Multimedia Systems (2022) 28:939–992
https://doi.org/10.1007/s00530-021-00873-8

REGULAR PAPER

A comprehensive survey of image and video forgery techniques: variants, challenges, and future directions

Syed Tufael Nabi[1] · Munish Kumar[2] · Paramjeet Singh[1] · Naveen Aggarwal[3] · Krishan Kumar[3]

Received: 17 July 2021 / Accepted: 10 November 2021 / Published online: 30 January 2022

Abstract

With the advent of Internet, images and videos are the most vulnerable media that can be exploited by criminals to manipulate for hiding the evidence of the crime. This is now easier with the advent of powerful and easily available manipulation tools over the Internet and thus poses a huge threat to the authenticity of images and videos. There is no guarantee that the evidences in the form of images and videos are from an authentic source and also without manipulation and hence cannot be considered as strong evidence in the court of law. Also, it is difficult to detect such forgeries with the conventional forgery detection tools. Although many researchers have proposed advance forensic tools, to detect forgeries done using various manipulation tools, there has always been a race between researchers to develop more efficient forgery detection tools and the forgers to come up with more powerful manipulation techniques. Thus, it is a challenging task for researchers to develop h a generic tool to detect different types of forgeries efficiently. This paper provides the detailed, comprehensive and systematic survey of current trends in the field of image and video forensics, the applications of image/video forensics and the existing datasets. With an in-depth literature review and comparative study, the survey also provides the future directions for researchers, pointing out the challenges in the field of image and video forensics, which are the focus of attention in the future, thus providing ideas for researchers to conduct future research.

Keywords Image forgery · Video forgery · Forensic science · Features · Classifications techniques

1 Introduction to image/video forensics and its importance

Compared to text, visual media has proved to be an efficient way of communication. Visual media includes images and videos which provide information very effectively. Various devices are used to capture this type of information. This information is regarded as certification to truthfulness. Also, CCTV footage is presented in a court of law as exploratory evidence. There are so many other fields that need visual material as key information. This increases the need for authenticity and integrity of images. In this era of the digital world, it is almost in every field that we require the authenticity and integrity of images and videos. But there are various easily available tools that can be used to manipulate these images and videos. This poses threat to their authenticity and integrity. It can, therefore, be concluded that "seeing is no longer believing" [1–3]. For example, the forgers can take advantage of image manipulation tools to hide the crime evidences, or to impersonate s to defame well-known and reputed persons, an organization or some political party. Thus, it is more important to have a robust and highly efficient tool that can cope up with this problem. Although there is easy availability of powerful manipulation tools, researchers have proposed many techniques to detect these forgeries accurately and efficiently and thus contribute to society in crime and corruption control.

Communicated by Y. Zhang.

✉ Munish Kumar
munishcse@gmail.com

[1] Department of Computer Science and Engineering, GZS Campus College of Engineering and Technology, Maharaja Ranjit Singh Punjab Technical University, Bathinda, Punjab, India

[2] Department of Computational Sciences, Maharaja Ranjit Singh Punjab Technical University, Bathinda, Punjab, India

[3] University Institute of Engineering and Technology, Panjab University, Chandigarh, India

1.1 Novelty of this article

This survey presents a systematic and detailed study in the field of image and video forensics. It was found that many of the researchers have come up with survey articles in this field. However, they have carried out their survey either in image forensics or video forensics and not covering all the topics. And there are very few survey papers that have presented both the domains under one roof. Still there exist no such survey paper that has carried out the survey in all the related categories of both image and video forensics. Thus, we have come up with the latest combined systematic survey on both image and video forensics with the detailed literature review along with the simplified comparative study that can prove to be the backbone of all the future research in these fields. At the end of this survey article, some common challenges are also discussed based on the comprehensive survey carried out in these fields. From these challenges, the future directions can be proposed. The main goal of carrying out this survey has been to provide extensive information about the related research work carried out in these fields. In order to make this possible, the survey was carried out in a systematic manner to analyze and investigate different digital image and video forensic techniques. This paper also provides the quality evaluation that was carried out to ensure that the papers selected for carrying out the survey are of high quality. After quality evaluation, the selected papers were surveyed to answer the formulated research questions. The important points to notice about this survey are as follows:

1. This survey uses the quality assessment approach for identifying the quality papers for study in the concerned fields.
2. This survey provides a systematic and well-organized review with each topic being extensively surveyed.
3. This survey provides an extensive review of image and video forgery detection methods.
4. This survey also suggests the researchers the future research directions by providing the research gaps and challenges of existing studies.
5. This survey aims at providing the review of both image and video forensics under one roof.

This survey is carried out in an organized way and is divided into six main sectionsAs follows: Sect. 1 is an introductory section with first sub-section discussing about the novelty of this article; the second sub-section is about design constraints for this survey with five sub-sub-sections discussing about background, inclusion and exclusion criteria, quality evaluation, research questions and motivation for the readers; the third subsection discusses general structure for image forgery detection; the fourth subsection discusses about general structure for video forgery detection, and the fifth subsection discusses the applications of forensic techniques, and the final subsection summarizes the existing datasets for image and video forensics. In Sect. 2 the literature review of various categories of image forensic approaches are discussed, and in Sect. 3, the literature review of various categories of video forensic approaches have been discussed. In Sect. 4 the various deep learning approaches to image and video forensics are discussed. In Sect. 5 the future directions are discussed and finally in Sect. 6 the conclusions drawn from the survey have been discussed. Figure 1 shows the pictorial representation of various sections of this survey article.

1.2 Design constraints for this survey

In this section, we have discussed the design constraints for this survey. The survey was conducted stepwise which includes survey protocol development, carrying out the survey, experimental results analysis, results reporting, and research finding discussion.

1.2.1 Background

Digital forensic techniques provide a way to authenticate images or videos and check whether they are forged or not. It has been a long way back that this field has come into existence. Since then, it has been a common practice and has been practiced worldwide due to the advent of very powerful and freely available forgery tools like Adobe Photoshop, etc. However, in parallel, researchers are in a queue to develop the powerful forgery detection techniques, also called as forensic techniques. The image forensic techniques are of either active or passive type, whereas the video forensic techniques are of either inter-frame or intra-frame types. The active methods use the information that is hidden in an image at the time of their acquisition or before being publicly published. This hidden information is then used to detect the source and hence forgery. The active forensic methods make the use of watermarking, Digital signatures, and steganography for image authenticity confirmation. Passive-forensic-techniques do.not use acquisition time information for a forensic purpose that is inserted into the image. They use the traces that are left during the image processing steps which may include image acquisition phases or during their storage phase. The passive techniques have been further categorized into tempering operation-based and source identification-based. Tempering operation-based techniques are either of the type-dependent or of the type-independent technique. Each technique has been discussed

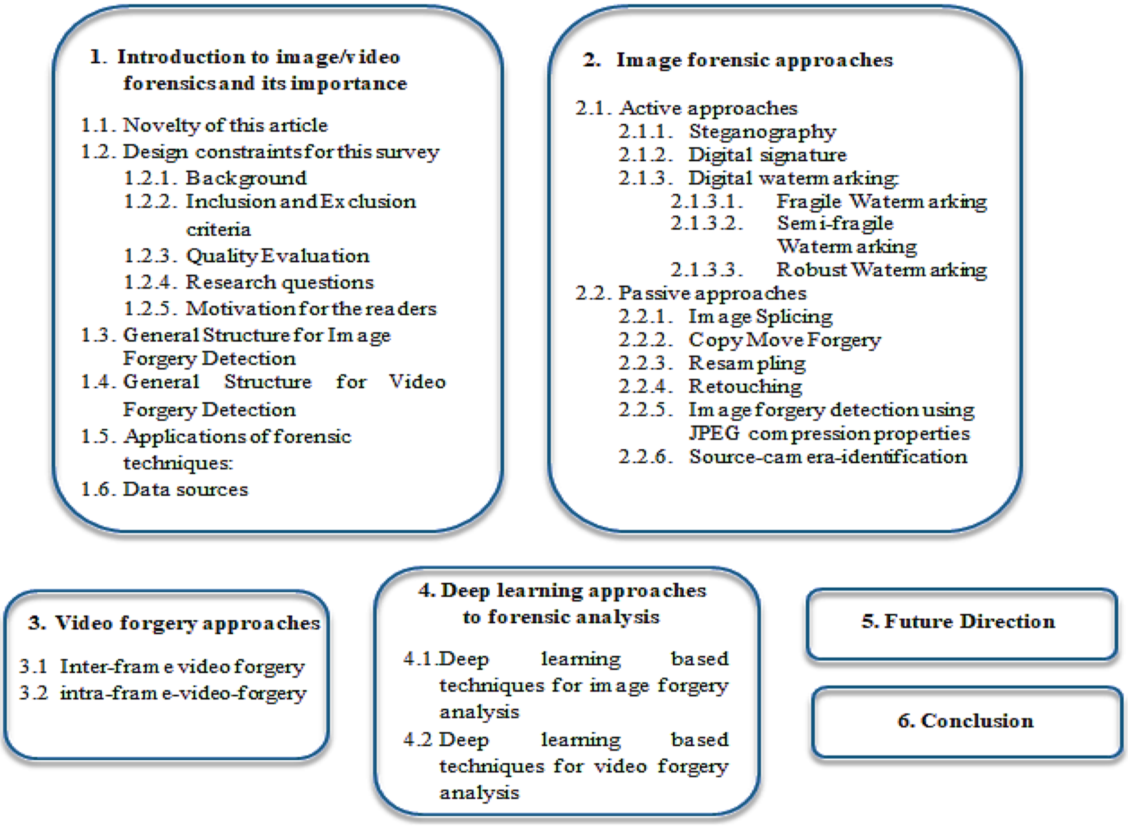

1. Introduction to image/video forensics and its importance
1.1. Novelty of this article
1.2. Design constraints for this survey
1.2.1. Background
1.2.2. Inclusion and Exclusion criteria
1.2.3. Quality Evaluation
1.2.4. Research questions
1.2.5. Motivation for the readers
1.3. General Structure for Image Forgery Detection
1.4. General Structure for Video Forgery Detection
1.5. Applications of forensic techniques:
1.6. Data sources
2. Image forensic approaches
2.1. Active approaches
2.1.1. Steganography
2.1.2. Digital signature
2.1.3. Digital watermarking:
2.1.3.1. Fragile Watermarking
2.1.3.2. Semi-fragile Watermarking
2.1.3.3. Robust Watermarking
2.2. Passive approaches
2.2.1. Image Splicing
2.2.2. Copy Move Forgery
2.2.3. Resampling
2.2.4. Retouching
2.2.5. Image forgery detection using JPEG compression properties
2.2.6. Source-camera-identification
3. Video forgery approaches
3.1 Inter-frame video forgery
3.2 intra-frame-video-forgery
4. Deep learning approaches to forensic analysis
4.1 Deep learning based techniques for image forgery analysis
4.2 Deep learning based techniques for video forgery analysis
5. Future Direction
6. Conclusion

Fig. 1 Various sections of this survey article

in the upcoming sections with a detailed literature review and comparative study.

1.2.2 Inclusion and exclusion criteria

The set of rules that determine the research boundaries has been adopted in order to conclude a systematic review on two forensic types of images and video. Moreover, research manuscripts published in top journals like SCI and E-SCI, the research work carried out by proficient scientists, and also those published in top conferences have been included in the survey, whereas the irrelevant manuscripts that were not concerned with the field of our interest have been excluded. This standard has been set only after defining the research question. The main aim of this survey was the qualitative and quantitative research that includes the latest research studies and the other much older research has been excluded.

1.2.3 Quality evaluation

After the inclusion and exclusion criteria were set, the appropriate high-quality papers were selected to carry out the survey. The research topic under consideration is a vast area having many sub-areas with a large high-quality research paper available so far. Thus it was a must to have some rules for the selection of quality papers to carry out this study and according to these rules our survey must have included:

1. High-quality research papers.
2. Research carried out on high-quality dataset
3. High-quality survey articles.
4. Most cited research papers.
5. Must have included sufficient data for analysis.

1.2.4 Research questions

This survey has been carried out to find and categorize various existing literature on forensic approaches in images and videos so as to provide the researchers of these fields with handy information about the work carried out in this

Table 1 Research questions

S. No	Research question	Remarks
1.	What is the present status of topic under study?	This helps to understand techniques associated with the related problem
2.	What are various categories of digital forensic techniques?	Reporting of various techniques that have been used in digital forensics
3.	Which techniques have been used for feature extraction and what type of scripts do they took into consideration?	Different types of techniques/tools that have been developed for digital forensics till date are mentioned along with their application
4.	Which studies have used which tool and what results have they achieved?	The research question explores the studies which evaluated/compared different word recognition techniques. The number of studies for each type of script is also reported
5.	What are the main areas associated with image and video forensics and the number of studies carried out in each area along with their findings?	It is important to understand the number of studies for each sub-area which helps in identifying key areas for future research
6.	What is the size of the database used in forensic techniques?	It is necessary create the database on which the research on digital forensics can be processed
7.	Which type of system is this, Is it open source or commercial?	It helps in creating benchmark and standardizes the comparative analysis studies

field. To carry out this survey, a set of research questions were kept into account and these have been tabulated in the Table 1 given below.

1.2.5 Motivation for the readers

The word forgery means manipulation or modification of contents for fraudulent purposes or to deceive some proof. Forgeries may be done to either images or videos and hence the name image forgery and video forgery, respectively. Forgery has been a custom since old ages and thus is not new to this world. In earlier times, the two or more images were combined using the photomontage process. In this process, the images are overlapped, glued or pasted, or sometimes reordered so as to obtain a single photocopy. But with time, many researchers and developers have come up with forgery tools that are more powerful and easily available over the internet. Thus, it has now become a common custom to manipulate images and videos using these tools. Researchers are racing to develop such a tool that can efficiently and accurately detect forgery. Many researchers have developed many tools for forgery detection, but lack high efficiency and high accuracy. This survey aims at helping the researchers to provide them with the handful of information of research carried in this field so far.

1.3 General structure for image forgery detection

The process of image forgery detection requires a systematic approach in a step-by-step manner as shown in Fig. 2 below.

Step 1: Acquisition The noise is introduced during the acquisition of images or videos due to irregularities in the camera imaging sensors and optical lenses [4]. Color Filter Array (CFA) is used to filter this noise [5]. After that, some

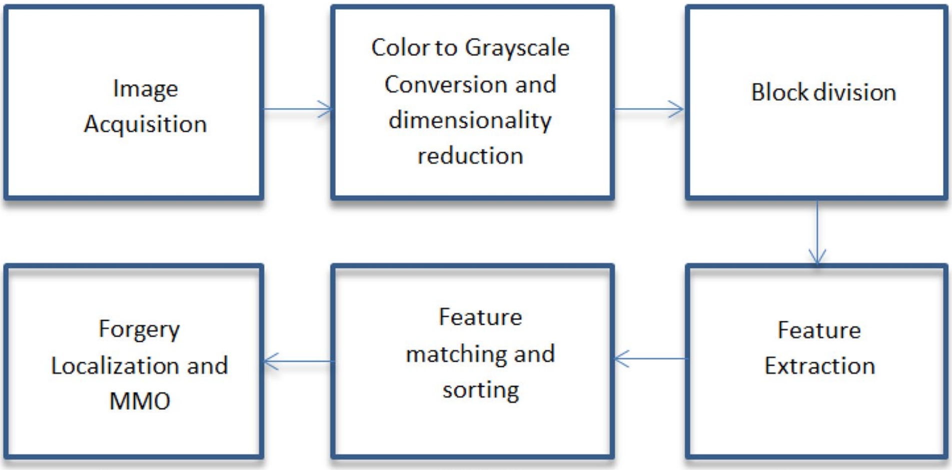


Image Acquisition
Color to Grayscale Conversion and dimensionality reduction
Block division
Feature Extraction
Feature matching and sorting
Forgery Localization and MMO

Fig. 2 Block diagram of image forgery detection process

Image enhancement process is done before actually storing it in the memory, which results in the addition of more noise. Nowadays we have high-quality acquisition devices which result in lesser noise. Some recent image de-noising techniques include [6–12].

Step 2: Color to grayscale conversion and dimensionality reduction This process is used to reduce the computational complexity [13].

Step 3: Block division In this step, the resultant image from step 2 is divided into blocks that may be either overlapping or non-overlapping [14]. The nature of block division depends on the constraints like complexity and accuracy.

Step 4: Feature extraction This process includes the extraction of features, also called as descriptors, from the image which may be local or global [15, 16]. Local descriptors denote the texture in blobs, color, patches, corners, and other parameters which are mainly used for image identification and image recognition. Global descriptors denote counter, the shape of the image and are used for object classification and identification in an image and also used from image retrieval.

There are many existing algorithms used for feature extraction so far. Among the existing techniques of feature extraction, we apply the most the most important and efficient algorithms like Mirror-reflection Invariant Feature Transformation (MIFT) [17], Scale Invariant Feature Transformation (SIFT) [18], Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) [19], Affine SIFT [20], Speeded up Robust Features (SURF) [21], and Singular Value Decomposition (SVD) [22]. Deep learning has also been a prominent technique for feature extraction. There also exist various deep learning based techniques [23–30] for image retrieval.

Step 5: Feature Sorting and matching After feature extraction is done, the resultant feature matrices are sorted so as to bring the identical ones closer to each other using sorting algorithms like KD-Tree sorting, Radix sorting, best bin (BFS) first Sorting, etc. These sorted feature blocks are then matched with every other block using various algorithms [15, 31, 32]. This is achieved by calculating certain parameters which include Euclidean distance, hamming distance, K-nearest neighbor (KNN), shift vectors, pattern entropy, probabilistic matching, clustering, etc.

Step 6: Forgery localization and MMO: After matching, a similarity score obtained is used to locate the forged region. To improve the localization, various mathematical morphological operations are performed.

1.4 General structure for video forgery detection

The video forgery detection also requires a step-by-step process in a systematic approach as shown in Fig. 3 below.

Video is the collection of images also called as frames that vary with time [33, 34]. Thus the process of forgery detection starts from frame extraction from the video and saves them in any image format like jpeg, etc. After the frame extraction, the process for forgery detection remains the same as image forgery detection. For a colored image, the conversion to greyscale is done. After that, the dimensionality reduction algorithm is applied to each image for the purpose of reducing the computational complexity. The resultant images obtained are then divided into blocks. These blocks may be either overlapping or may be non-overlapping blocks. Afterward, the feature extraction is done so as to extract the feature matrices of an image. These feature matrices are then sorted and the sorted feature matrices are then matched with every other feature matrix to obtain the similarity score, which is then used to locate the actual forged region. Once the forged region is located, the last step is attacking for robustness test, in which some attacks are added explicitly to check the optimization and efficiency of the video forgery detection algorithm. These attacks create the forged part in a video which is very tough to detect.

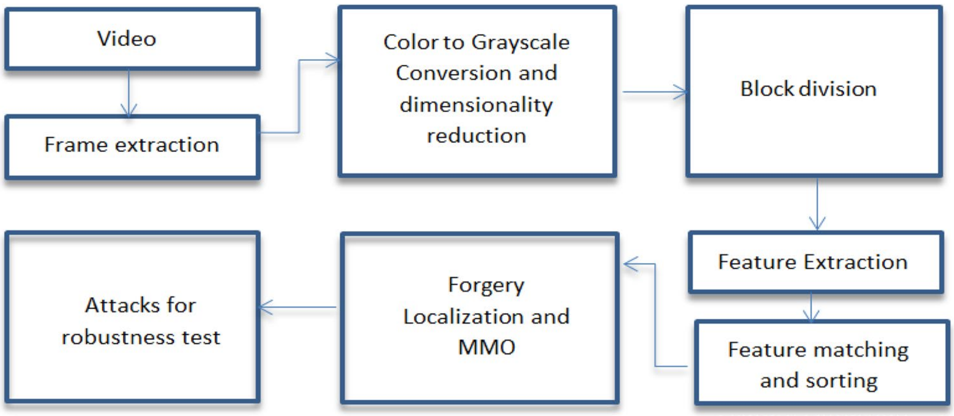

Video
Frame extraction
Color to Grayscale Conversion and dimensionality reduction
Block division
Feature Extraction
Feature matching and sorting
Forgery Localization and MMO
Attacks for robustness test

Fig. 3 Block diagram of video forgery detection process

1.5 Applications of forensic techniques

The crime investigating agencies use the forgery detection techniques to get the clue about criminal behind the scene. Without these techniques it would have not been possible to serve the justice to the innocent people who never had done that crime. The major applications of forgery detection techniques are as follows:

I. *Crime detection* The modification of digital evidences like videos, images by using various tools in order to hide or eliminate the evidence of crime is considered to be the serious crime in the court of law.

a. These crimes include the following:
b. The creation of fake digital documents for defaming any community, industry, any political party or any person.
c. Alteration of property documents in order to impersonate as an owner of that property.
d. Alteration of academic records to falsely make oneself eligible for the job post, promotion to higher post or for achieving admission in some prestigious college without actually being eligible.
e. Alteration of CCTV surveillance images or videos in order to hide or even destroy the evidence of crime.
f. Alteration of medical records to hide the cause of death.
g. Alteration of DNA reports to hide the identity of dead body for political or personal reasons.
h. Alteration of social media videos or images to defame someone, some industry or some political party. The other reason may be to hide the actual source of crime.
i. These crimes can prove to be varying hazardous/dangerous to the society. But using the digital forensic techniques, these crimes can be detected well on time and the culprit may be sent behind the bars.

II. *Crime prevention* If the forgery and the culprit are detected well in time and the actual criminal gets punished, it can thwart other criminals to do this crime in future and can thus help in prevention of crime. Also the consequences of the crime can be stopped if the forensic analysis is done properly and well on time.

III. *Authentication* The authentication of digital document is done through digital signatures, watermarks and steganography techniques. If the documents are compromised in any form then the forensic techniques can detect them and hence can find that if they are from authentic source or not.

1.6 Data sources

The datasets available for image forgery detection techniques have been summarized in the Table 2 given below.

The datasets available for video forgery detection have been tabulated in the Table 3 given below.

2 Image forensic approaches

There are two main categories of image forgery techniques, namely active and passive [65]. Active approaches include Steganography, Digital Signatures, and Watermarking. The passive digital image forgery methods are categorized into two main categories viz. tempering operation based and source camera identification based. Further, the tempering operation-based techniques are categorized into tempering operation-dependent and tempering operation independently. The dependent techniques include image slicing or image composites and copy-move methods. On the other hand, the independent ones include resampling, retouching, sharpening and blurring, brightness and contrast, image filtering, compression, image processing operations, image cropping and interpolation, and geometric transformations. The source camera identification-based methods include lens aberration, color filter array interpolation, sensor irregularities, and image feature-based techniques. Figure 4 shows the classification graphically. Some of the survey papers related to image forensics are tabularized in Table 4 given below.

2.1 Active approaches

Active forensic approaches rely on trustworthy image acquisition sources like cameras for forensic purposes [74, 75]. At the time of image acquisition, the digital signature [76, 77] and digital watermarking [78–80] are computed from the image, which can later be used for modification detection by simply verifying their values. The limitation of active approaches is that the authentication of images takes place at the very moment of their acquisition before actually storing in the memory card, making the use of specially designed digital signature and watermarking chips in the cameras. This limits their applications to very few situations. In contrast to these active approaches, passive approaches do not require prior information of image acquisition. Each of the active techniques has been explained below with the related work.

2.2 Steganography

Steganography refers to the hiding of information in the carrier using the key known as the steganography key. The sender hides the secret information in image pixels using a stego-key which is later read by the receiver using the shared key. Figure 5 shows an example of steganography.

