10.1007/978-981-16-5689-7_64
[116] Jothi N.J, Letitia S (2020) Tampering detection using hybrid local and global features in wavelet-transformed space with digital images. Soft. Comput. 24 (7), 5427–5443. https://doi.org/10.1007/s00500-019-04298-4.
[117] Liu Y, Wang H, Chen Y, Hanzhou W, Wang H (2020) A passive forensic scheme for copy-move forgery based on superpixel segmentation and K-means clustering. Multimed. Tools Appl. 79 (1–2), 477–500. https://doi.org/10.1007/ s11042-019-08044-8.
[118] Ahmed B, Gulliver T.A, Zahir S.A (2020) Image splicing detection using mask-RCNN, Signal, Image Video Process., vol. 14, no. 5, pp. 1035–1042, Jul. 2020.
[119] Zhou G., Tian X, Zhou A (2022) Image copy-move forgery passive detection based on improved PCNN and self-selected sub-images. Front. Comput. Sci. 16, 164705 (2022). https://doi.org/10.1007/s11704-021-0450-5.
[120] Rao A.V, Rao C.S, Cheruku D.R (2022). An enhanced copy-move forgery detection using machine learning based hybrid optimization model. Multimedia Tools and Applications. 81. 1-21. 10.1007/s11042-022-11977-2.
[121] Wang XY., Wang Xq., Niu Pp. (2023) Accurate and robust image copy-move forgery detection using adaptive keypoints and FQGPCET-GLCM feature. Multimedia Tools and Applications (2023). https://doi.org/10.1007/s11042-023-15499-3.
[122] Alkawaz M.H, Sulong G, Saba T, Rehman A (2018) Detection of copy-move image forgery based on discrete cosine transform, Neural Computing and Application, vol. 30,pp. 183–192.
[123] Hayat K, Qazi T (2017) Forgery detection in digital images via discrete wavelet and discrete cosine transforms, Computers & Electrical Engineering, vol. 62, pp. 448-458
[124] Tripathi A, Misra A, Kumar K (2023) Optimized Machine Learning for Classifying Colorectal Tissues. S N Computer Science, 4, 461. https://doi.org/10.1007/s42979-023-01882-2
[125] Tripathi E, Kumar U, Tripathi S (2022). Image splicing detection system using intensity-level multi-fractal dimension feature engineering and twin support vector machine based classifier. Multimedia Tools and Applications. 1-19. 10.1007/s11042-022-13519-2.