There are two types of techniques, based on domains in which they work; these may be either spatial or frequency

Table 2 Dataset available for image forgery detection

References	Dataset (Year)	Number of images in a dataset	Size of image	Description
[35]	Columbia gray (2004)	Nine hundred thirty-three (933) (Original) Nine hundred Twelve (912) (Modified)	128 × 128 pixels	This dataset includes 1. Splicing 2. BMP format gray images
[36]	Columbia color (2006)	One hundred eighty-three (183) (Original) One hundred eighty (180) (Modified)	757 × 568–1152 × 768 pixels	This dataset includes 1. Splicing 2. TIFF format color images
[37]	INRIA-Copy days (2008)	Sixteen hundred forty-two (1642) images	Multiple variations	This dataset includes 1. Cropped images 2. Scaling 3. JPEG compression 4. Combined strong attacks
[38]	Dresden (2010)	Twenty-five thousand one hundred thirty-seven (25,130) images	Multiple variations	This dataset includes 1. Images that have been taken from multiple cameras of various model 2. Images of multiple file format and different visual quality
[39]	MICC-F220 (2011)	One hundred ten (110) (original) One hundred ten (110) (modified)	722 × 480–800 × 600 pixels	This dataset includes 1. Colored images 2. Copy Move forged images 3. JPEG formatted images 4. Images with no mask 5. Lacks post processing
[39]	MICC-F2000 (2011)	Thirteen hundred (1300) (original) Seven hundred (700) (Modified)	2048 × 1536 pixels	This dataset includes 1. Colored images 2. Copy Move forged images 3. JPEG formatted images
[40]	BOSSBases v0.93 (2011)	Nine thousand seventy-four (9074) images	512 × 512 pixels	This dataset includes 1. Greyscale images 2. Image are of the format PGM and taken from multiple camera-models and appropriate raw EIF
[41]	Bianchi (2012)	One Hundred (100) images	1024 × 1024 pixels	This dataset includes 1. JPEG and TIFF formatted
[42]	CMEN (2012)	Three hundred thirty-six (336) images	800 × 533–3872 × 2592 pixels	This dataset includes 1. Forty-eight copy moved images 2. One hundred forty-four rotated images 3. One hundred forty-four resized images
[43]	Copy-Move-Forgery-Detection (CoMoFoD) (2013)	Five thousand two hundred (5200) images	512 × 512	This dataset includes 1. Colored PNG and JPEG formatted images 2. Copy Move forged images
[44]	CASIAv1.0 (2013)	Eight hundred (800) (original) Nine hundred twenty-one (921) (Modified)	374 × 256 pixels	This dataset includes 1. JPEG formatted and spliced (at preprocessing) images
[44]	CASIAv2.0 (2013)	Seven thousand two hundred (7200) (original) Five thousand twenty-three (modified)	320 × 240–800 × 600 pixels	This dataset includes 1. JPEG, TIFF and BMP formatted and spliced (at post-processing) images

Table 2 (continued)

References	Dataset (Year)	Number of images in a dataset	Size of image	Description
[45]	MICC-F600 (2013)	One hundred and sixty (160) images	800×533–3888×2592 pixels	This dataset contains Colored PNG and JPEG formatted images 1. Copy Move forged images
[46]	Copy-Move-Forgery-Detection-database (CMFDdb) grip (2014)	Three thousand four hundred forty (1440) images	Multiple variations	This dataset includes 1. Rotation 2. Scaling 3. JPEG compression
[47]	Computer Vision and Image Processing (CVIP) (2015)	One thousand and one hundred sixty (1160) images	1000×700 700×1000 pixels	This dataset includes 1. Translation 2. Copy-move 3. rotation 4. Scaling
[48]	RAISE (2015)	Eight thousand one hundred fifty-six (8156) images	Multiple variations	This dataset includes 1. High luminance images 2. Uncompressed images 3. Camera native images
[49]	Wattanachote (2015)	Not mentioned clearly	Multiple variations	This dataset includes Seam-carved and seam-inserted images at various quality factors
[50]	Copy Move Hard (CMH) (2015)	One hundred and eight (108) images	845×634–1296×972 pixels	This dataset includes 1. Twenty-three copy moved images 2. Twenty-five rotated images 3. Twenty-five resized images 4. Thirty-five both rotated and resized images
[51]	WildWEB (2015)	Ten thousand six hundred forty-six (10,646) images	Multiple variations	This dataset includes 1. Cut paste forged images 2. Copy moves forged images 3. Erase fill forged images
[52]	COVERAGE (2016)	One Hundred (100) (original) One Hundred (100) (modified)	400×486 pixels	This dataset contains 1. Copy moved images along with interpretations
[53]	Nimble challenge (NC) (2016)	Ten thousand (10,000) images	Multiple variations	This dataset contains: 1. The Splice detection and also localization 2. The Provenance modification
[54]	Realistic tempered dataset 2.0 (RTD 2.0) (2017)	Two hundred twenty (220) handmade modifications	1920×1080 pixels	This dataset contains 1. Modifications such as object addition and deletion 2. PRNU signatures 3. TIFF and PNG Formatted images 4. Ground Truth Maps of 3-level
[55]	Media Forensic Challenge (MFC) (2018)	Over one lakh (100,000) images	Multiple variations	This dataset includes five evaluation tasks 1. Detects-Splice-forgery and-also-localization 2. Investigates-processing-events 3. Detects-source-modification 4. Creates-e- source-graph And two challenges 1. Camera-verification 2. Detects-modifications based-on-Generative-Adversarial-Network (GAN)

Table 2 (continued)

References	Dataset (Year)	Number of images in a dataset	Size of image	Description
[56]	IMD (2020)	Seventy-thousand (70,000) images {35,000-original and 35,000-forged)	480×480 pixels	This dataset contains 1. Multiple-forged-and-advanced-GAN-and-in painting-forged-images 2. Images-from-2322-camera-models

domain. Some of the spatial domain techniques include Least Significant Bit (LSB) [81], Pixel Mapping Method (PMM) [82], Random Pixel Selection (RPS) [83], Histogram based [84], and Grey Level Modification (GLM) [85]. LSB techniques use LSBs of image pixels to replace them with some secret information and this technique was able to reduce the system payload by 62.5%. PMM uses some mathematical function to map some image pixels with secret information bits. Similarly, RPS replaces randomly selected bits with the secret information to be hidden. Histogram-based technique hides the secret information in the image histogram and-GLM-technique-hides the information by simply modifying the image grey level. The frequency domain-based techniques are based on Discrete-Wavelet-Transform (DWT) [86], Discrete-Cosine-Transform (DCT) [87], Discrete-Fourier-Transform (DFT) [88], Discrete-Curve-Transform (DCVT) [89] and integer-wavelet- transform- (IWT) [90]. In these methods, the pixels are selected using corresponding transform functions. These pixels are then replaced by the secret information bits. Table 5 given below provides a brief description of various steganography techniques.

2.2.1 Digital signature

The digital signature provides a way to authenticate the document source. It uses the concept of two keys viz. private-and-public. Private-Key is known-to-its-owner whereas public-key-is-known to all. In a digital signature, the hash value is calculated using some hash function and then the hash value is encrypted using the sender's private key. This becomes the digitally signed document. At the receiver side, this document is first decrypted using the public key and then the hash value of this decrypted document is calculated using the same hash function and afterward, these hash values are compared.

If the hash values do not match, then it indicates that the document is modified in between source and destination and if matched, the document is verified to be authentic. The whole process of digital signature is shown in Fig. 6. The digital signature ensures that the content is authentic, reliable, and from an authentic source [91, 92]. There exist various other techniques which use digital signature concept. One of the techniques [93] uses digital-signature for improving Genetic-algorithm (GA) and Particle-swarm-optimization (PSO)-based-watermarking system. Another technique [94] used a digital-signature formed by combining Rivest–Shamir–Adleman (RSA), Vigenere–Cipher and Message-Digest-5 (MD-5), which proved to be robust against different image-forgery-attacks. Another technique [95] developed an improved-digital-signature-technique for improved data-integrity and authentication of biomedical-images in cloud. One more technique [96] was used to keep digital-signature-image-information invisible in cover-image for message-authenticity, integrity and non-repudiation. Another technique [97] combined digital-signature with LBP-LSB-Steganography-Techniques in order to enhance security of medical-images.

2.2.2 Digital watermarking

Digital watermarking involves the insertion of a certain code called as digest into the image right at its acquisition time. This is later used for an image authentication process which includes comparing extracted digest with the original digest [98–100]. If this extracted digest and original digest do not match then it means that some modification has happened to the image. Figure 7 shows a brief process of watermark embedding and its extraction. Watermark embedding is done by embedding algorithm which uses embedding key to embed watermark and the watermark extraction algorithm does the reverse process.

For example, in a technique [101] proposed recently, the division of an image into blocks is done based on similarity measurement. Then after blocking, some statistical measures are computed like mean, mode, median, and range of pixel values followed by encryption which encrypted values are then embedded in the image. This encrypted information is later used for forgery detection. Although the watermarking technique is very vigorous, still there are some limitations also. One of these limitations is that not all the devices come up with an inbuilt watermarking mechanism and some of the devices come up with the very expensive embedded watermarking features. The other drawback is that if some modifications are done for image enhancement, the watermarking mechanism is unable to recognize this legitimate

Table 3 Dataset available for video forgery detection

References	Dataset (Year)	Video source	Camera type	Description
[57]	Surrey University Library for Forensic Analysis (SULFA) (2012)	Canon SX220 Nikon S3000 Fujifilm S2800HD	Static	This dataset includes 1. Copy-Move forged videos 2. 150 videos 3. MOV & AVI (codec H.264 MJPEG) formatted videos 4. Video speed = 30 FPS 5. Video resolution 320 × 240
[58]	REWIND (2013)	SULFA	static	This dataset includes 1. Copy-Move forged videos 2. 10 videos 3. MOV and AVI (codec H.264, MJPEG) formatted 4. 30 FPS speed 5. Video resolution = 320 × 240
[47]	Hybrid dataset (2015)	SULFA&CANTATA	Static and Dynamic	This dataset includes 1. Copy-Move 2. 160 videos 3. AVI and MP4 formatted 4. 20–30 FPS speed 5. Video resolution = 960 × 540 640 × 360 320 × 240
[59]	Video Tempering Detection (VTD) (2016)	Internet	Static and Dynamic	This dataset includes 1. Splicing forgery, Copy-Move forgery and swapping-fames forged videos 2. 33 videos 3. AVI formatted 4. 30 FPS speed 5. Video resolution = 1280 × 720
[60]	SYSU-OBJFORG (2016)	Commercial Surveillance Cameras	Static	This dataset includes 1. Object based forgery (Adding or removing the moving object) 2. 110 videos 3. H.264/MPEG-4 encoded videos 4. Video speed = 25 FPS 5. Video resolution = 1280 × 720
[61]	GRIP dataset (2017)	YouTube & Internet	Static	This dataset includes 1. Splicing forged videos 2. 10 videos 3. AVI (codec H.264) formatted 4. 30 FPS speed 5. Video resolution = 720 × 1280
[62]	Test Database (2018)	SULFA & Different movie scene	Static and Dynamic	This dataset includes 1. Frame Duplication forged videos 2. 31 videos 3. MPEG-4 formatted 4. Video resolution = variable
[63]	GRIP dataset (2018)	Internet	Static	This dataset includes 1. Copy-Move (Additive & occlusive) forged videos 2. 15 videos 3. AVI formatted 4. 30 FPS speed 5. Video resolution = variable

Table 3 (continued)

References	Dataset (Year)	Video source	Camera type	Description
[64]	Temporal Domain Tampered Video Dataset (TDTVD) (2020)	Sixteen videos of SULFA (original) Twenty-four videos of VTD (Original)	Static and Dynamic	This dataset includes: 1. All-temporal-domain-tempering-videos 2. One hundred twenty (120) videos with Event-or-object-or-person (EOP) removal tempering. Ninety (90) videos with Multiple-tempering (Within a Single-Video) including ten (10)-frames-modified at three-different-locations, Thirty-frames-tempered-at-three-different-locations and 20-frames-modified at-3-different-locations-in-a-video 3. Video-length = 6–18 s 4. Video resolution = 320 × 240/640 × 360

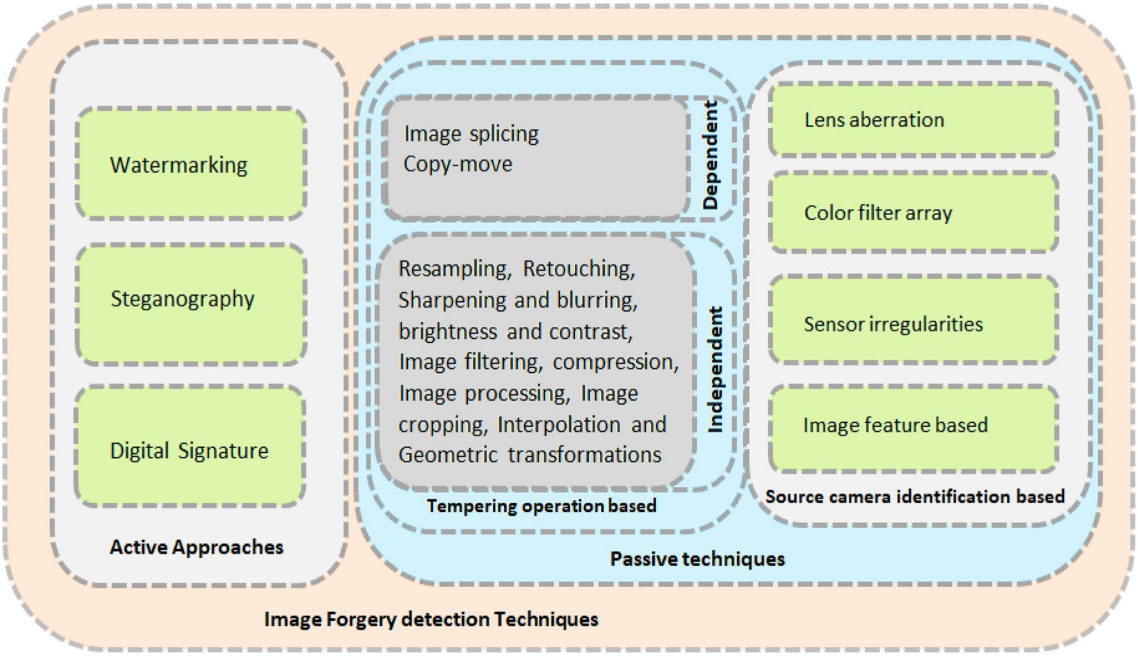

Watermarking
Steganography
Digital Signature
Active Approaches
Image splicing
Copy-move
Dependent
Resampling, Retouching, Sharpening and blurring, brightness and contrast, Image filtering, compression, Image processing, Image cropping, Interpolation and Geometric transformations
Independent
Tempering operation based
Lens aberration
Color filter array
Sensor irregularities
Image feature based
Source camera identification based
Passive techniques
Image Forgery detection Techniques

Fig. 4 Classification of image forgery detection techniques

modification. One another limitation is that there remains a requirement of an embedded system that can embed digest in an image. The watermark approaches may be Spatial-or-frequency domain. The spatial domain works on Least Significant Bit (LSB) [102, 103], Random Insertion in File (RIF) [104], and Spread Spectrum (SS) [105]. The technique [102] chains LSB and an inverse bit to determine the region to insert the watermark. Frequency domain techniques include discreet-fourier-transform (DFT) [106, 107], discrete-cosine-transform (DCT) [107, 108], singular-value-decomposition (SVD) [109, 110] and discrete-wavelet-transform (DWT) [111] depending upon the transform function used to determine the region in the image for embedding watermark. These techniques along with their brief description are tabulated in the Table 6 given below.

2.2.2.1 Fragile watermarking These types of watermarks are used for the detection of tampering as they are highly sensitive to any sort of tampering. This makes it intolerable to any change even to only one bit. This type of watermarking is used for complete authentication purpose and any sort of watermark exposure designates the intentional

Table 4 Survey papers available for image forensics

Reference	Contribution	Research gap
[66]	Reviewed-various-passive image-forensic-methods	For minor areas to be copy-moved, the existing forensic techniques do not perform better and need to be addressed for increasing their performance Also, these techniques prove to be complex computationally and result in high FPR
[67]	Survey on various-forensic approaches-to image forgery	Lack-of-advanced forensic tools currently that would have been able to-detect high-level forgery
[68]	Reviewed different blind forgery detection techniques	Techniques based on DCT and PCA have low accuracy and high computational complexity and when taking into account small forged and highly textured regions, DCT-based techniques prove not to be effective which can be addressed in the future
[69]	Survey on pixel-based-forensic-methods	Some techniques have less accuracy and some have high time complexity
[70]	Survey on digital camera image forensics techniques	Compared to other forgery detection techniques, Camera identification techniques perform better Compared to techniques based on camera software parts like scene content such as lighting and image statistics, techniques-based-on intrinsic features of camera hardware like an aberration and CRF show better accuracy and are more reliable
[71]	Surveyed-Blind-forensic techniques	Some of the techniques result in high FPR and thus require developing more robust and reliable techniques Existing techniques require more human involvement and thus require automation in the future
[72]	Reviewed block-based and key point based CMFD techniques	Techniques like PCA, SVD and DWT have been suggested for dimensionality reduction to increase the performance SIFT and SURF prove to be more reliable techniques in the case of geometrical transformation Real-world big-data problems cannot be solved using existing techniques and hence need to be addressed
[73]	Survey on copy-move-approaches of-image-forensics	Compared to the forensic tools that are-block-based, the time-complexity of key-point based is less and hence more performance but in terms of accuracy block based techniques perform better

or unintentional modifications to the image [114–127]. There exist various fragile watermarking techniques. Among these techniques, the robust and invisible technique [128] uses Spread Spectrum, Quantization DWT, and HVM. Another color image watermarking technique [129] used Hierarchical and BFW-SR¬ approaches. A reconstruction rate of 80% has been achieved. Another technique proposed [130] is based on Logistic map-based chaotic cryptography and histogram. The results obtained show that this Watermarking technique is secure and also a feasible technique for outsourced data. One another technique proposed related to fragile watermark [131] is based on LWT, DWT, and Amold-Transform (AT). The results obtained in this technique show that this technique is both robust and also secure watermarking technique and is thus best for copyright protection. It supports high capacity and has the capability of detecting any type of forgery attempt. One more imperceptible, secure, and robust technique proposed [132] is based on chaotic amp and Chi-Square test. The results show that this technique offers less complexity than other techniques like SVD based Watermarking and has an optimal watermark payload. These techniques have been summarized in Table 7.

2.2.2.2 Semi-fragile Watermarking These types of watermarks are capable of being used for forensic purposes. In these techniques, the Authenticator can distinguish between the images whose content is intentionally modified and the authentic images which are intentionally modified with some modification approach that preserves the content of an image. These approaches may include compression technique (JPEG) with a reasonable compression rate [133–139]. There exist various semi-fragile techniques. The technique [140] uses the Discrete-Fourier-Transform (DFT). This technique makes the use of Substitution-box (S-box) and randomly selects the cover which is decided by the random number that is produced using the chaotic map. Results offered by this technique show that the technique is a secure and robust watermarking technique from all types of forgery attacks. However, its computational complexity is higher. One more technique proposed related to fragile and adaptive watermarking [141] is based on DWT

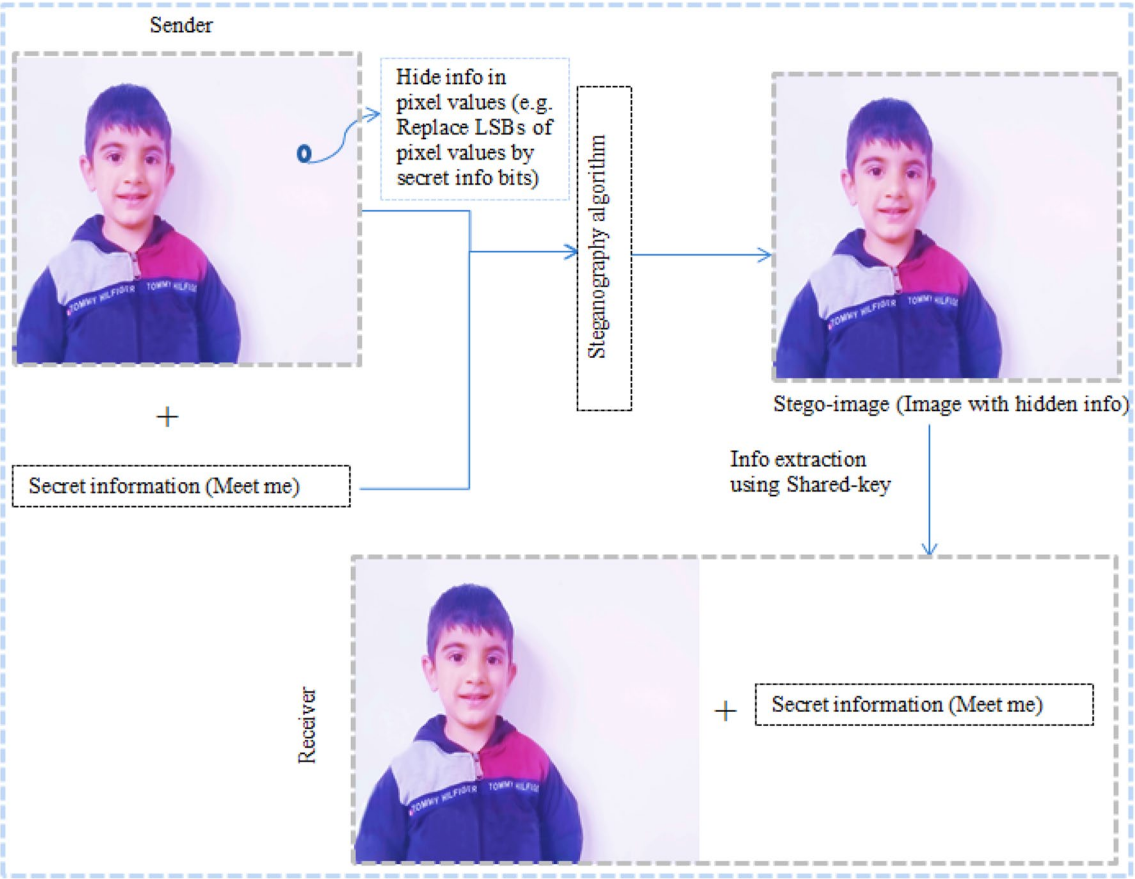

Sender
Hide info in pixel values (e.g. Replace LSBs of pixel values by secret info bits)
Steganography algorithm
+
Secret information (Meet me)
Stego-image (Image with hidden info)
Info extraction using Shared-key
Receiver
+
Secret information (Meet me)

Fig. 5 Original image followed by LSB steganography

and Set-Partitioning-In-Hierarchical-Tree (SPIHT) structure. After applying DWT on various sub-bands, the coefficients obtained from selected sub-bands are combined using SPHIT-algorithm. The partitioned image is further partitioned into bit-plane images and the selected bit planes of DWT coefficients receive the binary watermark. The results obtained in this technique show that this technique offers high accuracy and is adaptive in nature. One more proposed technique [142] is based on Singular-Value Decomposition (SVD) and-chaotic-permutation. This permutation is used to portion the watermark image into a number of fixed-sized blocks. These blocks are then transformed using SVD and the singular values of the cover receive the watermark using codebook techniques [143, 144]. The results show that this technique is a secure and robust watermarking scheme. Another Watermarking scheme for self-detection of JPEG-compression-forgery [36] embeds a watermark at the time of JPEG2000-compression. In order to generate the watermark, Perceptual-Hash-Function (PHF) has been applied on DWT-coefficients of the image. Another technique was proposed [145] that explores discrete-cosine-transform (DCT)-and-spread-spectrum (SS) to achieve the watermarking. DCT is- applied-on-the cover-image to transform it and-the-DCT-coefficients obtained receive the watermark. This technique is a secure and robust watermarking scheme and offers resistance against various forgery attacks. Table 8 given below summarizes the comparative study of semi-fragile watermarking techniques.

2.2.2.3 Robust watermarking This type of watermarking algorithm can survive content preserving modification like compression, noise addition, filtering, and also geometric modifications like scaling translation, rotation, shearing, and many more. It is used for ownership authentication [146, 147]. Various robust watermarking techniques have been proposed so far. Recently the robust watermarking technique [148] was proposed which uses lifting wavelet- transform (LWT), singular value decomposition (SVD), multi-objective artificial bee colony optimization (MOABC), and logistic chaotic encryption (LCE) algorithms to create an encrypted watermarking scheme for grayscale images and showed robustness against multiple image processing attacks. Another technique [149] is based on the false positive problem (FPP) of SVD. This technique aims at resolving the FPP problem in previously existed transform domain techniques like DWT-SVD, RDWT-SVD, and IWT-SVD. It

Table 5 Steganography techniques with brief description

Category	Reference	Technique	Description
Spatial based Steganography techniques	[81]	LSB	The pixel Least-Significant-Bits (LSBs) are replaced with some secret information bits Embedding and decoding process here is simple Have good payload capacity and visual quality Lacks security and has a poor defense against some attacks like statistical, geometric and compression attacks
	[82]	PMM	Uses some mathematical functions to map some image pixels with secret information bits Produces better quality stego-images than LSB techniques, result in less distortion and good imperceptibility Has lower payload capacity and has a poor defense against noise attacks
	[83]	RPS	Replaces randomly selected bits with the secret information to be hidden
	[84]	Histogram Based	The secret information is embedded within an image histogram The technique retains good visual quality and supports the reversible hiding of data Limited payload capacity and is poor defensive against attacks
	[85]	GLM	The secret information is hidden in the gray-level-of-an-image
Frequency based Steganography techniques	[86]	DWT	The wavelet decomposition is applied to select the pixels in an image that will store the secret information Provides more security than DCT and is also robust Has moderate capacity for payload embedding Requires large supplementary data so as to achieve reversibility
	[87]	DCT	The Discrete Cosine transformation is applied to select the pixels in an image that will store the secret information
	[88]	DFT	The Discrete Fourier transformation is applied to select the pixels in an image that will store the secret information Simple to implement Has poor embedding capacity, low visual quality and lacks of security
	[89]	DCvT	The discrete curve transformation is applied to select the pixels in an image that will store the secret information
	[90]	IWT	The integer wavelet transformation is applied to select the pixels in an image that will store the secret information Supports reversible data hiding and provides better security Has low embedding capacity

can be concluded from the simulation results of this work that if for the watermark embedding, instead of S vector, U vector is used, the problem of FPP can be resolved, and also the maximum values of robustness and imperceptibility can be obtained with the sacrifice of stability reduction which is obtained from S-vector singular values. Another technique [150] is based on DWT and encryption. This watermarking technique is applicable for the protection of image copyright. The technique makes use of Euclidean distance to identify those pixels of DWT-decomposed image that are supposed to receive the watermark. The simulation results obtained from this technique show that this technique is robust against various modifications which include compression, salt and pepper noise, and rotation. However, this technique has not been evaluated against geometric attacks. One more technique [151] is a content-based watermarking scheme for color images based on the local invariant significant bit-plane histogram. The results obtained proved that this technique is robust and shows resistance against the desynchronization attacks, and offers good visual quality and improved detection rates. This method has, however, high computation complexity and also offers less embedding capacity which needs to be taken care of. Another technique [152] is an adaptive watermarking scheme. The scaling factor has been evaluated using Bhattacharyya and Kurtoris technique. The simulation results depicted that it offers a high PSNR than the techniques [153, 154] which are in the same domain. However, the technique offers lower values for NCC, which makes it prone to attacks. Table 9 given below summarizes all these techniques.

2.3 Passive approaches

Passive approaches use intrinsic information and do not require prior information of an acquisition. They detect the image forgery when the watermark or digital signature is unavailable and also, they do not require the original image at the time of comparison. The passive digital image forgery methods are categorized into two main categories: tempering operation based and source camera identification based. Further, the tempering operation-based techniques are categorized into tempering operation-dependent and tempering

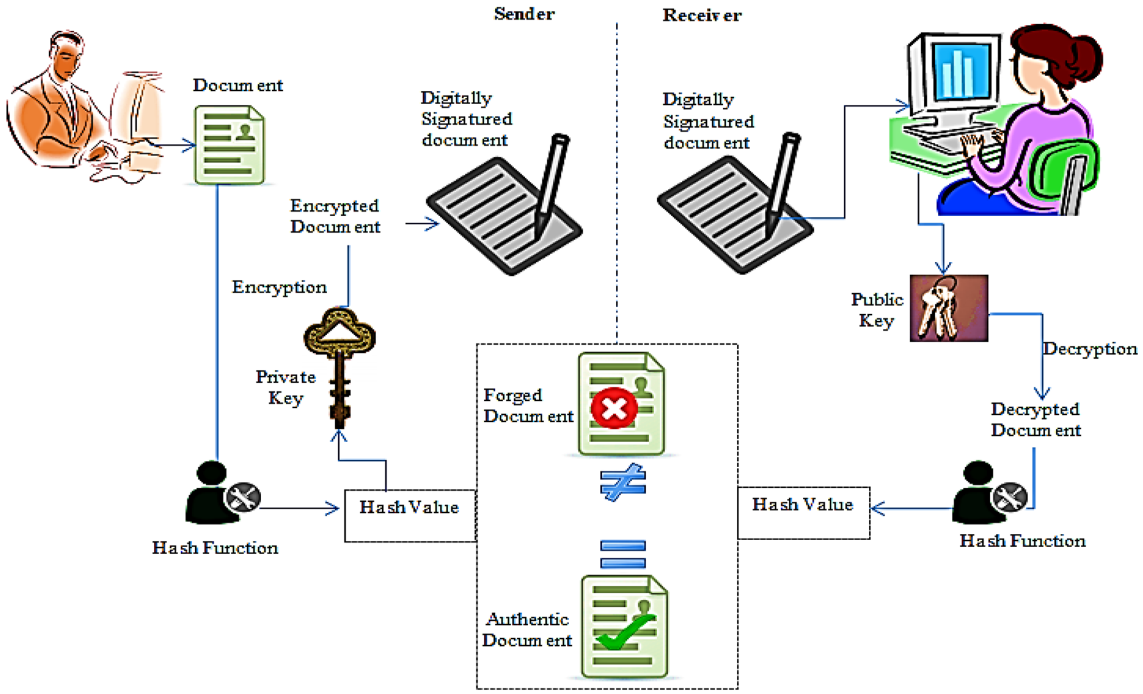


Fig. 6 The process of image authentication through digital signature

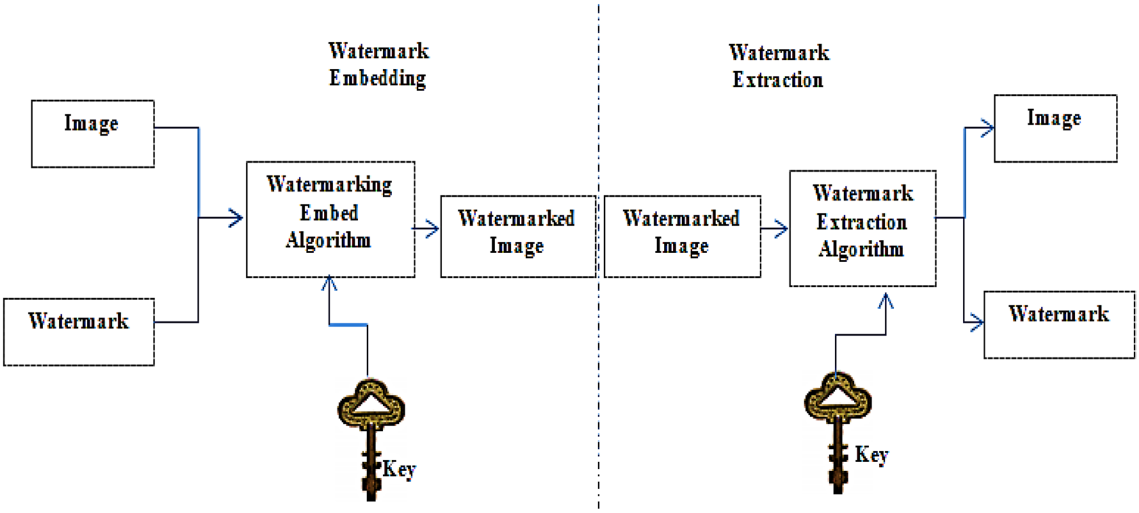


Fig. 7 Image Watermarking Process

operation-independent. The dependent techniques include image slicing or image composites and copy-move methods. On the other hand, the independent ones include resampling, retouching, sharpening and blurring, brightness and contrast, image filtering, compression, image processing operations, image cropping and interpolation, and geometric transformations. The source camera identification-based methods include lens aberration, color filter array interpolation, sensor irregularities, and image feature-based techniques. Each of these has been discussed below along with the comparative study.

2.3.1 Image splicing

Image splicing means to cut some object from one image and paste it on some other image [74]. Image splicing forgery is hard to detect than copy-move forgery because, in case of image splicing, different image object with different

Table 6 Digital watermarking techniques with description

Category	References	Technique used	Description with pros and cons
Spatial based Watermarking techniques	[102, 103]	LSB	This technique uses the LSBs of image pixels for embedding of watermark This technique withstands various attacks like cropping and compression transformations The watermark can easily be modified once it is known to the attacker
	[104]	RIF	In this technique, the watermark embedded in an image is the random code or text Used for digital forensics and security purpose
	[105]	SS	This technique uses spectral scattering to embed the watermark in the image
	[112, 113]	hardware-based watermarking	In this type of watermarking technique, the watermark in an image is embedded using custom-designed circuitry These techniques consume less power and less area The disadvantage of these techniques is that there remains the requirement of the original image for watermark detection
Frequency based watermarking techniques	[111]	DWT	In this technique, the region in which the watermark is to be embedded is found by wavelet transform. The temporal information is reserved during the process of transformation that is unlike the DFT
	[107, 108]	DCT	The DCT is applied on image blocks to get high, low, and mid-frequency-sub-bands. The coefficients of the mid-frequency sub-band are then modified to embed the watermark. This is done so that it does not affect the visibility of an image and the watermark becomes immune to compression attack
	[106, 107]	DFT	These techniques select the region by applying DFT so as to embed a watermark in it
	[109, 110]	SVD	Regions that will receive watermark are found by decomposition of singular values This technique is an optimal decomposition technique that packs maximum signal energy into least possible coefficients

features and texture are pasted in a different environment. Figure 8 below shows an example of image-splicing.

There do currently exist a number of image-splicing techniques. One of such techniques [155] uses deep learning networks like ResNet-Conv, Mask-RCNN, ResNet101, and ResNet50 to detect the splicing forgery in an image and this technique has the ability to learn to detect the discriminative artifacts from forged regions. The dataset for the training model was a computer-generated- image-splicing dataset from COCO-dataset and set-of-random-objects with transparent backgrounds. The results reported are AUC-value = 0.967. Another technique [156] uses block-based partitioning to explore the Partial blur type inconsistency over the dataset of 800-natural-blurred-photos. This technique has been able to achieve different accuracies at various Spliced-Region-Sizes (SRS). Another technique [157] has used CNN which is a deep learning algorithm to extract the features and the SVM classifier over the CASIAv1.0-and-CASIAv2.0-datasets. The detection accuracy achieved was 96.38%. One more approach [158] has used the auto-encoder-based anomaly feature and SVM. The detection accuracy obtained varies for various datasets viz. 91.88% for Columbia, 98% for CASIAv1.0, and 97% for CASIAv2.0. Another technique [159] explores block-based techniques, Otsu-Based-Enhanced-Local-Ternary-Pattern (OELTP), and SVM as a classifier over the CASIAv1.0, CASIAv2.0, CUISDE, and CISDE datasets, and this technique achieved detection accuracies of 98.25% using CASIAv1.0, 96.59% using CASIAv2.0, and 96.66% using CUISDE-datasets. These techniques along with some other important techniques have been summarized in in Table 10.

2.3.2 Copy move forgery

It is a process in which a certain image object is cut and pasted within an image [50, 166]. This type of forgery is done so as to hide some object in an image and this forgery is easy to get detected because of similar outlines of the object in the same image with similar features like texture, size, lines, curves, and others. Figure 9 given below shows an example of copy-move forgery.

Based on how this forgery is done, copy-move forgery is divided into the following four types:

(1) *Plain copy-move-forgery* In this forgery, the process is as follows: copy from one region and paste in another region within an image with no additional modifications (see Fig. 10).

(2) *Copy-move with reflection attacks* Copy-paste with 180° rotation to create an image with an object of different orientation (see Fig. 11).

(3) *Copy-move with image inpainting* This includes reconstruction of depreciated regions of an image with its corresponding neighboring regions so that it can look like real image. The modification is done in such a way that it becomes undetectable (see Fig. 12).

(4) *Multiple copy-move forgery* This type of forgery includes copying multiple regions or objects and pasting them in different regions (see Fig. 13).

Table 7 Comparative study about fragile watermarking techniques

Ref	Technique	Description	Experimental results
[128]	Spread Spectrum	This technique is imperceptible and Robust dual watermarking scheme	The Maximum Bit-Error-Rate (BER) = 7.06 at-PSNR-of = 42 dB and at a Message-length of 256bits and cover size = 768 × 512
	Quantization DWT		
	HVM	And this technique uses 1000 images from Corel-database	
[129]	BFW-SR (Designed technique)	This technique is robust against the-tempering-coincidence-problem	Reconstruction rate = 80% Good visual quality for reconstructed-images 1. For F-16 PSNR = 33.82 SSIM = 0.9637 PSNR-HVS-M (dB) = 32.15 2. For House PSNR = 26.90 SSIM = 0.8480 PSNR-HVS-M (dB) = 23.43 3. For Pepper PSNR = 32.83 SSIM = 0.9074 PSNR-HVS-M (dB) = 30.25 4. For Sailboat PSNR = 22.22 SSIM = 0.6654 PSNR-HVS-M (dB) = 19.77
	Hierarchical-tamper detection-algorithm	This watermarking-technique is for color-image authentication and self-recovery	
	Inpainting-algorithm	High quality of the resultant watermarked image	
	Bilateral altering		
[130]	Logistic map based chaotic cryptography	This Watermarking technique is secure and also a feasible technique for an outsourced data	MSE = 0
	Histogram		Payload = 8234 @ 0.0314 bpp and cover size = 512 × 512
[131]	LWT	This technique is both robust and also a secure watermarking technique and is thus best for copyright protection	PSNR = 50.01 dB for dual-watermarking cover size = 512 × 512
	DWT	It supports high capacity	
	Arnold Transform	This technique has the capability of detecting any type of forgery attempt	
[132]	Chaotic map	This technique is imperceptible, secure and robust dual watermarking scheme	Embedding Efficiency = 2 0.107 s and
	Chi-square test	Offers less complexity than other techniques like SVD based watermarking and has an optimal watermark payloads	Extraction efficiency = 1.086 Maximum-PSNR-obtained = 44.94 dB at-a-Quality-of-index-value = 0.9989 (Maximum) and at a maximum Payload = 1.73

Currently, there exist many copy-move forgery detection techniques. Some of these recent techniques have been highlighted below. An Adaptive CMFD-SIFT based technique [167] was proposed for copy-move image-forgery detection. This approach offers improvement to invariance to mirror transformation over a CoMoFoD dataset and also provides the *F* score value greater than 90%. Another recent technique [168] is based on Tetrolet-transform and Lexicographic-sorting. This technique offers high localization and detection accuracy and uses two datasets CoMoFoD and GRIP. The technique [169] is based on scaled ORB features. In this technique, first the Gaussian scale is created and afterward, the FAST and ORB features are extracted in each scale-space followed by removal of mismatched key points using the RANSAC algorithm. This technique has been found to be robust for geometric transformations. However, it suffers high time complexity when dealing with high-resolution images. Another copy-move detection technique [170] is based on FFT, SVD, and PCA. This technique offers high detection accuracy of around 98%. One more recent

Table 8 Comparative study of semi-fragile watermarking techniques

Ref	Technique	Description	Experimental results
[140]	Chaotic fractional Rossler system	This technique is robust and secure watermarking scheme	MSE = 4.8876 (Min)
	S-box, DFT	The watermark embedding is performed through chaos	PSNR value = 91.4512 dB (Max) Cover size = 256 × 256
[141]	DWT, SPIHT	This Watermarking technique is adaptive in nature and	WPSNR < 0.9405 dB
		Uses different databases for experimental purpose	PSNR = 48.1476 dB (Average)
		This technique offers high accuracy	Cover size = 512 × 512
[142]	Chaotic mixing, SVD	This technique is both robust and also a secure watermarking technique	PSNR = 50.01 dB for dual watermarking
		The watermark embedding is performed through chaotic permutation	Cover size = 256 × 256
[36]	Perceptual-Hash-Function (PHF)	This is a Watermarking-scheme for self-detection of JPEG compression. In order to generate the watermark, Perceptual-Hash-Function (PHF) has been applied on DWT coefficients	At bit rates 0.1 and 1 difference between the SSIM for max and minimum bit rates are between 0.0361 and-0.0074 for-Lena, 0.103 and 0.204for pepper, 0.0063 and 0.0033 for Boat, 0.0028 and-0.0048 for Bike
[145]	DCT, spread spectrum	This technique is secure and Robust watermarking scheme	BER = 0.0213
		Offers resistance against various forgery attacks	PSNR > 37 dB Cover size = 512 × 512

technique [171] is based on DOA-GAN. Three datasets have been used CASIA-CMFD, USC-ISI-CMFD, and CoMoFoD datasets and offer different accuracies on different datasets. One more technique [172] uses adaptive-attention and residual-refinement-network (RRN) over CASIA-CMFD, USC-ISI-CMFD, and CoMoFoD-datasets and achieves distinct accuracies on each dataset. Another technique [173] is based on interest point detector. This detector is first used to detect all the points of interest. Then afterwards the description of features has been done using Polar Cosine Transform. This technique can be employed in scene recognition or image retrieval and many others. This technique is, however, prone to resizing attacks. These techniques along with some other techniques have been summarized in the Table 11.

2.3.3 Resampling

Resampling means the transformation of image sample into another sample done by increasing or decreasing the pixel numbers of an image [185]. Resampling is done in different ways as follows:

(1) Up-sampling: In this method the number of image pixels is increased as shown in the Fig. 14.

(2) Down-sampling: In this method the number of image pixels is decreased as shown in the Fig. 15.

(3) Mirroring/flipping: In this method, the flipping of an entire image is done either vertically or horizontally as shown in Fig. 16.

(4) Scaling: In this method, the corner points of an image are dragged using various image editing tools like Photoshop (See Fig. 16).

(5) Rotation: In this method, image is rotated across its axis as shown in Fig. 16.

There exist multiple resampling detection techniques. One such technique [186] used two techniques, the A-Contrario-analysis algorithm, and a Deep-Neural-Network. The dataset used was NIST-Nimble (2017) and Nimble (2018). The technique reported an accuracy Area-under-Curve (AUC) = 0.73 and False alarm rate (FAR) = 1. Another technique [187] is based on random matrix theory (RMT). The technique offers a very low computational complexity. One more technique [188] makes the use of probability of residues noise and LRT detector for the detection of resampling forgery. This technique performs better with both compressed and uncompressed images. Another technique [189] is based used multiple algorithms over the UCID dataset and was able to achieve an accuracy of 90% for a high scaling factor. Another CNN-based technique [190] achieved 91.22% accuracy for all Quality Factors and 84.08% for a Quality-factor (QF) = 50. One more technique [191] is deep learning networks like iterative pooling network and branched network (BN) and the performance accuracy was 96.6% and 98.7% for IPN and BN, respectively. Another technique [192] used the Auto-Regressive model and FD detector and achieved true positive rate (TPR) = 98.3% and false positive rate (FPR) = 1% which is considered to be a

Table 9 A comparative study on Robust watermarking techniques

Reference	Technique	Description	Experimental results
[148]	Lifting wavelet transform (LWT)	Watermarking Scheme for grayscale-images	Reported results of watermarking images NC = 1 for all images and PSNR{ = 53.5755 (for Lena) = 52.7260 (for Baboon) = 53.0909 (for Cameraman) = 53.2531 (for Boat) = 51.3444 (for Peppers) = 48.4382 (for man)}
	SVD	The technique shows robustness against multiple image-processing techniques	
	Multi-objective artificial bee colony Optimization (MOABC)	Provides encrypted watermarking using LCE	
	Logistic-Chaotic-Encryption (LCE)		
[149]	DWT-SVD	The problem of FPP has been resolved and this technique is highly robust and imperceptible	Max − PSNR = 54.81
	RDWT-SVD	The technique however suffers from reduced stability due to singular-values of singular-vector	NCC = 0.9993
	IWT-SVD		SSIM = 0.999 Cover − size = 256 × 256
[150]	DWT	This Watermarking technique embeds the watermark in an image using DWT and encryption which makes it good Copyright Protection	WPSNR < 0.9405 dB PSNR = 48.1476 dB (Average)
	Encryption	The technique also offers high robustness against most of the image processing attacks This technique is not evaluated against the geometric attacks	Cover size = 228 × 228 Watermark image size = 90 × 90

[151]	Local invariant significant bit plane histogram	This technique is a content-based watermarking scheme for color images based on local invariant significant bit-plane histogram
		This technique is resistance against the desynchronization attacks and offers good visual quality
		This method has, however, high computation complexity and also offers less embedding capacity which needs to be taken care off
			Max-PSNR = 49.62 (peppers)
			Max-SSIM = 0.9893 (peppers)
			Cover-size = 512 × 512 × 24bit (10-color images)

[152]	DWT
	Bhattacharyya and Kurtosis-technique
		This technique is an adaptive watermarking scheme
		It offers a high-PSNR and has been tested on 10 grayscale images
		However the technique offers lower values for NCC, which makes it prone to attacks
			Max-PSNR = 52.07 (for Barbara image)
			NCC = 1 (when no attack)
			10 cover images of size = 256 × 256
			Watermark-image is cameraman [size = (256 × 256)]

better accuracy rate. The above-mentioned techniques have been summarized in Table 12 given below.

2.3.4 Retouching

Retouching of an image is done in order to remove the errors in an image like scratches, blemishes, etc. and this process is done in many ways [193]. Retouching is also done to hide the forgery left traces for the illegal attempt and some of the widely used techniques for this are contrast enhancement, sharpening manipulation. Retouching is also used for entertainment media like magazine covers etc. Various approaches to image retouching are shown in Fig. 17 below.

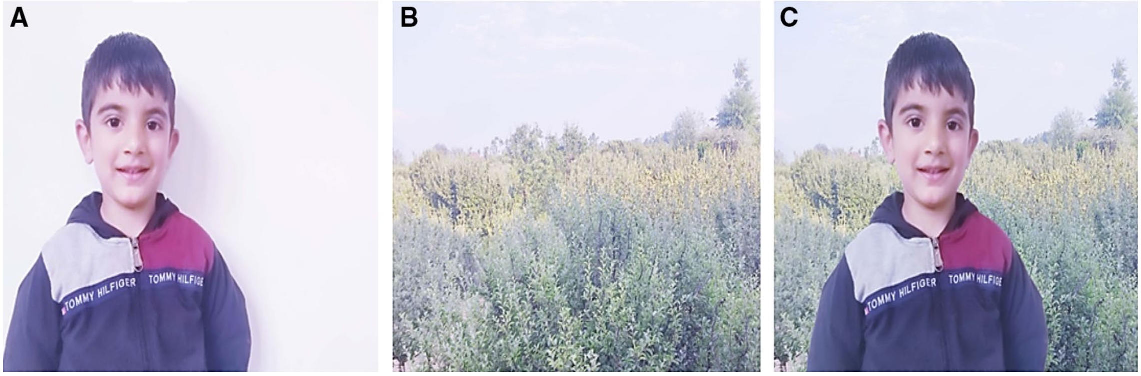


Fig. 8 An example of image splicing (**B** is used as background for image **A** which resulted in spliced image **C**)

Various retouching detection techniques have been proposed so far. Among these techniques, the technique [194] uses the multiresolution overshoot artifact analysis (MOAA) and non-subsampled contourlet transform (NSCT) classifier for the sharpening detection. Another CE detection technique [195] uses the histogram equalization detection algorithm (HEDA). The technique [196] used an overshoot artifact detector for un-sharp masking sharpening (UMS) detection and this technique shows robustness against post-JPEG compression and Additional Gaussian white noise (AGWN). One more technique [197] used histogram gradient aberration and ringing artifacts to detect the image sharpening operation. Another image sharpening detection technique [198] used edge perpendicular binary coding for USM sharpening detection. Another technique [199] explored deep learning and used CNN for image sharpening detection. The technique [200] used Benford's law for the contrast enhancement (CE) detection. Another technique [192] used anti-forensics contrast enhancement detection (AFCED) for the detection of CE. The technique [201] used Modified CNN for CE detection. One more recent technique [202] used multi path network (MPN) for the detection of contrast enhancement (CE). These techniques along with their performance are summarized in Table 13.

2.3.5 Image forgery detection using JPEG compression properties

One of the prominent compression-techniques is JPEG compression and is widely used in many applications. Detection of weather an image has undergone any sort of compression or not helps in image forensic investigation. Till date, many researchers came up with their JPEG-compression detection techniques. Among these techniques, we have some of the recent techniques which are worth noting. One of these techniques is [203] which used multi-domain, frequency-domain, and spatial-domain CNNs to locate the DJPEG (Double-JPEG). Another technique [175] is a CNN based DJPEG-detection technique which used aligned and non-aligned JPEG-compression for evaluation purpose. One more technique [204] used stack-auto-encoder for image-forgery-localization for multi-format-images. One more recent technique [205] used Modified-Dense-Net to detect primary-JPEG-compression and used a special-filtering-layer in-network for image classification. Another technique [206] used CNN with preprocessing-layer to detect DJPEG-compression. Another recent DJPEG-compression-detection-technique [207] used 3D-CNN in DCT-domain. One more recent technique [208] used Dense-Net for block-level-DJPEG-detection for image-forgery-localization. These techniques along with the description and dataset used have been summarized in Table 14.

2.3.6 Source camera identification

The source camera identification (SCI) involves the extraction of features that are used during image acquisition using an acquisition device (Camera). These characteristic features include the following:

(1) Lens aberration.
(2) Sensor imperfections.
(3) Color Filter Array (CFA) interpolation.
(4) Interpolation & image-features.

Lens aberration or imperfections refers to the artifacts that result from optical lens of digital camera. Because of lens radial distortion, the straight lines look like the curved lines on the output images. This creates different patterns of different camera models which are then used to identify camera models. Once the source is known, it then becomes easy to detect the forgery. Another type of source camera identification is based on sensor imperfections. These imperfections can be described with the use of sensor pattern noise and pixel artifacts. One of the techniques [210] can detect the source camera using sensor pattern noise. The main cause of this pattern-noise is irregularities of sensors resulted from its manufacturing processes. These patterns are later used

Table 10 A comparative study on Image splicing detection techniques

References	Technique	Description with dataset	Experimental results
[155]	ResNet-conv Mask-RCNN ResNet-50	This technique has ability to learn detect the discriminative-artifacts from forged regions	The proposed network has an e area under the curve (AUC) value of 0.967, which is excellent
	ResNet-101	The dataset for training model is computer-generated image-splicing dataset from COCO-dataset and set-of-random-objects with transparent-backgrounds	The convergence of ResNet-50 was shown to be faster than ResNet-101

[156]	Partial-blurtype inconsistency	Dataset used includes
		1. 800 natural blurred-photos (400-out-of-focus and 400-motion) in TIFF-format (Uncompressed)with-size-ranging-from 1024×768 to 3456×2304 px, from 4 cameras
			Reported results:
			For SRS (spliced region Size) = 100×100
			Accuracy = 94.5%
			TNR = 94.4%
			TPR = 95.1%
			For SRS (spliced region size) = 200×200
			Accuracy = 95.4%
			TNR = 95.3%
			TPR = 96.8%
			For SRS (spliced region Size) = 512×384
			Accuracy = 96.3%
			TNR = 96.6%
			TPR = 95.1%

	Block-based partitioning	2. For Splicing localization various Spliced-region sizes including 100×100, 200×200 and 512×384	
[160]	Characteristicfunction moments for the inter-scale co-occurrence matrix in the wavelet-domain	This technique is applicable to both color- and grayscale-image datasets and relies on luminance component of an image	Detection accuracy = 96.2% (Max) for 100 features = 93.6% (for 50 features)
	SVM-with-RBF-Kernel (Classifier)	This technique used CASIA1, CASIA2 and Columbia-gray DVMM datasets	
[157]	SRM-CNN/Xavier-CNN	This technique used CASIAv1.0, CASIAv2.0 and DVMM-dataset	Reported detection accuracy For CASIAv1.0 = 98.04% For CASIAv2.0 = 97.83 For DVMM = 96.38
	SVM (classifier)		
[158]	Textural features based on the gray-level co-occurrence matrices (TF-GLCM) SVM (as-classifier)	This technique used CASIAv1.0, CASIAv2.0	Reported detection accuracy For CASIAv1.0 = 98% For CASIAv2.0 = 97%
[159]	Block-based technique	Used a new descriptor for local feature extraction by optimal threshold value	Accuracy reported as = 98.25% on CASIAv1.0 = 96.59% on CASIAv2.0 = 96.66% on CUSIDE

Table 10 (continued)

References	Technique	Description with dataset	Experimental results
	Otsu-based enhanced local ternary Pattern (OELTP)	Used parallel processing to evaluate overlapping blocks for better computational efficiency	
	SVM (as Classifier)	Datasets used are CASIAv1.0,CASIAv2.0,CUISDE and CISDE Need focus on forgery Localization	
[161]	Logistic-regression	The datasets used are CASIAv1.0, CASIAv2.0, COLUMBIA Used four handcrafted features	Reported accuracy: =98.3% on CASIAv1.0, =99.5% on CASIAv2.0 and =98.8% on COLUMBIA
[162]	Convolutional neural network (CNN)	Datasets used are CASIAv1.0 and CASIAv2.0	Reported results: For full CASIAv1.0 dataset 95.45% accuracy 98.04% precision 97.09% recall For CASIAv2.0-dataset 97.27% accuracy 99.04% precision 98.09% recall For DCT-based-algorithm 90.01% for CASIAv1.0 and 96.36% for CASIAv2.0
	DWT	Also tested the model using DCT instead of DWT and afterwards using PCA Need focus on forgery localization DCT-based-algorithm yields less accuracy with CASIAv1.0	
	SVM (as-Classifier)	DWT-based algorithm yields better precision for CASIAv2.0 dataset	

[163]	Low-dimensional DCT and DWT-based features	Dataset used is 200 random copy-move images chosen from datasets CASIA v1.0-and- CASIA v2.0	Reported results:
			Accuracy = 94.10%
			TPR = 93.62%
			TNR = 97.44%

	Ensemble-classifier	Robust against various post-processing-operations such as scaling, rotation, and Gaussian-noise	
[164]	VM KNN LDA Decision-tree naïve-bayes LBP-histogram	Dataset used was CASIAv2.0 This approach offers less computational complexity Need focus on forgery localization	Accuracy = 65.83% for FVS = 256, = 92.98% for FVS = 512 = 94.59% for FVS = 768
[165]	Noise print	Dataset used is CUISDE-dataset	Reported performance: average-classification-accuracy = 97.24%
	ResNet-50-network	This technique makes the use of noise print-based residual-noise map which recognizes the splicing modifications with better accuracy	
	SVM-classifier	This technique also uses deep-CNN-ResNet-50-based feature-extractor for feature extraction	

for the detection of the source camera of an image. Another characteristic feature used for SCI is CFA interpolation. One of the techniques [211] uses CFA-interpolation. One more characteristic feature used for SCI is image features. The technique [212] differentiates these features into three main categories viz. wavelet-domain statistics, color features and image quality metrics in order to identify the source camera model. One of the limitations of these techniques is that they are not effective for images that are taken from a camera having a similar charge coupled device (CCD) and hence fail to detect the exact source camera model. Other techniques are based on the photo response non uniformity (PRNU), feature extraction, and camera response function (CRF). The technique [213] provides a counter measure in order to avoid the PRNU. Another technique [214] makes the use of the texture features of colored images as a left-out fingerprint of the camera which was used to capture the image. One more technique [215] used to assess the camera response function (CRF) from local invariant planar irradiance points (LPIP).

3 Video forgery approaches

As the videos are the collection of frames or images, any sort of modification can be done to these frames and hence to the videos. There are two types of video forgery techniques which are Inter-frame forgery and Intra-frame-forgery methods. The classification of video forgery detection techniques is shown in Fig. 18 below.

3.1 Inter-Frame video forgery

In *Inter-frame Video Forgery,* we have frame insertion, frame deletion, frame replication and frame duplication which results in the change of frame sequence in the video. This includes frame insertion, deletion and duplication. The various inter-frame video forgery approaches are diagrammatically explained in Fig. 19.

(1) *Frame insertion* refers to the insertion of a set of frames into the already existing frame sequence in the video.

(2) *Frame deletion* refers to the deletion of frames from the already existing set of frames in the video.

(3) *Frame duplication* refers to the duplication of frames or simply copying the set of frames and pastes them in some other location in the existing frame sequence of the video.

(4) *Frame replication/shuffling* refers to the shuffling or modifying the original order of frames in a video that makes the video different in meaning from the original one.

There exist various inter-frame video forgery detection techniques. These techniques are summarized in Table 15.

3.2 Intra-frame video forgery

In intra-frame video forgery, the alteration of content is done within a frame. Many a times, in a whole length of the video, the objects are put so as to make the altered frame unrecognizable. The intra-frame video forgery is of two types which include:

(1) *Splicing* Splicing in a video forgery refers to a fresh arrangement of video frames created from the original sequence by adding or removing some object to or from its frames, respectively.

(2) *Upscale crop video forgery* This refers to the cropping an extreme outer part of a video frame so as to remove the incidence proof and later the size of these frames is increased so that their inner dimension remains unchanged.

(3) *Copy-Move forgery* It refers to an insertion or the deletion of an object from a video frame take place. It can also be sometimes like copy-paste type forgery and hence is also called as region manipulation forgery. Removal of objects from videos is sometimes compensated by filling the vacant area with similar background content. This is called as inpainting. Inpainting can be carried out in any of the following two ways:

> Temporal copy and paste Inpainting (TCP) refers to filling up the void with similar pixels from the surrounding coherent blocks or regions of the same video frame.
> Exemplar-based texture synthesis inpainting: refers to filling up the void with the use of sample textures.

The techniques related to these types of video forgeries along with comparative study are summarized in the Table 15.

4 Deep learning approaches to forensic analysis

Deep learning is one of the promising subsets of machine learning that offers the automatic feature extraction capability without external intervention. It provides combined service of feature extraction and classification. Deep learning network is an interconnected multi-layer network. It has one input layer to feed input to the network and one output layer which provides the actual prediction. In between these layers there exist multiple hidden layers. There are two most important deep learning algorithms which have gained popularity due to their high accuracy rates for pattern recognition from an image.

There are two types of deep learning algorithms: convolutional neural networks (CNNs) and recurrent neural networks (RNNs). CNN is the most prominent deep learning

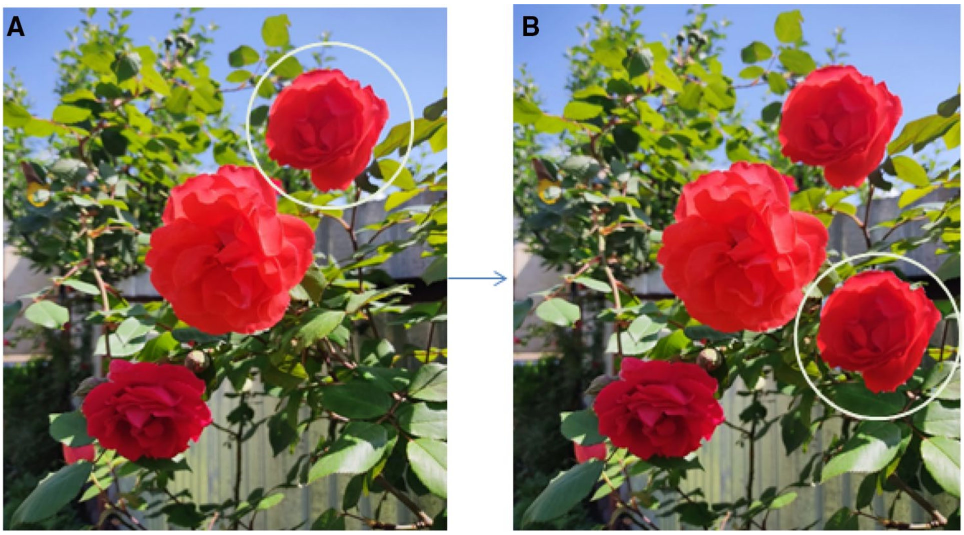


Fig. 9 Copy-move-forgery

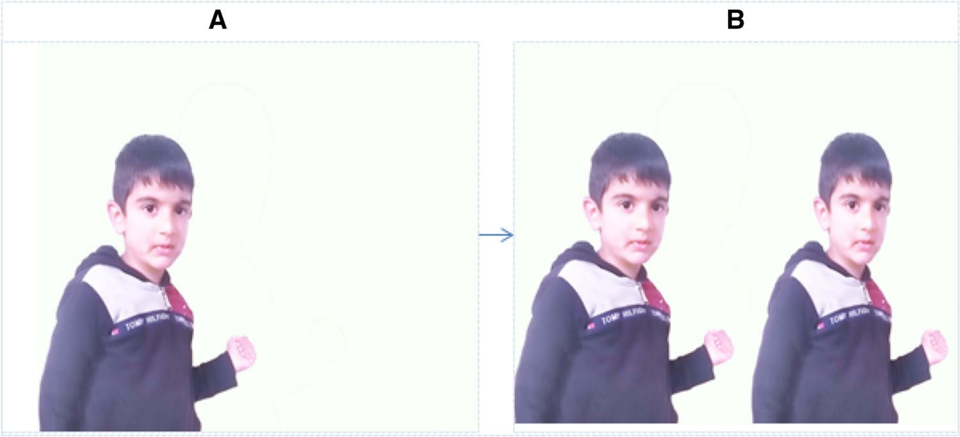


Fig. 10 Plain-copy-move forgery (**A**–**B**)

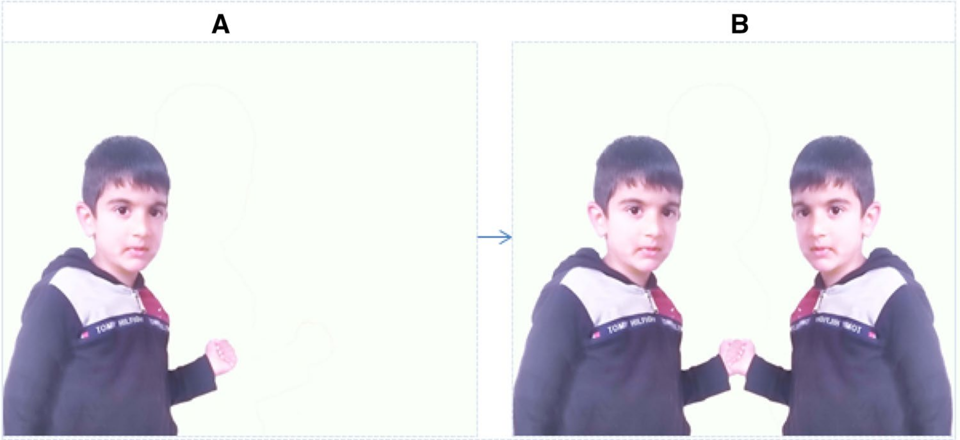


Fig. 11 Copymove with reflection (**A**–**B**)

algorithm that uses its convolution layer for the purpose of feature extraction. It finds its applications in pattern recognition and image processing. It has the capability to find the content pattern in an image and thus extract the features from it. RRNs find their applications in natural language processing (NLP) and speech recognition areas due to the fact that these networks process sequential and time series data.

Because of the high accuracy rate for pattern recognition, deep learning has found its application in image and video

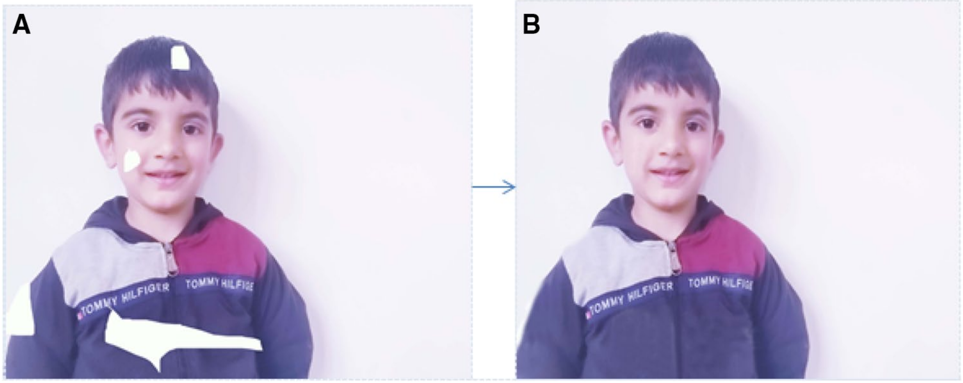


Fig. 12 Copy-move with image inpainting (**A**–**B**)

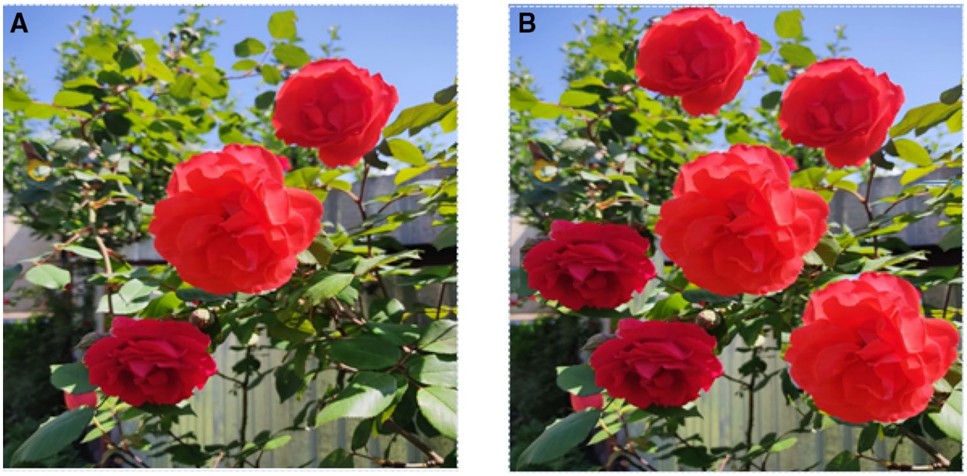


Fig. 13 Multiple copy-move forgery (**A**–**B**)

forensic analysis. Till date many researchers have come up with the image and video forensic techniques based on deep learning algorithms.

4.1 Deep learning-based techniques for image forgery analysis

Chen et al. [255, 256] proposed a CNN based approach which extracts median filtering residuals from image. The first layer of CNN is a filter layer which reduces the interference that arises due to presence of the edges and textures. The removal of interference helps model to investigate the traces left by median filtering. The approach was tested on a dataset of 15,352 images, obtained by composition of five image datasets. A spliced image may consist of traces of multiple devices. A CNN based image forgery detection technique [256] can detect media filtering and cut-paste forgeries using the filtering residuals. Using this 9-layer CNN framework the accuracy rate achieved was 85.14%. Another image forgery detection technique [257] can detect cut-paste and copy-move forgeries using the stacked auto-encoders (SAE). The technique used CASIA v1.0, CASIA v2.0, and Columbia datasets and thus achieved an accuracy of 91.09%. One more CNN based technique [258] can detect Gaussian blurring, Media filtering and resampling using prediction error filters. The dataset used are the images from 12 different camera models, thus achieving an accuracy of 99.10%. Another auto-encoder-based technique [222] can detect the cut-paste forgery. The dataset used various images from six smart phones and a camera, thus achieving an $F1$-score of 0.41 for basic forgery and 0.37 for post-processing forgeries. One more CNN based technique [223] can detect the cut-paste forgery using the hierarchal representation from the color images. The datasets used were CASIA v1.0, CASIA v2.0, and Columbia gray DVMM and achieved an accuracy of 98.04%, 97.83% and 96.38%, respectively. Another CNN based image forgery detection and localization technique [259] can detect and localize the cut-paste forgery using the source camera model features. The datasets used are Dresden image database, thus achieving a detection accuracy of 81% and localization accuracy of 82%.One more tempering localization technique [260] is based on multi-domain

Table 11 A comparative study on copy-move image forgery detection techniques

Reference	Technique	Description with dataset	Performance

[167]	Modified-edition of SIFT-technique	Dataset used id CoMoFoD	Reported results:
			TPR = 95.88%
			FPR = 9.02%

	AHC-algorithm	This technique shows better performance in terms of invariance for mirror-transformation	
[168]	Tetrolet-Transform	Datasets used are CoMoFoD and GRIP	For GRIP dataset: F1 score = 0.9876 CPU-time/image = 37.51 s
	Lexicographical-sorting	High localization and detection accuracy even for most of the post-processing operations and is capable of detecting very-small duplicated regions and multiple-forgeries even for smooth images	For CoMoFoD-dataset: Average-precision = 0.9981 Average-recall = 0.9603 F1 score = 0.9789 CPU-time/image = 11.63 s
[169]	FAST key-points	This technique used the 107-original and 170-forged images as dataset	Reported results running-time: = 270 ms/image (86 ms for feature-extraction + 184 ms for matching)
	ORB features	This technique shows good results for geometric-transformations	
	Hamming distance	High computational complexity for forgery-detection of high-resolution images	
	RANSAC-algorithm		
[170]	FFT, SVD, PCA	Dataset used is CASIA v1.0	Reported results accuracy = 98% at 6%FNR for JPEG-QF = 20 and region-size = 32 × 32px
	Exhaustive-search	The technique is fully free from threshold This technique offers good detection-accuracy	

[171]	DOA-GAN	Datasets used CASIA-CMFD, USC-ISI-CMFD and CoMoFoD-datasets
		Datasets used for training 80,000 copy-move forged images from USC-ISI-dataset and 80, 000 pristine-images and for Testing 10,000 forged images and 10,000 pristine-images (collected from COCO-dataset)
			Reported results on USC-ISI dataset
			Precision = 96.83%
			Recall = 96.14%
			F1-Score = 96.48%
			On CASIA-CMFD dataset (Detection -accuracy, Loc-accuracy)
			Precision = 63.39,54.70%
			Recall = 77.00,39.67%
			F1-Score = 69.53,41.44%
			CoMoFoD dataset (Det-acc, Loc-acc)
			Precision = 60.38,48.42%
			Recall = 65.98,37.84%
			F1-Score = 63.05,36.92%

[172]	Adaptive-attention and residual-refinement-network (RRN)	Used CASIAII, COVERAGE, and CoMoFoD-datasets	Reported Results on CASIAII dataset
			Precision = 58.32%
			Recall = 37.33%
			F1-Score = 45.52%
			On COVERAGE
			AUC = 0.8488
			For CoMoFoD
			Precision = 54.21%
			Recall = 46.55%
			F1-Score = 50.09%

[173]	Interest-point detector Adaptive matching	Dataset used is SBUCM161 Robust technique	Reported Results CPU time = 436 ms/image
[174]	Matching Triangles Mean-Vertex-Descriptors	Dataset used is CMFDA The technique performs well for complex-scenes	Reported Results CPU time = 10 s/image
[47]	Multi-level Dense Descriptor Hierarchical Feature Matching	Dataset used is CMFDA Shows robustness	Reported Results F score > 91%

Table 11 (continued)

Reference	Technique	Description with dataset	Performance
[175]	Multiscale analysis SURF NNDR	Dataset used are CMH and CMEN developed for forgeries like rotation-and-resizing However, this technique does not perform well for small or homogeneous region	Reported Results CPU time = 1.881 s/image
[176]	Multiscale feature Adaptive patch	Dataset used is CMFDA Performs better for down-sampling and multiple copies	Reported Results $F = 95.05\%$
[177]	Particle-swam-optimization plus SIFT Best bin first	Dataset used is CMFDA Does not perform well for small regions	Reported results precision = 99%

[178]	SIFT
	Morphological operation
		Dataset used is CMFDA
		Offers good accuracy
			Reported results
			precision = 96.6%
			Recall = 100%

[179]	Super-pixels classification adaptive key-points Reversed g2NN	Dataset used is CMFDA This technique performs better for geometric-transform However this technique is computationally complex	Reported results CPU time = 221 s/image
[180]	VlFeat software, RANSAC K nearest neighbors	Datasets used are CMFDA,MICC-F600 and MICC- F2000 Offers good detection accuracy but slow performance	Reported results precision = 86%
[181]	Zernike moments SIFT g2NN	Datasets used are CMFDA and CoMoFoD This technique can detect smooth regions	Reported results $F = 84.91\%$

[182]	SIFT and reduced-LBP-histogram	Datasets used are MICC-F220,CMH,D and COVERAGE	Reported results on MICC-F220 dataset
			TPR = 99.10%
			FPR = 5.45%
			ACC = 96.82%
			On CMH
			TPR = 95.68%
			FPR = 0.35%
			ACC = 97.66%
			For COVERAGE
			TPR = 78%
			FPR = 43%
			ACC = 67.5%

[183]	Image-blobs and binary-robust-invariant-scalable-Key points (BRISK) feature	Datasets used are MICC-F8multi, MICC-F220, and CoMoFoD	Running-time = 6.24 s Reported results on MICC-F220 dataset TPR = 93% FPR = 5.4% On 220images from MICC-F220 dataset TPR = 94.49% FPR = 93.63% For 400-images from CoMoFoD $P_r\% = 96.84$ $r_c = 92\%$ $F1$-Score = 94.35%

[184]	Block-and-keypoint-based-approaches
	adaptive-galactic-swarm-optimization (AGSO)
	hybrid-wavelet Hadamard-transform (HWHT)
	random-sample-consensus (RANSAC)
	forgery-region-extraction-algorithm (FREA)
		Datasets used are MICC-F600 and Benchmark-dataset	Reported results at pixel level:
			For MICC-F600-dataset
			Precision = 92.4%
			Recall = 93.67% and $F1 = 92.75\%$
			For benchmark dataset
			precision = 94.5% Recall = 95.32% and $F1 = 93.56\%$

Fig. 14 Image Up-sampling

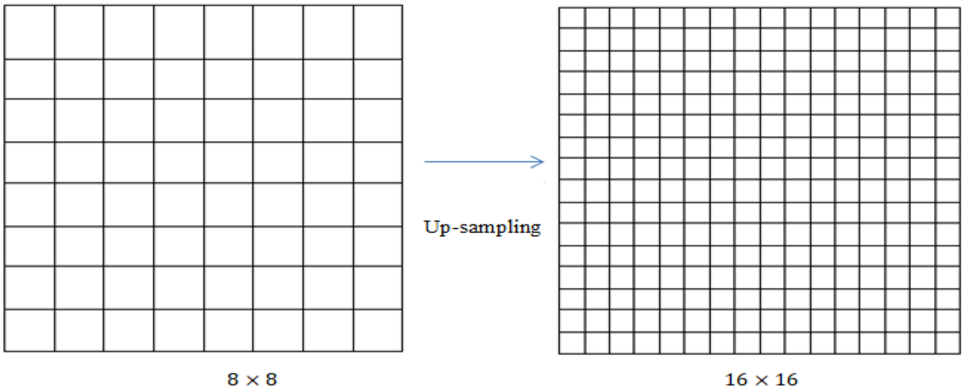


Fig. 15 Image Down-sampling

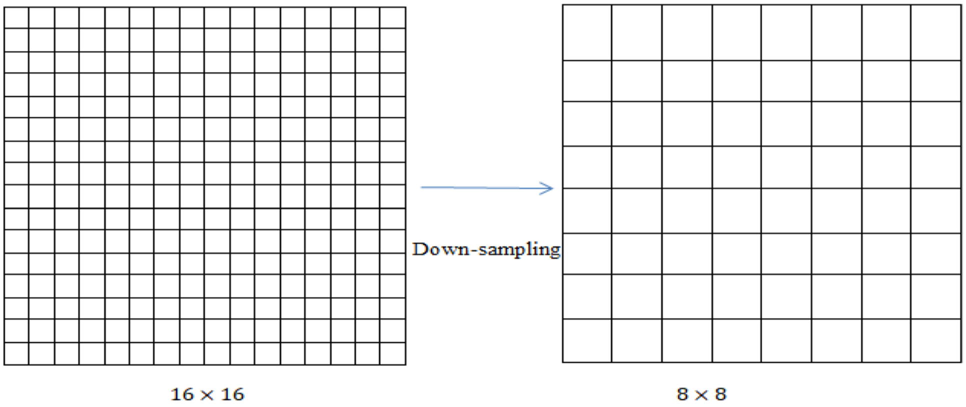
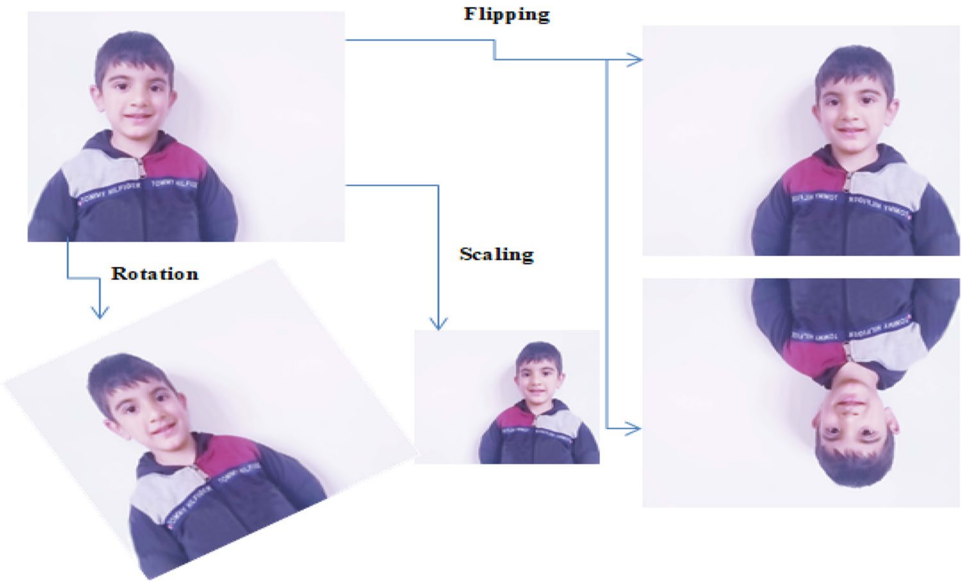


Fig. 16 Resampling-techniques



CNN and UCID dataset, thus achieving an accuracy of 95%. Another image splicing localization technique [261] used multi-task fully convolutional network and Columbia, CASIA v1.0, and CASIA v2.0, thereby achieving an $F1$ score of 0.54 on CASIA v1.0 and 0.61 on Columbia and MCC score of 0.52 on CASIA v1.0 and 0.47 on Columbia. Another copy-move forgery detection technique [262] with source localization used BurstNet, a deep learning network and VGG16 features. The datasets used are CASIA v2.0 and CoMoFoD datasets thereby offering an overall accuracy of 78%. One more image splicing detection technique [263] used Ringed Residual U-Net (RRU-Net) and the datasets

Table 12 A comparative study on image re-sampling forgery detection techniques

Ref	Technique	Description with dataset	Performance
[186]	A-Contrario-analysis algorithm	The dataset used is NIST-Nimble (2017) dataset	Reported accuracy: AUC = 0.73, False alarm rate (FAR) = 1
	Deep neural network	Nimble (2016)-dataset	
[187]	Asymptotic eigenvalue distribution Random matrix theory (RMT)	The dataset used is the 1317-raw-images from Dresden-image-dataset This technique offers low computational complexity	Reported results: For JPEG recompression: better detection accuracy for $F > 95$
[188]	Probability of residual noise LRT detector	The dataset includes the 500 uncompressed and non-resampled images and 500 compressed resampled JPEG images at a quality factor (QF) between 50 and 90 Effective with uncompressed/ compressed resampled images	As reported: Detection-accuracy = 100% and Computational complexity = 0.0996 s at RF = 200%
[189]	Inverse filtering process with blind deconvolution hierarchical multi-region fusion Second Difference sparsity (SDS) property Kernel scale searching (KSS) content-adaptive method	The dataset used is UCID This technique does not perform well for JPEG blocking artifacts and blurred images	Accuracy = 90% for high scaling-factor (*f*) Accuracy of both bilinear and bi-cubic interpolation image with Gaussian noise (SNR = 40)
[190]	Convolutional neural network (CNN)	This technique used includes 6500 images with varying size and minimum size = 2688 × 1520 This technique can detect resampling in recompressed images	Detection accuracies > 91.22% for all QF's = 84.08% for 120%upscaled images and QF = 50
[191]	Iterative pooling network (IPN) Branched network (BN),	Dataset used is Columbia dataset The proposed solutions, IPN and BN help to regain the lost accuracy	For IPN Accuracy = 96.6% (at average resampling factor (RF)) For BN Accuracy = 98.7% (at Average-resampling factor (RF)) Patch level accuracy (Columbia-dataset) For Google natural images (NI) = 90% For personal-NI = 94% For computer-generated = 78%
[192]	Autoregressive (AR) model Normalized histograms SVM FD-detector	This technique used BOSS dataset Training set includes 3000 unchanged images and 3000ALL-images As reported, with the increase in JPEG-CR performance decreases	Without JPEG compression $P_e < 0.2\%$ TPR = 98.3%, FPR = 1% (For Compressed or uncompressed)

of CASIA and COLUMB datasets, thereby achieving an accuracy of 76% and $F1$ score of 0.84 and 0.91 on CASIA and COLUMB datasets, respectively. Another recent image tempering localization and detection technique [264] used mask regional convolution neural network (Mask R-CNN) and the datasets of COVER and Columbia datasets, thereby achieving an average accuracy of 93% and 97%, respectively (see Figs. 20, 21) (see Table 16).

4.2 Deep learning-based techniques for video forgery analysis

The main task of video forensic analysis is the extraction of key-frame from the video scene. There is no better option other than deep learning techniques for feature extraction. Thus many researchers have come up with the deep learning-based video analysis techniques. One of such techniques [265] is based on ensemble learning for the summarization of the video events and named it as event bagging approach. Another technique [266] is an interest oriented video event summarization approach that represents image information using visual features. One more technique [267] was proposed using a nonconvex low-rank kernel sparse subspace learning for key-frame extraction and motion segmentation. Another event detects and summarization technique [268] for Multiview surveillance videos is based on machine learning technique Ada-Boost approach for the multi-view environment. The potential key frames have been selected for event summarization using deep learning framework CNN. Using these key frames the event boundaries are detected

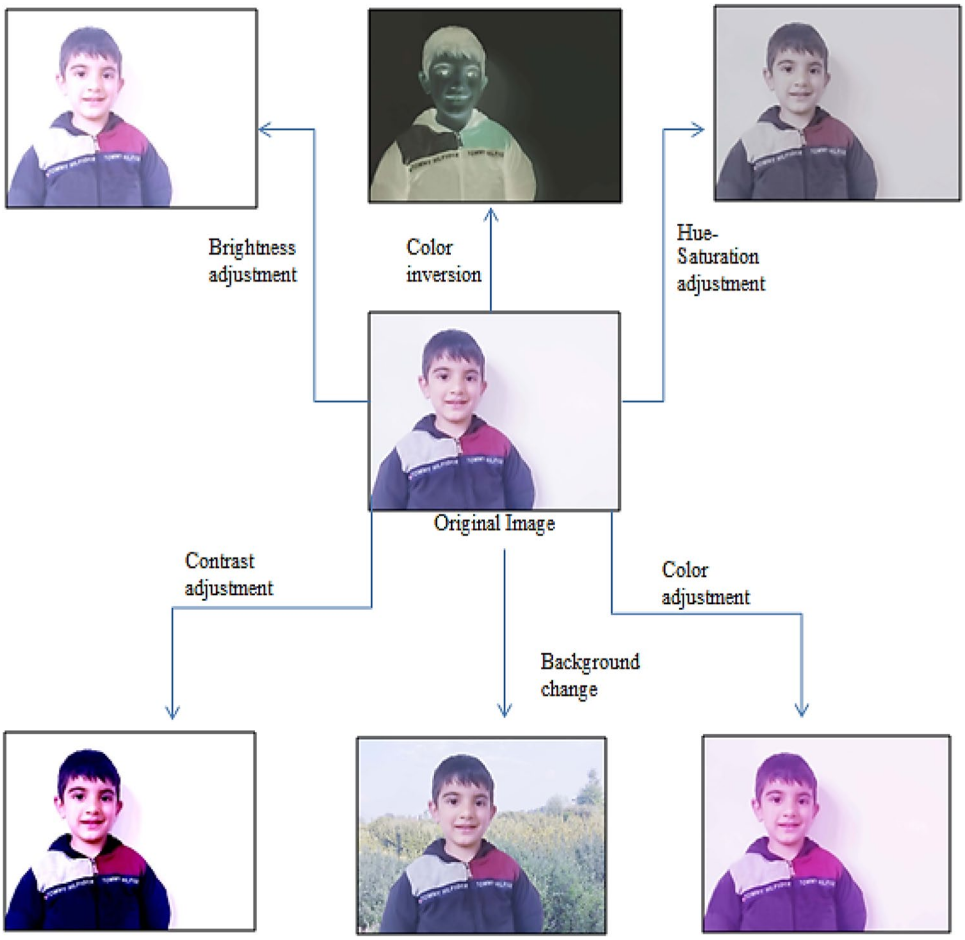


Fig. 17 Image retouching approaches

for video skimming. This model has been named as deep event learning boost-up approach (DELTA). The computational time reported for a sample rate of 30 frames per sec was 97.25 s. Another paper [269] introduces a fast and deep event summarization (F-DES) and a local alignment-based FASTA approach for the summarization of multi-view video events. Also a deep learning model has been used for feature extraction which dealt with the problem of variations in illumination and also helped in removing fine texture details to detect the objects in a frame. The FASTA algorithm is then used to capture the interview dependencies among multiple views of the video via local alignment. The computational time reported for a sample rate of 30 frames per second was 91.25 s. Another more related work [270] suggested key frame extraction technique based on Eratosthenes Sieve for event summarization. It combines all the video frames to create an optimal number of clusters using Davies-Bouldin index. The cluster head of each cluster is treated as a keyframe for all summarized frames. The results reported are for three variants AVS, EVS and ESVS and offers a maximum precision rate of 58.5% by ESVS variant, a recall of 50% and F-measure of 53.9%. Also the computational time reported for AVS, EVS, and ESVS are 65 s, 20 s and 20 s, respectively. Another similar work [271] proposed a Genetic algorithm and secret sharing schemes based genetic uses in video encryption with secret sharing (GUESS) model to generate sequence of frames with minimum correlation between the frames. The computational time reported is 16.375 s for 125frames and a block size of 25. Also the correlation reported is minimum and is equal to 0.01 for block size k = 35. Another paper [272] uses the spatial transformer networks (STN) that can efficiently be used for spatial and invariant information extraction from input to feed them to more plain NNs like artificial neural network (ANN) without comprising the performance. The authors suggest that this technique can replace the CNN for basic computer vision problems. The paper has reported different accuracy measures of precision, recall, F-measure and time per epoch for different models. One more recent work [273] has presented local alignment based multi-view summarization for generation of the event summary in the cloud environment. The reported computational time is 65.75 s per video at a sample rate of 30 frames per second and the accuracies of precision, recall and f-score have also been reported for three datasets Office, Lobby and BL-7F.

Table 13 A comparative study on image retouching forgery detection techniques

Ref	Technique used	Description with dataset	Performance
[194]	Multiresolution overshoot artifact analysis (MOAA)	Datasets used are 1. Uncompressed color image database (UCID) 2. Natural resource conservation service photo gallery (NRCS) 3. Break our watermarking system database (BOWS2)	For UCID Max detection accuracy = 92.38% (at $\sigma b = 1.0, \lambda = 1.5$) For NRCS Max detection accuracy = 91.07% (at $\sigma b = 1.0, \lambda = 1.5$) For BOWS Max Detection accuracy = 92.67% (at $\sigma b = 1.0, \lambda = 1.5$)
	Non-subsampled contourlet transform (NSCT)-Classifier		
[195]	Histogram equalization detection algorithm (HEDA)	This technique used 341 images taken from different camera models as its dataset	Detection probability (Pd/TPR) $Pd >$ 0.99 at false alarm probability (Pfa/FPR) Pfa $\leq 3\%$
[196]	USM sharpening detector	This technique used 400 images taken from different camera models as its dataset	The detection rates for all sharpening methods achieve > 88% at False Alarm Probability (Pfa/FPR) = 10%
	Overshoot artifact detector	It shows robustness against post-JPEG compression and additional Gaussian –hite noise (AGWN)	
[197]	Histogram gradient aberration	This technique used 403-images taken from different camera models as its dataset	For histogram technique Maximum precision = 0.941 at $\lambda = 0.4$ = 0.700 at $Q = 90$ For ringing technique Maximum precision = 0.0.864 at $\lambda = 0.4$ = 0.778 at $Q = 70$ For joint technique maximum precision = 0.939 at $\lambda = 0.4$ = 0.701 at $Q = 90$
	Ringing artifacts metric		
	Fisher classifier		
[198]	Edge perpendicular binary coding	The dataset used is the 1000-random images from UCID an NRCS datasets to create a new dataset of 2000 grayscale uncompressed images	Detection accuracy = 94.93%
[199]	CNN SVM-classifiers and Fisher linear discriminant (FLD)	Double-JPEG compression detection-technique As a training dataset it uses 800 images and as a validation dataset uses 200 images selected from UCID. And for testing dataset low-resolution images are from the still images in UCID having a resolution = 512 × 384, and the high-resolution images are from the Dresden image dataset	For DRESDEN dataset Max AUC value = 1.00 FOR UCID dataset Max AUC value = 0.98 Max accuracy achieved = 0.796

Table 13 (continued)

Ref	Technique used	Description with dataset	Performance
[200]	Benford's Law SVM	This technique uses UCID dataset	Detection performance of Benford's features for anti-forensic integrated contrast enhancement mapping Max detection accuracy Pd/TPR = 99.2%, Pfa/FPR = 1.8% and 1.3% at QF = 70and 50 and Gamma = 0.9 and 2.0, respectively Detection performance of Benford's features for original contrast enhancement mapping Max detection accuracy Pd/TPR = 98.7%, Pfa/FPR = 4% at QF = 70 and Gamma = 0.5
[192]	Anti forensics contrast enhancement detection (AFCED) technique	The dataset consists of 117 images selected from Dresden image dataset	Max TPR = 98.23% Max-TNR = 99%
[201]	Modified CNN	This technique is robust against JPEG-CE forensic technique and as a dataset uses 10,000 images from BOSS-RAW database	Max AUC = 1 (For global CE and training set size = 24,000) Max AUC = 1 (For Gamma correction (GC) at cropping parameter = 16)
[202]	Multi-path network (MP-Net)	Dresden, RAISE and UCID	Detection accuracy Pd > 0.6 atPfa = 0.01

Some encryption based techniques are also worth discussing. One of the encryption related work [274] came up with a model named as V ⊕ SEE based on Chinese Remainder Theorem and Multi-Secret Sharing scheme for the encryption of video in order to securely transmit it over the internet. The computational time and correlation value between secret frames reported are minimum 15.555 s and 0.0126, respectively, for 125 frames. Another recent work [275] proposed a model for encryption over cloud. In this the key is generated dynamically using the original information without the involvement of the user in the process which makes it hard for an attacker to guess the key. Another work related to data encryption in images [276] explored the multimode approach of data encryption through quantum steganography. Another work [277] have proposed a Polynomial congruence based Multimedia Encryption technique over Cloud (P-MEC) for the encryption of transmitting multi-media over the cloud by introducing a cubic and polynomial congruence that makes it difficult for an attacker to decrypt the encrypted content in a reasonable amount of time. The accuracy measures like MSE, PSNR, and correlation have been reported for four types of images.

5 Future direction

After carrying out the extensive study in a well-organized way, it was found that there still exists a lot of research gap which needs to be dealt with by the upcoming researchers. Furthermore, the forgery detection is now becoming more and more challenging because of the advent of more sophisticated and easily available tools.

Some of the most common challenges in image forgeries are as follows:

- Feature extraction is the most challenging task in forgery detection process on which the efficiency of the whole process depends. Deep learning is the most preferred one. There are a very few forgery detection techniques proposed till date based on deep learning. So in future deep learning can be explored further.
- For watermarking schemes, the common challenges include imperceptibility, security, embedding capacity, and computational complexity which need a future focus.
- Feature dimensionality is another challenge which also needs future attention.
- Computational complexity of most of the forgery detection techniques is more and needs to be minimized in the future.
- Lack of robustness against the post-processing operations in the case of many forensic approaches.

Table 14 A comparative study on JPEG compression-based image forgery detection techniques

Ref	Technique used	Description and dataset	Performance
[97]	Multi-domain CNN	Dataset used is UCID dataset	For QF2 = 80 multi-domain-CNN shows accuracy ≈ 95% Frequency-CNN shows accuracy ≈ 83% Spatial-CNN shows accuracy ≈ 80%
	Frequency CNN	Multi-domain CNN shows higher accuracy at QF2 = 80	For QF2 = 95 Multi-domain CNN shows accuracy ≈ 99% Frequency-CNN shows accuracy ≈ 99% Spatial-CNN shows accuracy ≈ 88%
	Spatial-CNN	This technique, however, is computationally complex and also does not perform well for QF1	
[201]	CNNs for DJPEG-detection	Dataset used is RAISE The three CNNs considered for evaluation of performance are *Cpix*, *Cnoise*, *andChist* denoting CNN in pixel domain, noise domain and embedding DCT histogram computation, respectively	Accuracy < 0.75 (for 10% training dataset) And ≈ 0.82 (for 70% training data) For histogram-Enhancement accuracy ≈ 99% (at 8 × 8 grid-desynchronization) For cropping, accuracy≈80% For light-blurring accuracy ≈ 62% (at 3 × 3 Gaussian-smoothing-kernel with variance $\sigma^2 = 1$) For resizing, accuracy ≈ 30% (
	Stochastic gradient descent (SGD) algorithm	To evaluate the robustness of the technique, aligned JPEG compression and non-aligned JPEG compression were taken into account	

[202]	Stack auto-encoder	Dataset used is CASIA
		This approach can work for multi-format-images
		To achieve better accuracy, this technique also integrates the contextual information to forged feature blocks
			Accuracy = 0.9284
			*F*1 score = 0.5839
			AUC = 0.9375

[203]	Modified –dense net with special filtering layer F-LDA	Dataset used is UCID Detects double-JPEG Uses F-LDA for selection of kernel-filters	For spatial domain network comprehensive accuracy = 88.6% For multi-domain-basednetwork comprehensive accuracy = 95.0%
[209]	CNN with pre-processing layer	Dataset used for performance evaluation is BOSSbase-v1.01 and UCID-dataset for testing generalization capability Detects double-JPEG compression	Average accuracy = 87.71% Max detection accuracy on UCID = 96.89% (for QF = 90)
[204]	3D-CNN in DCT domain	The dataset used for training is 1,026,387 images and for testing 114,043-images Detects double-JPEG compression	Error rate = 8.84% (without feature scaling and 1.66 M parameters) Error-rate = 6.14% (with feature scaling and 1.66 M-parameters)

Table 14 (continued)

Ref	Technique used	Description and dataset	Performance

[205]	Dense Net	Dataset used are RAISE, Dresden, and BOSS
		Block-level DJPEG detection for image forgery localization
			Performance Using 90% Patch's for Training:
			Detection accuracy = 94.49%
			TPR = 91.74%
			TNR = 97.25%
			performance for unseen Q-matrices:
			Test accuracy = 92.83%
			TPR = 89.40%
			TNR = 96.25%

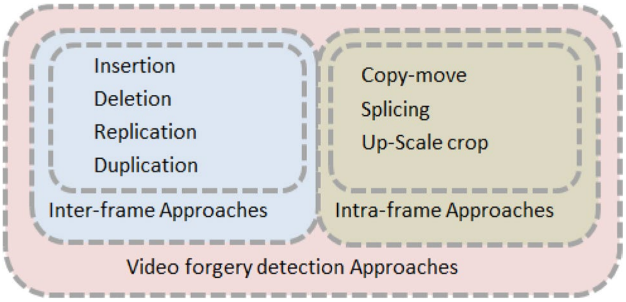


Fig. 18 Video forgery approaches

- Most of the techniques also show invariance against the geometrical transformations and hence also need a future focus.
- Some techniques show a slow feature learning rate which needs to be improved.
- Improvisation of localization accuracy for most of the forgery detection techniques is also needed.
- There is a lack of datasets that can cover all the possible attacks.
- Most of the techniques show vulnerability to different types of forgery-attacks like JPEG Compression and others.
- The single technique fails to detect all the present forgery types in an image which limits its utilization.

These challenges need a focus in future and hence open the gates for the researchers to carry out their future research in this area.

Furthermore, from the comparative study of video forensics techniques, it was worth noting that although we have many forensic tools and techniques that can efficiently detect video forgery, due to advancement in forgery tools and their easy availability, there still exists a research gap that can be dealt with in future. Some of the important and common challenges in video forgery include the following:

- *Computational complexity* There exist many techniques with high computational complexity for forgery detection which need to be dealt with.
- Currently we have very few anti-forensic techniques. Thus, researchers in the future can develop more such tools.
- Robustness against post-processing operations requires to focus on in future.
- Deep-fake detection is another interesting area for future research in the domain of video forensics.
- Deep learning is gaining huge popularity in every field because of its novel feature extraction capability. There are very few algorithms existing that have explored deep learning techniques. Therefore, it opens a gate for

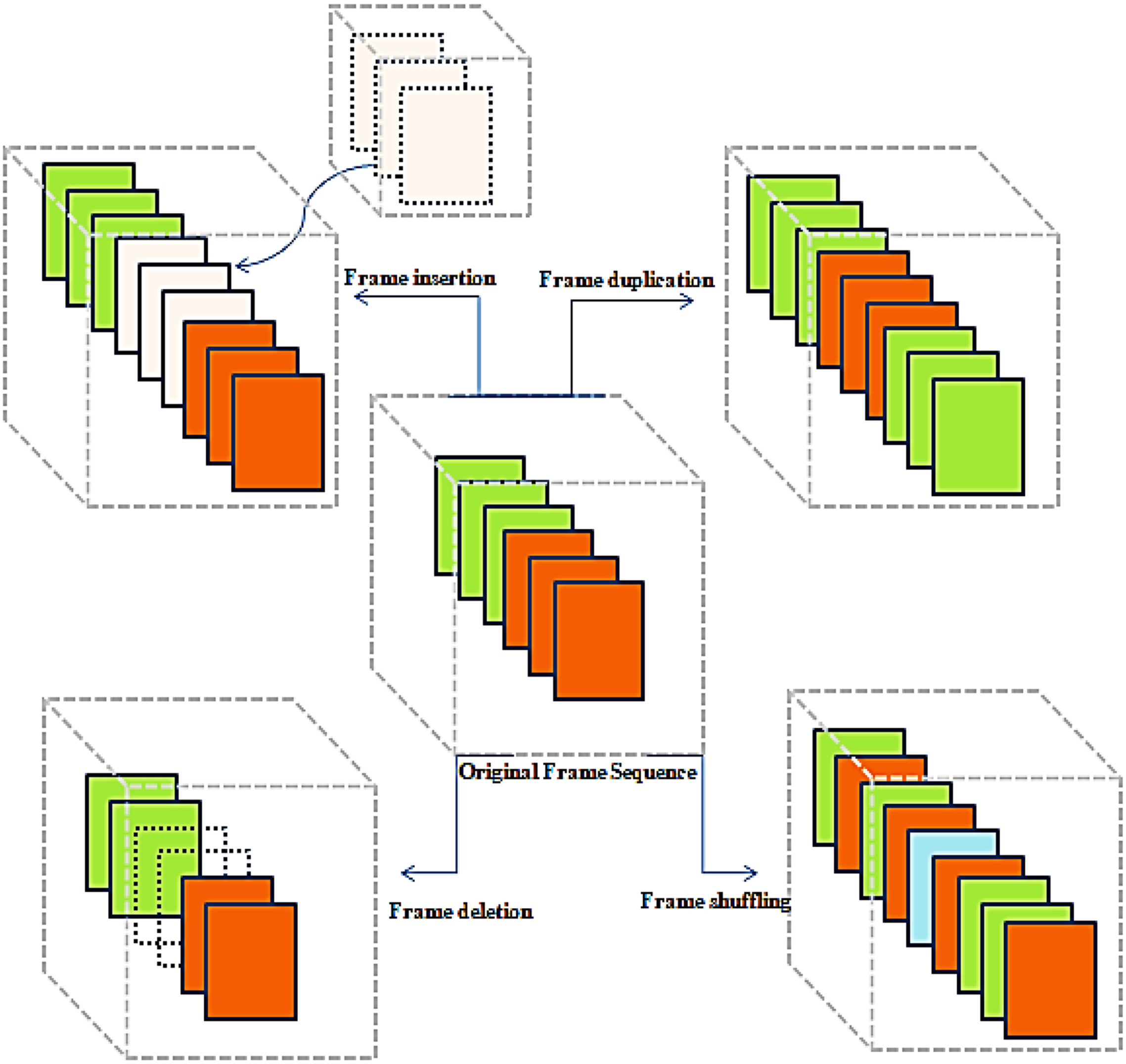


Fig. 19 Inter-frame video forgery approaches

researchers to explore it further in the domain of video forensics.

- There also exist some machine learning-based video forgery detection techniques. These machine learning algorithms also prove to be very efficient with high detection accuracy and can hence be explored with other video forgery detection techniques in the future.
- Many existing techniques fail to work for moving background and variable GOP structure videos, which again prove to be the hot topic to focus on in future.

6 Conclusion

With a systematic and well-organized research approach, a detailed and high-quality survey article has been presented. This review article not only provides a comparative study of various existing technologies, but also provides future directions and challenges in the field of image and video forensics. The first section of this article provides the brief introduction of image and video forensics along with their applications and the existing datasets.

Table 15 A comparative study on various video forgery detection techniques

References	Technique	Description with dataset	Performance
Inter-frame video forgery			
[216]	Block-wise brightness-variance descriptor (BBVD)	Detects and locates frame insertion	For detection precision rate (PR) = 94.09% Recall-rate (RR) = 98.67%

		Dataset used includes 240 AVI format Videos from KTH Database and TRECVID	For localization
			PR = 79.45%
			RR = 89.23%

		If the frame insertion or deletion count is < 25, then the efficiency decreases	Results based on no. of frames inserted
			PR = 75.8% ($N \leq 25$)
			RR = 83.5% ($N \leq 25$)
			PR = 86.32% ($N > 25$)
			RR = 94.25% ($N > 25$)

		The Forgery localization accuracy is low	
		It is effective for the still-backgrounded videos & fixed-length GOP structure	
[217]	Sequence of average residual of P frames (SARP)	Detects frame deletion forgery Dataset used comprises of 20YUV-Videos and every video has 300frames with resolution = 176 × 144	True-positive rate (TPR) = 91.82%
		Used × 264-encoder and H.264 Joint Model (JM) decoder Effective for slow-motion-videos	True-Positive Rate (FPR) = 5% & average-detection-accuracy = 92.08%
[218]	Inter-frameinterpolation Global and Local joint feature	Detects frame-deletion with anti-forensic operation	Running-time = 0.0971 s DA average-reduction = 2.01% for 63-frame-interpolation without global frequency-domain statisticalfeature in AVC-videos, and
		Dataset used includes H.264-codec encoded 100 CIFvideo sequences	DA average-reduction = 3.13%in 63 frame interpolation in HEVC videos
[219]	Stepwise-regression KNN, LR & SVM	Detects frame-deletion forgery Also effective for varying length GOP implication Dataset used includes 36 MPEG-2 coded video	Average TPR = 95% Average-FNR = 4%
[220]	Convolutional-3D-Neural-Network (C3D)	Detects frame-deletion in a single-video-shot	For Nimble-Challenge2017 dataset: C3D-based-network + output-score, AUC = 86% C3D-based-network + confidence-score, AUC = 96%

Table 15 (continued)

References	Technique	Description with dataset	Performance
		Training-dataset includes 2394-iPhone4-videos of 1–3 min duration from world-dataset through medifor-rankone-browser 2650-forged-videos created YFCC100m and NimbleChallenge2017	For YFCC100m-dataset C3D-based-network + output-score, AUC = 86% C3D-based-network + confidence-score, AUC = 96%

[221]	Residual Frames
	Entropy of DCT Coefficients
	subsequence feature analysis
		Detects and localizes inter-frame duplication	On SULFA [222]:
			RR = 98.3%
			TPR = 99%
			$F1 = 98.6\%$ &

		The datasets used include
		SULFA
		VIRAT
			On VIRAT [223]:
			RR = 97.1%
			TPR = 98.2%
			$F1 = 97.6\%$

		Ineffective for motion-backgrounded and changing-length-GOP videos	Computational time: Clip-sequence duplication (CSD) = 0.02 s/frame Single-frame duplication (SFD) = 0.01 s/frame
[224]	Scale-invariantfeatures transform (SIFT)	Detects copy-move and frame-duplication forgeries	For Spatial-CMFD At Rotation = 10 and $Sx, Sy = 1, 1$ Max-DA,PR,RR = 100% Spatial-CMFD for region-size (128 × 128) Max-DA = 100% (at BR = 9Mbps and FP = 0.001
	Residue and Correlation-technique	Used their own dataset and SULFA Accuracy is less for more compressed videos Ineffective for motion-backgrounded and changing-length-GOP videos	For frame duplication Max-DA = 100% (at BR = 9Mbps at FP = 0)

[225]	Temporally informative representative images discrete cosine transform (TIRI-DCT)	Detects Frame-duplication-forgery
		Personal dataset with 3 YUV format video clips with 300Frames/video with 100 intentionally duplicated frames
		Ineffective for motion-backgrounded and changing-length-GOP videos
		Does not perform localization
			TPR = 100%
			FPR = 0%

[226]	Coarse-tofine-technique
	block-based algorithm
		Detects Frameduplication forgery
		Created own dataset of 15 fake video clips
		Ineffective for motion-backgrounded and changing-length-GOP videos
			Precision = 84.9%
			Recall = 100%
			DA = 100%
			dice-coefficient (DC) = 95.1%
			Computational time = 109.6 s/frame

Table 15 (continued)

References	Technique	Description with dataset	Performance

[227]	Tamura-Texture Features	Detects and locates copy-move video forgery
		Created own dataset of ten videos which were taken using both stationary and handheld cameras
			Precision = 99.60%
			Recall = 100%

[228]	Structural similarity	Detects and locates copy-move video forgery
		Dataset includes
		15 videos captured from mobile and digital cameras with every frame resolution = 640 × 480px and FR = 30and15f/s
		Ineffective for motion-backgrounded and changing-length-GOP videos
			PR = 99.7%
			RR = 100%

[229]	Window-based rough detection technique and binary searching
	Frame-to-frame-optical flows and double-adaptive thresholds
		Detects frame insertion and deletion
		Dataset used includes
		Videos from KTH & TRECVID datasets
		And 40 Videos from TRECVI1D (MPEG-2 codec)
		Ineffective for motion-backgrounded and changing-length-GOP videos
			For Insertion:
			Precision = 98%
			Recall = 95%
			For deletion:
			precision = 89%
			Recall = 85%

[230]	Improved existed algorithm Anti-forensic technique Video inter-frame forgery (VIF)-game	Detects video-frame deletion forgery Dataset includes 32-QCIF-video-sequences in YUV uncompressed Format Localization is not done Ineffective for motion-backgrounded and changing-GOP-length effects' performance	Detection rate = 100% False-positive rate = 6.3%
[231]	Automatic frame deletion or insertion detection techniques based on *P* frame-prediction error Anti-forensics detector	Detects frame-insertion and deletion forgeries Dataset used 36 standard-video test-sequences of QCIF-format and frame size = 176 × 144 px Ineffective for changing GOP-length effects performance Localization of frame deletion is not done	Detection accuracy = 85%False-positive rate = 15%
[232]	Consistency of correlation-Coefficients of gray values (CCCoGV) Support vector machine (SVM)	Detects frameinsertion and deletion videoforgery Dataset used is 5 video databases (1original and 4 are forged) with 598-videos with still-background and little camera shake Ineffective for motion-backgrounded and changing GOP length effects performance	For original video dataset Classification-accuracy (CA) = 99.34% (For 100frame insertion) = 99.22% (for 25frame-insertion) = 97.27% (For 100frame-deletion) = 94.19% (for 25frame deletion) For forged-video datasets Classification-accuracy (CA) = 96.21% (For 25frame-deletion) = 95.83% (for 100frame-deletion)

Table 15 (continued)

References	Technique	Description with dataset	Performance
[233]	Technique with 3modules 1.Double-compression detection, 2. Malicious tampering detection 3.Decision fusion SVM classifier	Dataset used includes 22 YUV raw video sequences in CIF/QCIF-formats from video trace library (VTL) (MPEG-2 encoded)	Detection accuracy = 83.39%
		Detects malicious inter-frame video forgery-detection in MPEG-videos	Precision = 88.4%
		Ineffective for motion-backgrounded videos	Recall = 90.5%
[234]	SCREs of P frames DCT coefficient traces of quantization error wavelet-based-algorithm	Detect frame insertion or deletion and double compression with different GOP structures and lengths	True-positive Rate (TPR) = 92.73%
		Dataset used includes 22 YUV videos from VTL (MPEG-2 encoded)	False-positive rate (FPR) = 92.73%
		Ineffective for motion-backgrounded videos	Detection accuracy (DA) = 92.73%
[235]	DCT coefficients distribution GOP analysis	Detects double-quantization in digital video from double-MPEG compression or from hybridizing two different quality videos	DA = 25% (QR < 1.3)
		Dataset includes three MPEG2-encoded videos	DA = 41.2% (1.3 < QR < 1.7)
		Ineffective for motion-backgrounded and changing-length-GOP videos	DA = 99.4% (QR > 1.7)
		Forgery localization needs improvement	

[236]	unified-identification-algorithm
	anomaly detection technique
		fDetects frame deletion, insertion and duplication forgeries	For insertion:
			DA = 85%
			LA = 100%

		Dataset includes 40 videos from TRECVID (MPEG-2 codec) & SULFA (H.264 & MJPEG encoded videos)	For deletion:
			DA = 72%
			LA = 96.9%

		Detection accuracy for frame-deletionforgery detection is low	For duplication
			DA = 82.5%
			LA = 86.2%

		Ineffective for motion-backgrounded videos	
[237]	Modified-Huber–Markov-Random-Field (HMRF)	Detect MPEG-videos-forgery and double-compression in both MPEG-2andMPEG-4 videos	DA > 95%
		Dataset used is Video from video testmedia, Derf's collection and YUV-sequences (MPEG-2 & 4 encoded) Localization is not done	Efficiency = 100%

Table 15 (continued)

References	Technique	Description with dataset	Performance
[238]	Temporal & spatial correlations	Detects frame duplicationvideo forgery	For stationary cameras Average DA 87.9% (for3Mbps BR) 84.8% (for 6Mbps BR) 84.4% (for 9Mbps BR)
		Dataset includes Videos Recorded by SONY-HDR-HC3 camera Forgery-localization needs improvement	For moving cameras Average DA 86.8% (for3Mbps BR) 99.0% (for6Mbps BR) 100% (for9Mbps BR)
Intra-frame video forgery			
[239]	Sensor pattern noise- based scheme (SPNC)	Detects copy-move video forgery	For NRC average DA = 64.5–82.0% FPR = 2.3–9.7%
	CFA-V	Dataset used comprises videos from SULFA and VTL (MJPEG,MPEG-2,MPEG-4, and H.264/AVC encoded)	For SPNC: Average DA = 89.9–98.7% FPR = 5.2–11.4%

	H-DC		For CFA-V:
			Av-DA = 83.2–93.3%
			FPR = 10–20.5%

	NRC		For H-DC:
			Av-DA = 79.1–90.1%
			FPR = 12.5–25.2%
			[FPR-for-compressed-videos (QFs 100–70)]

[240]	Novel approach	Copy-move video forgery detection	Accuracy ≈ 92% (for Multimodal fusion of residue features transformed in cross-modal subspace)
	Noise & Quantization Residue Features	Dataset comprises videos collected from internet-streamed movies Ineffective for motion-backgrounded-videos	

Table 15 (continued)

References	Technique	Description with dataset	Performance

[241]	CNN	Detects copy-move video forgery
		Dataset includes SYSU-OBJFORG (H.264/MPEG-4 encoded video)
		Computation cost is high
		Ineffective for motion-backgrounded videos with high-BR and high resolution
			PFACC = 98.08%
			FFACC = 88.75%
			FACC = 96.68%
			PR = 96.5%
			RR = 90%
			F1-Score = 93.26%

[242]	Chrominance-value-of-Consecutive frame difference (CCD)
	Discriminative robust local binary pattern (DRLBP)
	SVM
		Forged frame detection and localization
		Dataset comprises f 12,463 frames (6500 authentic and 5966 forged frames)
			TPR = 96.5%
			TNR = 93.6%
			DA = 96.68%
			Video acc = 98.32%
			Testing time = 0.1058 s

[243]	Technique that Analyzes the foot prints that are left on the residual	local tampering detection and localization in video sequences
		Created own-dataset-REWIND with 120 realistic sequences and resolution = 320 × 240px and each with 300 frames and some from SULFA (videos with H.264/ AVC codec)
		Ineffective for motion-backgrounded and changing length GOP videos
			TP = 0.62
			FN = 0.38
			TN = 0.94
			FP = 0.06
			AUC = 0.91

[58]	Adjustable-width object boundary (AWOG)
	Non-subsampled Contourlet transform (NSCT) & gradient information
	SVM
		Detects object-based video forgery
		Dataset used includes 9 typical static AVI & WMV formatted videos
		Ineffective for motion-backgrounded videos
			DA = 96.83%
			PR = 96.28%
			RR = 96.43
			FPR = 1.18%

[244]	Laplacian-pyramid
	Spatial-decomposition
	Sequential-analysis
		Detects object-based video forgery
		Dataset used comprises of Videos taken from static surveillance camera (uncompressed and resolution = 1280 × 520px)
		Ineffective for motion-backgrounded videos
			For uncompressed videos:
			PR = 93.3%,
			RR = 93.3%,
			*F*1-Score = 93.3%
			For compressedMPEG4-Videos:
			Precision = 92.8%
			Recall = 92.8%
			*F*1 = 92.8%

Table 15 (continued)

References	Technique	Description with dataset	Performance

[245]	Sequential and patch analyses	Detects and localizes object removal video-forgery
		Dataset used comprises videos from SYSU-OBJ-FORG taken by static-surveillance-camera and resolution = 1280 × 720 and BR = 25F/s
		Ineffective for motion-backgrounded videos
			For Uncompressed video
			PR = 96.65%,
			RR = 97.78%,
			DA = 96.70%
			For-Compressed video
			precision = 95.51%,
			Recall = 94.44%,
			Detection Acc. = 94.97%

[246]	Noise-level-function (NLF)
	Expectation–maximization (EM) algorithm
		Detects forgeries in static video scene
		Used a dataset created by their own videos compressed by the lossless huffyuv,MPEG2,H.264 and Cinepak codecs
		Ineffective for motion-backgrounded videos
			For huffyuv-Codec
			True-positive = 97.02%
			True-negative = 98.60%
			For MPEG2:
			True-positive = 46.41%
			True-negative = 55.03%,
			For H.264
			True-Positive = 39.38%
			True-Negative = 53.91%
			For Cinepack:
			True-positive = 6.2%
			True-negative = 91.07%

[247]	Software de-interlacing algorithms
	Inter-Field & Inter-frame motions correlation factor
		Detects de-interlaced and interlaced video forgery
		Used a dataset comprising of videos captured by their own in lab, indoors, and outdoors
		Ineffective for motion-backgrounded and changing length GOP videos
		Sensitive against the compression and noise
			For de-interlaced uncompressed videos:
			DA = 100%
			For MPEG compressed videos:
			DA = 97%, 96.1%, and 93.3% at bit rate 9, 6, and 3 Mbps, respectively

[248]	Double-quantization (DQ) analysis VPF	localization of MPEG2 compressed video frame forgery Dataset used includes Selected videos of DERF (cropped-resolution = 720 × 576px and MPEG2-VBR-encoded using FFMPEG software) Ineffective for changing length GOP videos	AUC Ranges from 0.63 to 0.98 for different values of Q1 and Q2

Table 15 (continued)

References	Technique	Description with dataset	Performance

[249]	Video Compression Properties and HOG features	Detects spatial- andtemporal video forgeries
		Dataset includes 6000-frames from-15-videos for spatial-forgery and 150-GOPs (size = 12 frames each) for temporal forgery
		Forgery localization is not done
			For spatial forgery:
			DA = 94.65%
			For temporalforgery:
			DA = 91.75%

[250]	Noise residue
	GMM
	Bayesian classifier
	EM algorithm
	statistical classification scheme
		Detects temporal copy-paste Inpainting and example-based texture-synthesis inpainting
		Used personal dataset with MPEG-2 coded video
		Noise residue extraction is complicated
		Sensitive against illumination and the quantization noise
		Appropriate only for videos having static background & fixed GOP length
			For TCP:
			RR = 57.76%
			PR = 96.61%
			MR = 44.23%
			FPR = 3.38%
			For ETS:
			RR = 74.58%
			PR = 92.80%
			MR = 25.41%
			FPR = 7.195%

[251]	Motion residue
	Markov models
	SVM
		Detects blind video forgery
		Dataset includes 20 videos from different datasets
		Ineffective for motion-backgrounded and changing length GOP videos
			For 324-features:
			DA = 87.09%
			PR = 89%
			RR = 86%
			For 81 features:
			DA = 87.2%
			PR = 89%
			RR = 87%
			ROC curve
			AUC = 0.9479

[252]	LADCT
	Weighted average-technique
	SPN
	Wiener filter
		Detects TCP-inpainting-video forgery
		Used customized-dataset
		Ineffective for motion-back-grounded video
			For seq-1:
			DA = 98.22%
			FPR = 7.78%%
			For seq-2:
			DA = 93.28%
			FPR = 6.72%
			For seq-3:
			DA = 98.34%
			FPR = 1.66%

Table 15 (continued)

References	Technique	Description with dataset	Performance

[253]	SPN
	Local noise variation
	Pixel- correlation examination
	MG-detector
	FMG-detector
		Detects upscale and splicing video forgery
		Videos from SULFA&VTL datasets (MPEG2&4-encoded)
		Ineffective for motion-backgrounded and changing length GOP videos
			DA = 99% (at QF = 80to100)
			DA = 98 (at QF = 60)

[254]	Sensor pattern noise (SPN) Minimum average correlation energy (MACE)-filter	Detects surveillance videos forgery created the dataset including 480 HQ videos taken by four surveillance cameras (resolution = 640 × 480, FR = 10 Hz, BR = 8Mbps and recording time = 30 s (MPEG-4-coded videos) (240 RGB videos, 240 infrared videos) Ineffective for motion-backgrounded video	True-positive rate (TPR) = 79.86% False-positive rate (FPR) = 0.45%

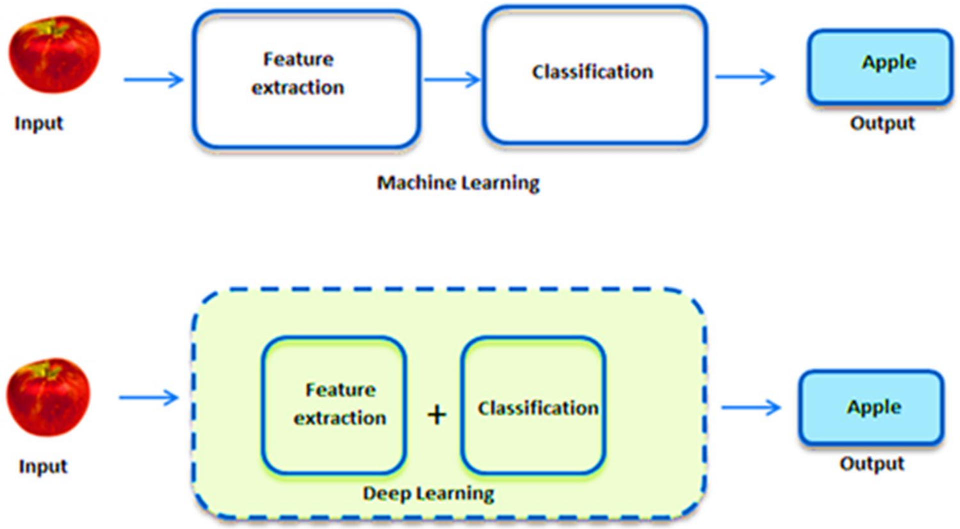


Fig. 20 Deep learning vs Machine learning

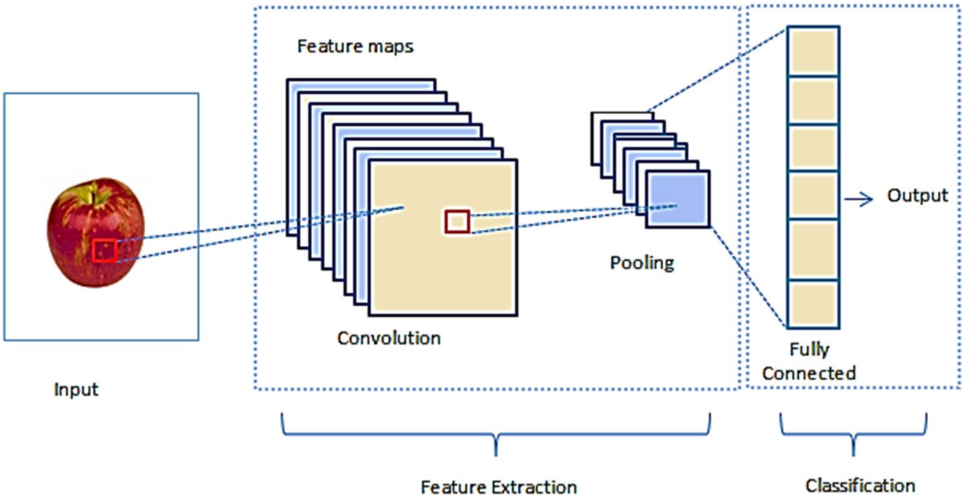


Fig. 21 Framework of convolutional neural network (CNN)

The following section presented the literature review of various sub categories of image and video forensics. The deep learning-based approaches to both image and video forensics have also been discussed in the separate section keeping in view its importance in the future research. After an in-depth literature review and comparative study, the survey finally provided future directions for researchers, pointing out the challenges in the field of image and video forensics, which are the focus of attention in the future, thus providing ideas for researchers to conduct future research.

Table 16 Comparative study of deep learning-based image forgery analysis techniques

References	Technique	Description with dataset	Performance
[255]	CNN	Detects median filtering and cut-paste forgeries	Detection accuracy =85.14%
	Median filter residuals	Dataset used comprises of 15,352 images from NRCS Photo Gallery, BOSS base 1.01, UCID, Dresden, BOSS RAW)	
[256]	Stacked auto encoders (SAE)	Detects cut-paste and copy-move forgeries	Detection accuracy =91.09%
	3-level 2D Daubechies wavelet decomposition	Dataset used includes CASIA v1.0, CASIA v2.0 and Columbia	
[257]	CNN	Detects Gaussian blurring, median filtering and resampling forgeries	Detection accuracy =99.10%
	Prediction error filters	Dataset used comprises images collected from 12 different camera models	
[222]	Auto-encoder	Detects cut-paste and copy-move forgery	*F*-Measure =0.41 (without post-processing) =0.37 (with post-processing)
	Noise residual features	Dataset used comprises images six smartphones and one camera	
[223]	CNN	Detects median filtering and cut-paste forgeries	Accuracy =98.04% (for CASIA v1.0)=97.83% (for CASIA v2.0) =96.38% (for DVMM)
	Hierarchical representation from color images	Dataset used include CASIA v1.0, CASIA v2.0, Columbia and gray DVMM	
[258]	CNN Camera model features	Detects cut-paste forgeries Dataset used is Dresden image database	Localization accuracy=82% Detection accuracy=81%
[259]	Multi-domain CNN	Detects double JPEG compression and cut-paste forgeries	Accuracy=95%
	R,G,B Features and histogram of DCT	Dataset used include 1338 images from UCID	
[260]	Multi-task fully convolution network (MFCN) Surface probability map and edge probability map	Detects image splicing forgeries Dataset used Columbia, CASIA v1.0, CASIA v2.0, Carvalho	*F*1-Score =0.54 (CASIA v1.0) =0.61 (Columbia) MCC Score=0.52 (CASIA v1.0) =0.47 (Columbia)
[261]	BusterNet VGG16	Detects copy-move forgeries Dataset used CoMoFoD and CASIA v2.0	Accuracy =78%
[262]	RRU-Net Image residuals	Detects cut-paste forgeries Dataset used CASIA and COLUMB	Accuracy=76% *F*-measure (pixel)=0.84 (for CASIA) =0.91 (for COLUMB)
[263]	Mask R-CNN ResNet-101	Detects cut-paste and copy-move forgeries Dataset used COVER and Columbia	Average Precision=93% (for Cover) =97% (for Columbia)

Author contributions SYED TUFAEL NABI: Writing—original draft, Data Collection, Relevant Articles Collection. Munish Kumar and Paramjeet Singh: Review Protocol, Testing, Writing—review & editing. Naveen Aggarwal and Krishan Kumar: Writing—review & editing.

Declarations

Conflict of Interest All the authors declare that they have no conflict of interest in this work.

References

1. Farid, H.: Digital doctoring: how to tell the real from the fake. Significance **3**(4), 162–166 (2006)
2. Zhu, B.B., Swanson, M.D., Tewfik, A.H.: When seeing isn't believing. IEEE Signal Process. Mag. **21**(2), 40–49 (2004)
3. "Photo tampering throughout history," (2012). http://www.fourandsix.com/photo-tampering-history/
4. Redi, J.A., Taktak, W., Dugelay, J.-L.: Digital image forensics: a booklet for beginners. Multimed. Tools ppl. **51**(1), 133–162 (2010)

5. Parveen, A., Tayal, A.: An algorithm to detect the forged part in an image. In: Proceedings of 2nd International Conference on Communication and Signal Processing, 1486–1490 (2016)
6. Yan, C., Li, Z., Zhang, Y., Liu, Y., Ji, X., Zhang, Y.: Depth Image denoising using nuclear norm and learning graph model. ACM Trans. Multimed. Comput. Commun. Appl. **16**(4), 1–17 (2021)
7. Zheng, H., Yong, H., Zhang, L. Deep convolutional dictionary learning for image de-noising. In: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 2021, 630–641 (2021)
8. Shi, Q., Tang, X., Yang, T., Liu, R., Zhang, L.: Hyperspectral image de-noising using a 3-D attention denoising network. IEEE Trans. Geosci. Remote Sens., pp. 1–16 (2021)
9. Yan, C., Hao, Y., Li, L., Yin, J., Liu, A., Mao, Z., Gao, X.: Task-adaptive attention for image captioning. IEEE Trans. Circ. Syst. Video Technol., 1–1 (2021)
10. Quan, Y., Chen, Y., Shao, Y., Teng, H., Xu, Y., Ji, H.: Image de-noising using complex-valued Deep CNN. Pattern Recognit. **111**, 107639 (2020)
11. Lan, R., Zou, H., Pang, C., Zhong, Y., Liu, Z., Luoet, X.: Image denoising via deep residual convolutional neural networks. SIViP **15**, 1–8 (2021)
12. Cheng, S., Wang, Y., Huang, H., Liu, D., Fan, H., Liu, S.: NBNet: Noise basis learning for image de-noising with subspace projection. In: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), pp. 4896–4906 (2021)
13. Jaseela, S., Nishadha, S.G.: Survey on copy move image forgery detection techniques. Int. J. Comput. Sci. Trends Technol. (IJCST) **4**(1), 87–91 (2016)
14. Fadl, S.M., Semary, N.O.A., Hadhoud, M.M.: Copy–rotate–move forgery detection based on spatial domain. In: Proceedings of 9th International Conference on Computer Engineering and Systems, pp. 136–141 (2014)
15. Ren, X.: An optimal image thresholding using genetic algorithm. Int. Forum Comput. Sci.-Technol. Appl. **1**, 169–172 (2009)
16. Hussain, M., Muhammad, G., Saleh, S.Q., Mirza, A.M., Bebis, G.: Copy–move image Forgery detection using multi-resolution weber descriptors. In: Proceedings of 8th International Conference on Signal Image Technology and Internet Based Systems, pp. 1570–1577 (2013)
17. Agarwal, V., Mane, V.: Reflective SIFT for improving the detection of copy–move image forgery. In: Proceedings of 2nd International Conference on Research in Computational Intelligence and Communication Networks, pp. 84–88 (2016)
18. Amerini, I., Ballan, L., Caldelli, R., Bimbo, A.D., Serra, G.: A SIFT-Based forensic method for copy–move attack detection and transformation recovery. IEEE Trans. Inf. Forensics Secur. **6**(3), 1099–1110 (2011)
19. He, Z., Lu, W., Sun, W., Huang, J.: Digital image splicing detection based on markov features in DCT and DWT domain. Pattern Recogn. **45**(12), 4292–4299 (2012)
20. Shahroudnejad, A., Rahmati, M.: Copy–move forgery detection in digital images using affine-SIFT. In: Proceedings of 2nd International Conference of Signal Processing and Intelligent Systems, pp. 1–5 (2016)
21. Lin, S.D., Wu, T.: An integrated technique for splicing and copy–move forgery image detection. In: Proceedings of 4th International Conference on Image and Signal Processing, 2:1086–1091 (2011)
22. Ting, Z., Rang-ding, W.: Copy–move forgery detection based on SVD in digital image. In: Proceedings of 2nd International Conference on Image and Signal Processing, 1–5 (2009)
23. Koppanati, R.K., Kumar, K.: P-MEC: polynomial congruence-based multimedia encryption technique over cloud. IEEE Consum. Electron. Mag. **10**(5), 41–46 (2021)
24. Yan, C., Gong, B., Wei, Y., Gao, Y.: Deep multi-view enhancement hashing for image retrieval. IEEE Trans. Pattern Anal. Mach. Intell. **43**, 1 (2020)
25. Chaudhuri, U., Banerjee, B., Bhattacharya, A.: Siamese graph convolutional network for content based remote sensing image retrieval. Comput. Vis. Image Underst. **184**, 22–30 (2019)
26. Tolias, G., Sicre, R., Jegou, H.: Particular object retrieval with ´ integral max-pooling of CNN activations. In: ICLR, pp. 1–12 (2015)
27. Xu, J., Wang, C., Qi, C., Shi, C., Xiao, B.: Unsupervised part-based weighting aggregation of deep convolutional features for image retrieval. In: AAAI, 2018, **32**(1), pp. 7436–7443 (2018)
28. Liu, H., Wang, R., Shan, S., Chen, X.: Deep supervised hashing for fast image retrieval. In: CVPR, 2016, pp. 2064–2072 (2016)
29. Yan, K., Wang, Y., Liang, D., Huang, T., Tian, Y.: CNN vs. SIFT for image retrieval: alternative or complementary? In: ACM MM, 2016, 407–411 (2016)
30. Liu, L., Ouyang, W., Wang, X., Fieguth, P., Chen, J., Liu, X., Pietikainen, M.: Deep learning for generic object detection: a survey. Int. J. Comput. Vis. **128**(2), 261–318 (2020)
31. Sridevi, M., Mala, C., Sandeep, S.: Copy–move image forgery detection in a parallel environment. In: Proceedings of CS & IT Computer Science Conference Proceedings (CSCP), pp. 19–29 (2012)
32. Kang, L., Cheng, X.P.: Copy–move forgery detection in digital image. In: Proceedings of 3rd International Congress on Image and Signal Processing (CISP), vol. 5, pp. 2419–2421 (2010)
33. Li, H., Luo, W., Qiu, X., Huang, J.: Image forgery localization via integrating tampering possibility maps. IEEE Trans. Inf. Forensics Secur. **12**, 1–13 (2017)
34. Al-Sanjary, O.I., Sulong, G.: Detection of video forgery: A review of literature. J. Theoret. Appl. Inf. Technol. **74**(2), 217–218 (2015)
35. Ng, T., Chang, S.: A data set of authentic and spliced image blocks (2004)
36. Hsu, Y., Chang, S.: Detecting image splicing using geometry invariants and camera characteristics consistency. In: 2006 IEEE International Conference on Multimedia and Expo, 549–552 (2006)
37. Jegou, H., Douze, M., Schmid, C.: Hamming Embedding and Weak geometry consistency for large scale image search. In: Proceedings of the 10th European conference on Computer vision, October, 2008 (2008)
38. Gloe, T., Bohme, R.: The dresden image database for benchmarking digital image forensics. J. Digital Forensic Pract. **3**(2–4), 150–159 (2010)
39. Amerini, I., Ballan, L., Caldelli, R., Del Bimbo, A., Serra, G.: A SIFT-based forensic method for copy-move attack detection and transformation recovery. IEEE Trans. Inf. Forensics Secur. **6**(3), 1099–1110 (2011)
40. Bas, P., Filler, T., Pevny, T.: (2011). May Break our steganographic system: the ins and outs of organizing BOSS. In: International Workshop on Information Hiding, pp. 59–70 (2011)
41. Bianchi, T., Piva, A.: Image forgery localization via block-grained analysis of JPEG artifacts. IEEE Trans. Inf. Forensics Secur. **7**(3), 1003–1017 (2012)
42. Christlein, V., Riess, C., Jordan, J., Riess, C., Angelopoulou, E.: An evaluation of popular copy-move forgery detection approaches. IEEE Trans. Inf. Forensics Secur. **7**(6), 1841–1854 (2012)
43. Tralic, D., Zupancic, I., Grgic, S., Grgic, M.: CoMoFoD—New database for copy–move forgery detection. In: International Symposium Electronics in Marine, pp. 49–54 (2013)
44. Dong, J., Wang, W., Tan, T.: CASIA image tampering detection evaluation database. In: 2013 IEEE China Summit and International Conference on Signal and Information Processing (2013)

45. Amerini, I., Ballan, L., Caldelli, R., Del-Bimbo, A., Del-Tongo, L., Serra, G.: Copy-move forgery detection and localization by means of robust clustering with J-Linkage. Signal Process. Image Commun. **28**(6), 659–669 (2013)
46. Cozzolino, D., Poggi, G., Verdoliva, L.: Copy-move forgery detection based on PatchMatch. In: 2014 IEEE International Conference on Image Processing (ICIP), pp. 5312–5316 (2014)
47. Ardizzone, E., Bruno, A., Mazzola, G.: Copy-move forgery detection by matching triangles of keypoints. IEEE Trans. Inf. Forensics Secur. **10**, 2084–2094 (2015)
48. Dang-Nguyen, D.T., Pasquini, C., Conotter, V., Boato, G.: RAISE- A raw images dataset for digital image forensics. In: Proc. 6th ACM Multimed. Syst. Conf. MMSys 2015, pp. 219–224 (2015)
49. Wattanachote, K., Shih, T.K., Chang, W.-L., Chang, H.-H.: Tamper detection of JPEG image due to seam modifications. IEEE Trans. Inf. Forensics Secur. **10**(12), 2477–2491 (2015)
50. Silva, E., Carvalho, T., Ferreira, A.: A. Rocha, going deeper into copy- move forgery detection: Exploring image telltales via multi-scale analysis and voting processes. J. Vis. Commun. Image Represent. **29**, 16–32 (2015)
51. Zampoglou, M., Papadopoulos, S., Kompatsiaris, Y.: Detecting image splicing in the wild (WEB). In: 2015 IEEE International Conference on Multimedia & Expo Workshops (ICMEW), pp. 1–6 (2015)
52. Wen, B., Zhu, Y., Subramanian, R., Ng, T.T., Shen, X., Winkler, S.: COVERAGE—a novel database for copy-move forgery detection. In: Proc. - Int. Conf. Image Process. ICIP.2016-August, 161–165 (2016)
53. National Inst. of Standards and Technology (2016). The 2016 Nimble challenge evaluation dataset, https://www.nist.gov/itl/iad/mig/nimble-challenge, (2016)
54. Korus, P., Huang, J.J.: Multi-scale analysis strategies in PRNU-based tampering localization. IEEE Trans. Inf. Forensics Secur. **12**(4), 809–824 (2017)
55. Guan, H., Kozak, M., Robertson, E., Lee, Y., Yates, A., Delgado, A., Zhou, D., Kheyrkhah, T., Smith, J., Fiscus, J.: MFC Datasets: Large-Scale Benchmark Datasets for Media Forensic Challenge Evaluation, IEEE Winter Conference on Applications of Computer Vision (WACV 2019), Waikola, HI, [online], https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=927035. (2019)
56. Novozámský, A., Mahdian, B., Saic, S.: IMD2020: a large-scale annotated dataset tailored for detecting manipulated images. In: 2020 IEEE Winter Applications of Computer Vision Workshops (WACVW), pp. 71–80 (2020)
57. Qadir, G., Yahahya, S., Ho, A.: Surrey University Library for Forensic Analysis (SULFA). In: Proceedings of the IETIPR 2012, 3–4 July, London (2012)
58. Bestagini, P., Milani, S., Tagliasacchi, M., Tubaro, S.: Local tampering detection in video sequences. In: 2013 IEEE 15Th International Workshop on Multimedia Signal Processing (MMSP). IEEE, pp. 488–493 (2013)
59. Al-Sanjary, O.I., Ahmed, A.A., Sulong, G.: Development of a video tampering dataset for forensic investigation. Forensic Sci. Int. **266**, 565–572 (2016)
60. Chen, S., Tan, S., Li, B., Huang, J.: Automatic detection of object-based forgery in advanced video. IEEE Trans. Circ. Syst. Video Tech. **26**(11), 2138–2151 (2016)
61. D'Avino, D., Cozzolino, D., Poggi, G., Verdoliva, L.: Autoencoder with recurrent neural networks for video forgery detection. Electron. Image **2017**(7), 92–99 (2017)
62. Ulutas, G., Ustubioglu, B., Ulutas, M., Nabiyev, V.V.: Frame duplication detection based on bow model. Multimed. Syst. **24**(5), 549–567 (2018)
63. D'Amiano, L., Cozzolino, D., Poggi, G., Verdoliva, L.: A patch match-based dense-field algorithm for video copy-move detection and localization. IEEE Trans. Circ. Syst. Video Technol. **29**, 669–682 (2018)
64. Panchal, H.D., Shah, H.B.: Video tampering dataset development in temporal domain for video forgery authentication. Multimed. Tools Appl. **79**, 24553–24577 (2020)
65. Ferreira, W.D., Ferreira, C.B., Junior, G.D., Soares, F.: A review of digital image forensics. Comput. Electr. Eng. **85**, 106685 (2020)
66. Birajdar, G.K., Mankar, V.H.: Digital image forgery detection using passive techniques: a survey. Digit. Investig. **10**(3), 226–245 (2013)
67. Farid, H.: A survey of image forgery detection techniques. IEEE Signal Process. Mag. **26**, 16–25 (2009)
68. Qazi, T., Hayat, K., Khan, S.U., Madani, S.A., Khan, I.A., Kołodziej, J., Li, H., Lin, W., Yow, K.C., Xu, C.-Z.: Survey on blind image forgery detection. Image Process IET **7**, 660–670 (2013)
69. Ansari, M.D., Ghrera, S.P., Tyagi, V.: Pixel-based image forgery detection: a review. IETE J. Educ. **55**, 40–46 (2014)
70. Lanh, T.V.L.T., Van-Chong, K.-S., Chong, K.-S., Emmanuel, S., Kankanhalli, M.S.: A survey on digital camera image forensic methods. In: 2007 IEEE International Conference on Multimedia and Expo, pp. 16–19 (2007)
71. Mahdian, B., Saic, S.: A bibliography on blind methods for identifying image forgery. Signal Process. Image Commun. **25**, 389–399 (2010)
72. Warif, N.B.A., Wahab, A.W.A., Idris, M.Y.I.: Copy-move forgery detection: survey, challenges and future directions. J. Netw. Comput. Appl. **75**, 259–278 (2016)
73. Christlein, V., Riess, C.C., Jordan, J., Riess, C.C., Angelopoulou, E.: An evaluation of popular copy-move forgery detection approaches. IEEE Trans. Inf. Forensics Secur. **7**, 1841–1854 (2012)
74. Friedman, G.L.: Trustworthy digital camera: restoring credibility to the photographic image. IEEE Trans. Consum. Electron. **39**(4), 905–910 (1993)
75. Blythe, P., Fridrich, J.: Secure digital camera. In: Proceedings of the Digital Forensic Research Workshop (DFRWS '04), pp. 17–19 (2004)
76. Rivest, R.L., Shamir, A., Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM **21**(2), 120–126 (1978)
77. Menezes, A.J., VanstoneOorschot, S.S.A.P.C.V.: Handbook of Applied Cryptography, 1st edn. CRC Press, Boca Raton (1996)
78. Cox, I.J., Miller, M.L., Bloom, J.A.: Digital Watermarking. Morgan Kaufmann Publishers, Berlin (2002). ISBN 978-1-55860-714-9
79. Barni, M., Bartolini, F.: Watermarking systems engineering: enabling digital assets security and other applications. In: Signal Processing and Communications. Marcel Dekker (2004)
80. Cox, I.J., Miller, M.L., Bloom, J., Fridrich, J., Kalker, T.: Digital Watermarking and Steganography, 2nd edn. Morgan Kaufmann, San Francisco (2008)
81. Carneiro-Tavares, J.R., Madeiro-Bernardino-Junior, F.: Word-hunt: a LSB steganography method with low expected number of modifications per pixel. IEEE Lat. Am. Trans. **14**(2), 1058–1064 (2016)
82. Laskar, S.A., Hemachandran, K.: Steganography based on random pixel selection for efficient data hiding. Int. J. Comput. Eng. Technol. (IJCET) **4**, 31–44 (2013)
83. Bhattacharyya, S.: Study and analysis of quality of service in different image-based steganography using Pixel Mapping

Method (PMM). Int. J. Appl. Inf. Syst. (IJAIS) **2**(7), 42–57 (2012)

84. Qazanfari, K., Safabakhsh, R.: A new steganography method which preserves histogram: generalization of LSB++. Inf. Sci. (NY) **277**, 90–101 (2014)
85. Shobana, M., Manikandan, R.: Efficient method for hiding data by pixel intensity. Int. J. Eng. Technol. (IJET) **5**(1), 74–80 (2013)
86. Ni, J., Hu, X., Shi, Y.Q.: Efficient JPEG steganography using domain transformation of embedding entropy. IEEE Signal Process. Lett. **25**(6), 773–777 (2018)
87. Ghoshal, N., Mandal, J.K.: A steganographic scheme for color image authentication (SSCIA), In: Proceedings of the international conference on recent trends in information technology, ICRTIT 2011, pp. 826–31 (2011)
88. Ibaida, A., Khalil, I.: Wavelet-Based ECG steganography for protecting patient confidential information in point-of-Care systems. IEEE Trans. Biomed. Eng. **60**(12), 3322–3330 (2013)
89. Al-dmour, H., Al-ani, A.: A steganography embedding method based on edge identification and XOR coding. Expert Syst. Appl. **46**, 293–306 (2016)
90. Jero, S.E., Ramu, P.: Curvelets-based ECG steganography for data security. Electron. Lett. **52**(4), 283–285 (2016)
91. Tayan, O., Kabir, M.N., Alginahi, Y.M.: A hybrid digital-signature and zero-watermarking approach for authentication and protection of sensitive electronic documents. Sci. World J. **8**, 1–15 (2014)
92. Subramanya, S.R., Yi, B.K.: Digital Signatures. IEEE Potentials **25**(2), 5–8 (2006)
93. Lee, W.B., Chen, T.H.: A public verifiable copy protection technique for still images. J. Syst. Softw. **62**(3), 195–204 (2002)
94. Damara-Ardy, R., Indriani, O.R., Sari, C.A., Setiadi, D.R.I.M., Rachmawanto, E.H.: Digital image signature using triple protection cryptosystem (RSA, Vigenere, and MD5). In: 2017 International Conference on Smart Cities, Automation & Intelligent Computing Systems (ICON-SONICS), pp. 87–92 (2017)
95. Meena, K.B., Tyagi, V.: A Deep Learning based Method for Image Splicing Detection. J. Phys. Conf. Ser. **1714**, 012038 (2021)
96. Pramanik, S., Bandyopadhyay, S.K., Ghosh, R.: Signature image hiding in color image using steganography and cryptography based on digital signature, concepts. In: 2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), pp. 665–669 (2020)
97. Moin, S.S., Islam, S.: Benford's law for detecting contrast enhancement. In: 2017 Fourth International Conference on Image Information Processing (ICIIP), pp. 1–4 (2017)
98. Friedman, G.L.: The trustworthy digital camera: restoring credibility to the photographic image. IEEE Trans. Consum. Electron. **39**(4), 905–910 (1993)
99. Rey, C., Dugelay, J.-L.: A survey of watermarking algorithms for image authentication. EURASIP J. Adv. Signal Proc. **6**, 613–621 (2002)
100. Langelaar, G.C., Setyawan, I., Lagendijk, R.L.: Watermarking digital image and video data. A state-of-the-art overview. IEEE Signal Proc. Mag. **17**(5), 20–46 (2000)
101. Tafti, A.P., Malakooti, M.V., Ashourian, M., Janosepah, S.: Digital image forgery detection through data embedding in spatial domain and cellular automata. In: 7th International Conference on Digital Content, Multimedia Technology and its Applications (IDCTA), pp. 11–15 (2011)
102. Bamatraf, A., Ibrahim, R., Najib, M., Salleh, M.: A new digital watermarking algorithm using combination of least significant bit (LSB) and inverse bit. J. Comput. **3**(4), 2151–9617 (2011)
103. Sharma, P.K., Rajni: Analysis of image watermarking using least significant bit algorithm. Int. J. Inf. Sci. Tech. (IJIST) **2**(4), 666–673 (2012)
104. Bhattacharya, S.: Additive watermarking in optimized digital image. In: IEEE Beacon, IEEE (Delhi Section), **79**(1) (2012)
105. Bose, A., Maity, S.P.: Spread spectrum watermark detection on degraded compressed sensing. IEEE Sens. Lett. **1**(5), 1–4 (2017)
106. Urvoy, M., Goudia, D., Autrusseau, F.: Perceptual DFT watermarking with improved detection and robustness to geometrical distortions. IEEE Trans. Inf. Forensics Secur. **9**(7), 1108–1119 (2014)
107. Chaturvedi, N., Basha, S.J.: Comparison of Digital Image watermarking Methods DWT & DWT- DCT on the Basis of PSNR, International Journal of Innovative Research in Science, Engineering and Technology IJIRSET www.ijirset.com, *1* (2):147 (2012)
108. Ernawan, F., Kabir, M.N.: A robust image watermarking technique with an optimal DCT-psychovisual threshold. IEEE Access **6**, 20464–20480 (2018)
109. Makbol, N.M., Khoo, B.E., Rassem, T.H.: Block-based discrete wavelet transform-singular value decomposition image watermarking scheme using human visual system characteristics. IET Image Proc. **10**(1), 34–52 (2016)
110. Mansouri, A., Aznaveh, A.M., Azar, F.T.: SVD-based digital image watermarking using complex wavelet transform. Sadhana **34**(3), 393–406 (2009)
111. Bapat, K.S., Totla, R.V.: Comparative analysis of watermarking in digital images using DCT & DWT. Int. J. Sci. Res. Publ. (IJSRP) **3**(2), 1 (2013)
112. Mathai, N.J., Kundur, D., Sheikholeslami, A.: Hardware implementation perspectives of digital video watermarking algorithms. IEEE Trans. Signal Process. **51**(4), 925–938 (2003)
113. Kougianos, E., Mohanty, S.P., Mahapatra, R.N.: Hardware assisted watermarking for multimedia. Comput. Electr. Eng. **35**(2), 339–358 (2009)
114. Zhang, X., Wang, S.: Fragile watermarking with error free restoration capability. IEEE Trans. Multimed. **10**(8), 1490–1499 (2008)
115. Chang, J., Chen, B., Tsai, C.: LBP-based fragile watermarking scheme for image tamper detection and recovery. In: International Symposium on Next Generation Electronics (Kaohsiung, 2013), pp. 173–176 (2013)
116. Doyoddorj, M., Rhee, K.H.: Multidisciplinary research and practice for information systems. In: IFIP WG 8.4, 8.9/TC 5 International Cross-Domain Conference and Workshop on Availability, Reliability, and Security, CD-ARES 2012, Prague, Czech Republic, August 20–24, 2012. Proceedings (ed. by (2012)
117. Quirchmayer, G., Basl, J., You, I., Xu, L., Weippl, E.: Multidisciplinary Research and Practice for Informations Systems. Springer Publishing (2012)
118. Tong, X., Liu, Y., Zhang, M., Chen, Y.: A novel chaos-based fragile watermarking for image tampering detection and self-recovery. Signal Process. Image Commun. **28**(2), 301–308 (2013)
119. Huo, Y., He, H., Chen, F.: Alterable-capacity fragile watermarking scheme with restoration capability. Opt. Commun. **285**(7), 1759–1766 (2012)
120. Wang, W., Men, A., Yang, B.: A feature-based semi-fragile watermarking scheme in DWT domain. In: 2010 2nd IEEE International Conference on Network Infrastructure and Digital Content, pp. 768–772 (2010)
121. Yu, M., Wang, J., Jiang, G., Peng, Z., Shao, F., Luo, T.: New fragile watermarking method for stereo image authentication with localization and recovery. AEU Int. J. Electron. Commun. **69**(1), 361–370 (2015)
122. Lin, S.D., Kuo, Y.C., Huang, Y.H. An image watermarking scheme with tamper detection and recovery. In: First International Conference on Innovative Computing, Information and Control-Volume I (ICICIC'06), vol. 3, pp. 74–77 (2006)

123. Zhang, H., Wang, C., Zhou, X.: Fragile watermarking for image authentication using the characteristic of SVD. Algorithms **10**(1), 27 (2017)
124. Li, C., Wang, Y., Ma, B., Zhang, Z.: A novel self-recovery fragile watermarking scheme based on dual-redundant-ring structure. Comput. Electr. Eng. **37**(6), 927–940 (2011)
125. Bravo-Solorio, S., Nandi, A.K.: Secure fragile watermarking method for image authentication with improved tampering localization and self-recovery capabilities. Sign. Proces **91**(4), 728–739 (2011)
126. Eswaraiah, R., Reddy, E.S.: ROI-based fragile medical image watermarking technique for tamper detection and recovery using variance. In: Seventh International Conference on Contemporary Computing (IC3), pp. 553–558 (2014)
127. He, H., Chen, F., Tai, H., Member, S., Kalker, T., Zhang, J.: Performance analysis of a block-neighborhood-based self-recovery fragile watermarking scheme. IEEE Trans. Inf. Forensics Secur **7**(1), 185–196 (2012)
128. Qin, C., Ji, P., Zhang, X., Dong, J., Wang, J.: Fragile image watermarking with pixel-wise recovery based on overlapping embedding strategy. Signal Process. **138**, 280–293 (2017)
129. Zhu, X.S., Sun, Y., Meng, Q.H., Sun, B., Wang, P., Yang, T.: Optimal watermark embedding combining spread spectrum and quantization. EURASIP J. Adv. Signal Process. **1**, 74 (2016)
130. Molina-Garcia, J., Garcia-Salgado, B., Ponomaryov, V., Reyes-Reyes, R., Sadovnychiy, S., Cruz-Ramos, C.: An effective fragile watermarking scheme for color image tampering detection and self-recovery. Signal Process. Image Commun. **81**, 115725 (2020)
131. Cao, X., Fu, Z., Sun, X.: (2016). A privacy-preserving outsourcing data storage scheme with fragile digital watermarking-based data auditing. J. Electr. Comput. Eng., pp. 1–7 (2016)
132. Abbas, N.H., Ahmad, S.M.S., Ramli, A.R.B., Parveen, S.: A multi-purpose watermarking scheme based on hybrid of lifting wavelet transform and Arnold transform. In: International Conference on Multidisciplinary in IT and Communication Science and Applications (2016)
133. Chen, F., He, H., Tai, H.M., Wang, H.: Chaos-based self-embedding fragile watermarking with flexible watermark payload. Multimed. Tool Appl. **72**(1), 41–56 (2014)
134. Chamlawi, R., Usman, I., Khan, A.: Dual watermarking method for secure image authentication and recovery. In: IEEE 13th International Multitopic Conference (Islamabad, 2009), pp. 1–4 (2009)
135. Yu, X., Wang, C., Zhou, X.: Review on semi-fragile watermarking algorithms for content authentication of digital images. Future Internet **9**(4), 56 (2017)
136. Wang, W., Men, A., Yang, B.: A feature-based semi-fragile watermarking scheme in DWT domain. In: 2nd IEEE International Conference on Network Infrastructure and Digital Content (Beijing, 2010), 768–772 (2010)
137. Qi, X., Xin, X.: A singular-value-based semi-fragile watermarking scheme for image content authentication with tamper localization. J. Vis. Commun. Image Represent **30**, 312–327 (2015)
138. Huo Y., He H, Chen F (2013). Semi-fragile watermarking scheme with discriminating general tampering from collage attack, *Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (Kaohsiung, 2013),* 1–6.
139. Li Y, Du L (2014). Semi-fragile watermarking for image tamper localization and self-recovery, *Proceedings 2014 IEEE International Conference on Security, Pattern Analysis, and Cybernetics (SPAC) (Wuhan, 2014),* 328–333.
140. Ekici, O., Sankur, B., Coşkun, B., Naci, U., Akcay, M.: Comparative evaluation of semifragile watermarking algorithms. J. Electron. Imaging **13**(1), 209 (2004)
141. Jamal, S.S., Khan, M.U., Shah, T.: Awatermarking technique with chaotic fractional S-box transformation. Wirel. Pers. Commun. **90**(4), 2033–2049 (2016)
142. Wang, S., Zheng, D., Zhao, J., Tam, W.J., Speranza, F.: Adaptive watermarking and tree structure-based image quality estimation. IEEE Trans. Multimed. **6**(2), 331–324 (2014)
143. Shieh, J.M., Lou, D.C., Chang, M.C.: A semi-blind digital watermarking scheme based on singular value decomposition. Comput. Stand. Interfaces **28**(4), 428–440 (2006)
144. Hsia, S.C., Jou, I.C., Hwang, S.M.: A gray level watermarking algorithm using double layer hidden. ICE Trans. Fund. Electron. ommun. Comput. Sci. **85**(2), 436–471 (2002)
145. Rao, R.S.P, Kumar P.R.: Digital Signature based Image Watermarking using Ga and Pso. Int. J. Eng. Res. Technol. (IJERT), *6* (6), (2017)
146. Singh, H.V., Singh, A.K., Yadav, S., Mohan, A.: DCT based secure data hiding for intellectual property right protection. CSI Trans. ICT **2**(3), 163–168 (2014)
147. Chen, T., Lu, H.: Robust spatial LSB watermarking of color images against JPEG compression. In: IEEE Fifth International Conference on Advanced Computational Intelligence (ICACI) (Nanjing, 2012), 872–875 (2012)
148. Wang, N., Kim, C.: Tamper detection and self-recovery algorithm of color image based on robust embedding of dual visual watermarks using DWT-SVD. In: 9th International Symposium on Communications and Information Technology (Icheon, 2009), 157–162 (2009)
149. Abdulazeez, A.M., Zeebaree, D.Q., Hajy, D.M., Zebari, D.A.: Robust watermarking scheme based LWT and SVD using artificial bee colony optimization. Indones. J. Electric. Eng. Comput. Sci. **21**(2), 1218 (2021)
150. Makbol, N.M., Khoo, B.E., Rassem, T.H.: Security analyses of false positive problem for the SVD-based hybrid digital image watermarking techniques in the wavelet transform domain. Multimed. Tools Appl. **77**, 1–35 (2018)
151. Ambadekar, S.P., Jain, J., Khanapuri, J.: Digital image watermarking through encryption and DWT for copyright protection. In: Recent trends in signal and image processing. Singapore: Springer, 187–195 (2019)
152. Pan-Pan, N., Xiang-Yang, W., Yu-Nan, L., Hong-Ying, Y.: A robust color image watermarking using local invariant significant bitplane histogram. Multimed. Tools Appl. **76**(3), 3403–3433 (2017)
153. Vaidya, S.P., Mouli, P.C.: Adaptive digital watermarking for copyright protection of digital images in wavelet domain. Proc. Comput. Sci. **58**, 233–240 (2015)
154. Wu, H.T., Huang, J.: Reversible image watermarking on prediction errors by efficient histogram modification. Signal Process. **92**(12), 3000–3009 (2012)
155. Peng, F., Li, X., Yang, B.: Adaptive reversible data hiding scheme based on integer transform. Signal Process. **92**(1), 54–62 (2012)
156. Ahmed, B., Gulliver, T.A., alZahir, S.: Image splicing detection using mask-RCNN. SIViP **14**, 1035–1042 (2020)
157. Park, T.H., Han, J.G., Moon, Y.H., Eom, I.K.: Image splicing detection based on inter-scale 2D joint characteristic function moments in wavelet domain. EURASIP J. Image Video Process **30**, 1–10 (2016)
158. Rao, Y., Ni, J.: A deep learning approach to detection of splicing and copy-move forgeries in images. In: 8th IEEE International Workshop Information Forensics Security WIFS (2016)
159. Shen, X., Shi, Z., Chen, H.: Splicing image forgery detection using textural features based on the grey level co-occurrence matrices. IET Image Process. **11**, 44–53 (2017)
160. Bahrami, K., Member, S., Kot, A.C., Li, L., Li, H., Member, S.: Blurred image splicing localization by exposing blur type inconsistency. IEEE Trans. Inf. Forensics Secur **6013**, 1–10 (2015)

161. Kanwal, N., Girdhar, A., Kaur, L., Bhullar, J.S.: Digital image splicing detection technique using optimal threshold based local ternary pattern. Multimed. Tools Appl. **79**, 12829–12846 (2020)
162. Jaiswal, A.K., Srivastava, R.: A technique for image splicing detection using hybrid feature set. Multimed. Tools Appl. **79**(17), 11837–11860 (2020)
163. El-Latif, E.I., Taha, A., Zayed, H.: A passive approach for detecting image splicing using deep learning and Haar Wavelet Transform. Int. J. Comput. Netw. Inf. Secur. **11**, 28–35 (2019)
164. Jaiprakash, S.P., Desai, M.B., Prakash, C.S., Mistry, V.H., Radadiya, K.L.: Low dimensional DCT and DWT feature based model for detection of image splicing and copy-move forgery. Multimed. Tools Appl. **79**, 29977–30005 (2020)
165. Niyishaka, P., Bhagvati, C.: Image splicing detection technique based on Illumination-Reflectance model and LBP. Multimed. Tools Appl. **80**, 2161–2175 (2021)
166. Prabhu-Kavin, B., Ganapathy, S., Suthanthiramani, P., Kannan, A. A modified digital signature algorithm to improve the biomedical image integrity in cloud environment. In: Advances in Computational Techniques for Biomedical Image Analysis, 253–271 (2020)
167. Sharma, V., Jha, S., Bharti, R.K.: Image forgery and it's detection technique: a review. Int. Res. J. Eng. Technol. (IRJET) **3**(3), 756–762 (2016)
168. Yang, B., Sun, X., Guo, H., Xia, Z., Chen, X.: A copy-move forgery detection method based on CMFD-SIFT. Multimed. Tools Appl. **77**, 837–855 (2017)
169. Meena, K.B., Tyagi, V.: A copy-move image forgery detection technique based on tetrolet transform. J. Inf. Secur. Appl. **52**, 2481 (2020)
170. Zhu, Y., Shen, X., Chen, H.: Copy-move forgery detection based on scaled ORB. Multimed. Tools Appl. **75**, 3221–3233 (2016)
171. Huang, D., Huang, C., Hu, W.: Robustness of copy-move forgery detection under high JPEG compression artifacts. Multimed. Tools Appl. **76**(1), 1509–1530 (2017)
172. Islam, A., Long, C., Basharat, A., Hoogs, A.: DOA-GAN: Dual-order attentive generative adversarial network for image copy-move forgery detection and localization. In: 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), pp. 4675–4684 (2020)
173. Zhu, Y., Chen, C., Yan, G., Guo, Y., Dong, Y.: AR-Net: adaptive attention and residual refinement network for copy-move forgery detection. IEEE Trans. Ind. Inf. **16**, 1–1 (2020)
174. Zandi, M., Mahmoudi-Aznaveh, A., Talebpour, A.: Iterative copy-move forgery detection based on a new interest point detector. IEEE Trans. Inf. Forensics Secur. **11**, 2499–2512 (2016)
175. Bi, X., Pun, C.M., Yuan, X.C.: Multi-level dense descriptor and hierarchical feature matching for copy-move forgery detection. Inf. Sci. (Ny) **345**, 226–242 (2016)
176. Silva, E., Carvalho, T., Ferreira, A., Rocha, A.: Going deeper into copy-move forgery detection: exploring image telltales via multi-scale analysis and voting processes. J. Vis. Commun. Image Represent. **29**, 16–32 (2015)
177. Bi, X.L., Pun, C.M., Yuan, X.C.: Multi-scale feature extraction and adaptive matching for copy-move forgery detection. Multimed. Tools. Appl. **77**, 1–23 (2016)
178. Wenchang, S.H.I., Fei, Z., Bo, Q.I.N., Bin, L.: Improving image copy-move forgery detection with particle swarm optimization techniques. China Commun. **13**, 139–149 (2016)
179. Pun, C., Member, S., Yuan, X., Bi, X.: Oversegmentation and feature point matching. IEEE Trans. Inf. Forensics Secur. **10**, 1705–1716 (2015)
180. Wang, X.Y., Li, S., Liu, Y.N., Niu, Y., Yang, H.Y., Zhou, Z.: A new keypoint-based copy-move forgery detection for small smooth regions. Multimed. Tools Appl. **76**(22), 23353–23382 (2016)
181. Li, J., Li, X., Yang, B., Sun, X.: Segmentation-based image copy-move forgery detection scheme. IEEE Trans. Inf. Forensics Secur. **10**(3), 507–518 (2015)
182. Zheng, J., Liu, Y., Ren, J., Zhu, T., Yan, Y., Yang, H.: Fusion of block and keypoints based approaches for effective copy-move image forgery detection. Multidimens. Syst. Signal Process. **27**, 989–1005 (2016)
183. Park, J.Y., Kang, T.A., Moon, Y.H., Eom, I.K.: Copy-move forgery detection using scale invariant feature and reduced local binary pattern histogram. Symmetry **12**, 492 (2020)
184. Niyishaka, P., Bhagvati, C.: Copy-move forgery detection using image blobs and BRISK feature. Multimed. Tools Appl. **79**, 26045–26059 (2020)
185. Tinnathi, S.G.: An efficient copy move forgery detection using adaptive watershed segmentation with AGSO and hybrid feature extraction. J. Vis. Commun. Image Represent. **74**, 1966 (2021)
186. Nguyen, H.C., Katzenbeisser, S.: Robust resampling detection in digital images. I*n*: International Conference on Communications and Multimedia Security, pp. 3–15 (2012)
187. Flenner, A., Peterson, L., Bunk, J., Mohammed, T.M., Nataraj, L., Manjunath, B.S.: Resampling forgery detection using deep learning and A-contrario analysis. Electron. Imaging **7**, 2121–2127 (2018)
188. Vazquez-Padin, D., Perez-Gonzalez, F., Comesana-Alfaro, P.: A random matrix approach to the forensic analysis of upscaled images. IEEE Trans. Inf. Forensics Secur. **12**(9), 2115–2130 (2017)
189. Qiao, T., Zhu, A., Retraint, F.: Exposing image resampling forgery by using linear parametric model. Multimed. Tools Appl. **77**, 1501–1523 (2018)
190. Bayar B, Stamm M.C.: On the robustness of constrained convolutional neural networks to JPEG post-compression for image resampling detection. In: IEEE International Conference on Acoustics Speech Signal Process, pp. 2152–2156 (2017)
191. Lamba, M., Mitra, K.: Multi-patch aggregation models for resampling detection. In: ICASSP 2020—2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp. 2967–2971 (2010)
192. Peng, A., Wu, Y., Kang, X.: Revealing traces of image resampling and resampling antiforensics. Adv. Multimed., pp. 1–13 (2017)
193. Bharathiraja, S., Rajesh Kanna, B.: Anti-forensics contrast enhancement detection (AFCED) technique in images based on laplace derivative histogram. Mob. Netw. Appl. **24**, 1174–1180 (2019)
194. Lin, X., Li, C., Hu, Y.: Exposing image forgery through the detection of contrast enhancement. In: International Conference on Image Process, pp. 4467–4471 (2013)
195. Zhu, N., Deng, C., Gao, X.: Image sharpening detection based on multiresolution overshoot artifact analysis. Multimed. Tools Appl. **76**, 16563–16580 (2017)
196. Stamm, M., Ray, K.J.: Blind forensics of contrast enhancement in digital images. In: Proceedings of International Conference on Image Process ICIP, 3112–3115 (2008)
197. Cao, G., Zhao, Y., Ni, R., Kot, A.C.: Unsharp masking sharpening detection via overshoot artifacts analysis. IEEE Signal Process. Lett. **18**(10), 603–606 (2011)
198. Cao G, Zhao Y, Ni R (2009). Detection of image sharpening based on histogram aberration and ringing artifacts, *2009 IEEE International Conference on Multimedia and Expo.,*1026–1029
199. Ding, F., Zhu, G., Yang, J., Xie, J., Shi, Y.-Q.: Edge perpendicular binary coding for USM sharpening detection. IEEE Signal Process. Lett. **22**(3), 327–331 (2015)

200. Wang, Q., Zhang, R.: Double JPEG compression forensics based on a convolutional neural network. EURASIP J. Inf. Secur. **1**, 23 (2016)
201. Madhusudhan, K.N., Sakthivel, P.: Combining digital signature with local binary pattern-least significant bit steganography techniques for securing medical images. J. Med. Imaging Health Inf. **10**(6), 1288-1293 (6) (2020)
202. Shan, W., Yi, Y., Huang, R., Xie, Y.: Robust contrast enhancement forensics based on convolutional neural networks. Signal Process. Image Commun. **71**, 138–146 (2018)
203. Zhang, C., Du, D., Ke, L., Qi, H., Lyu, S.: Global contrast enhancement detection via deep multi-path network. In: 2018 24th International Conference on Pattern Recognition (ICPR), pp. 2815–2820 (2018)
204. Barni, M., Bondi, L., Bonettini, N., Bestagini, P., Costanzo, A., Maggini, M., Tondi, B., Tubaro, S.: Aligned and non-aligned double JPEG detection using convolutional neural networks. J. Vis. Commun. Image Represent. **49**, 153–163 (2017)
205. Zhang, Y., Thing, V.L.L.: A semi-feature learning approach for tampered region localization across multi-format images. Multimed. Tools Appl. **77**, 25027–25052 (2018)
206. Zeng, X., Feng, G., Zhang, X.: Detection of double JPEG compression using modified DenseNet model. Multimed. Tools Appl. **78**, 8183–8196 (2018)
207. Peng, P., Sun, T., Jiang, X., Xu, K., Li, B., Shi, Y.: Detection of double JPEG compression with the same quantization matrix based on convolutional neural networks. In: 2018 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC., pp. 717–721 (2018)
208. Ahn, W., Nam, S.-H., Son, M., Lee, H.K., Choi, S.: End-to-end double JPEG detection with a 3D convolutional network in the DCT domain. Electron. Lett. **56**, 82–85 (2020)
209. Amerini, I., Uricchio, T., Ballan, L., Caldelli, R. Localization of JPEG double compression through multi-domain convolutional neural networks. In: 2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), 1865-1871 (2017)
210. Verma, V., Singh, D., Khanna, N.: Block-level double JPEG compression detection for image forgery localization. In: arXiv: Image and Video Processing (2020)
211. Lukas, J., Fridrich, J., Goljan, M.: Digital camera identification from sensor pattern noise. IEEE Trans. Inf. Forensics Secur. **2**(1), 205–214 (2006)
212. Bayram, S., Sencar, H.T., Memon, N., Avcibas, I.: Source camera identification based on CFA interpolation. In: IEEE International Conference on Image Processing (ICIP) 2005 (2005)
213. Kharrazi, M., Sencar, H.T., Memon, N.: Blind source camera identification. In: IEEE International Conference on Image Processing (ICIP) 2004 (2004)
214. Taspinar, S., Mohanty, M., Memon, N.: PRNU-based camera attribution from multiple seam-carved images. IEEE Trans. Inf. Forensics Secur. **12**(12), 3065–3080 (2017)
215. Xu, B., Wang, X., Zhou, X., Xi, J., Wang, S.: Source camera identification from image texture features. Neurocomputing **207**, 131–140 (2016)
216. Hsu, Y.-F., Chang, S.-F.: Camera response functions for image forensics: an automatic algorithm for splicing detection. IEEE Trans. Inf. Forensics Secur. **5**(4), 816–825 (2010)
217. Zheng L, Sun T, Shi Y. Q (2014). Inter-frame video forgery detection based on block-wise brightness variance descriptor. In: International workshop on digital watermarking, *Springer,* 18–30.
218. Liu, H., Li, S., Bian, S.: Detecting frame deletion in h. 264 video. In: International Conference on Information Security Practice and Experience, Springer, pp. 262–270 (2014)
219. Yao, H., Ni, R., Zhao, Y.: An approach to detect video frame deletion under anti-forensics. J. Real-Time Image Proc. **16**(3), 751–764 (2019)
220. Shanableh, T.: Detection of frame deletion for digital video forensics. Digit. Invest. **10**(4), 350–360 (2013)
221. Long, C., Smith, E., Basharat, A., Hoogs, A.: A c3d-based convolutional neural network for frame dropping detection in a single video shot. In: 2017 IEEE Conference on computer vision and pattern recognition workshops (CVPRW) IEEE, 1898–1906 (2017)
222. Bayar, B., Stamm, M. C.: A deep learning approach to universal image manipulation detection using a new convolutional layer. In: Proceedings of the 4th ACM Workshop on Information Hiding and Multimedia Security, pp. 5–10 (2016)
223. Cozzolino, D., Verdoliva, L.: Single-image splicing localization through autoencoder-based anomaly detection. In: 2016 IEEE International Workshop on Information Forensics and Security (WIFS), 1–6 (2016)
224. Fadl, S.M., Han, Q., Li, Q.: Authentication of surveillance videos: detecting frame duplication based on residual frame. J Forensic Sci. **63**(4), 1099–1109 (2018)
225. Pandey, R.C., Singh, S.K., Shukla, K.: Passive copy-move forgery detection in videos. In: 2014 International Conference on Computer and Communication Technology (ICCCT). IEEE, pp. 301–306 (2014)
226. Hu, Y., Li, C.T., Wang, Y., Liu, B.B.: An improved fingerprinting algorithm for detection of video frame duplication forgery. Int. J. Digit. Crime Forensics (IJDCF) **4**(3), 20–32 (2012)
227. Lin, G.S., Chang, J.F.: Detection of frame duplication forgery in videos based on spatial and temporal analysis. Int. J. Pattern Recognit. Artif. Intell. **26**(07), 1250017 (2012)
228. Liao, S.Y., Huang, T.Q.: Video copy-move forgery detection and localization based on Tamura texture features. In: 2013 6th International Congress on Image and Signal Processing (CISP), vol. 2, pp. 864–868 (2013)
229. Li, F., Huang, T.: Video copy-move forgery detection and localization based on structural similarity. In: Proceedings of the 3rd International Conference on Multimedia Technology (ICMT 2013 Springer, 63–76 (2014)
230. Chao, J., Jiang, X., Sun, T.: A novel video inter-frame forgery model detection scheme based on optical flow consistency. In: International Workshop on Digital Watermarking. Springer, 267–281 (2012)
231. Kang, X., Liu, J., Liu, H., Wang, Z.J.: Forensics and counter anti-forensics of video inter-frame forgery. Multimed. Tools Appl. **75**(21), 13833–13853 (2016)
232. Stamm, M.C., Lin, W.S., Liu, K.J.R.: Temporal forensics and anti-forensics for motion compensated video. IEEE Trans. Inf. Forensics Sec. **7**(4), 1315–1329 (2012)
233. Wang, Q., Li, Z., Zhang, Z., Ma, Q.: Video inter-frame forgery identification based on consistency of correlation coefficients of gray values. J Comput. Commun. **2**(04), 51 (2014)
234. Aghamaleki, J.A., Behrad, A.: Malicious inter-frame video tampering detection in mpeg videos using time and spatial domain analysis of quantization effects. Multimed. Tools Appl **76**(20), 20691–20717 (2017)
235. Aghamaleki, J.A., Behrad, A.: Inter-frame video forgery detection and localization using intrinsic effects of double compression on quantization errors of video coding. Signal Process. Image Commun. **47**, 289–302 (2016)
236. Wang, W., Farid, H.: Exposing digital forgeries in video by detecting double quantization, In: Proceedings of the 11th ACM Workshop on Multimedia and Security, 39–48 (2009)
237. Wang W, Jiang X, Wang S, Wan M, Sun T (2013). Identifying video forgery process using optical flow, In: International workshop on digital watermarking. Springer, 244–257.

238. Ravi, H., Subramanyam, A.V., Gupta, G., Kumar, B.A.: Compression noise based video forgery detection. In: 2014 IEEE International Conference on Image Processing (ICIP). IEEE, pp. 5352–5356 (2014)
239. Wang, W., Farid, H.: Exposing digital forgeries in video by detecting duplication. In: Proceedings of the 9th Workshop on Multimedia & Security, pp 35–42 (2007)
240. Singh, R.D., Aggarwal, N.: Detection and localization of copy-paste forgeries in digital videos. Forensic Sci. Int. **281**, 75–91 (2017)
241. Chetty, G., Biswas, M., Singh, R.: Digital video tamper detection based on Multimodal fusion of residue features. In: 2010 Fourth international Conference on Network and System Security. IEEE, pp. 606–613 (2010)
242. Yao, Y., Shi, Y., Weng, S., Guan, B.: Deep learning for detection of object-based forgery in advanced video. Symmetry **10**(1), 3 (2017)
243. Saddique, M., Asghar, K., Bajwa, U.I., Hussain, M., Habib, Z.: Spatial video forgery detection and localization using texture analysis of consecutive frames. Adv. Elect Comput. Eng. **19**(3), 97–108 (2019)
244. Chen, R., Dong, Q., Ren, H., Fu, J.: Video forgery detection based on non-subsampled contourlet transform and gradient information. Inf. Technol. J. **11**(10), 1456–1462 (2012)
245. Aloraini, M., Sharifzadeh, M., Agarwal, C., Schonfeld, S.: Statistical sequential analysis for object- based video forgery detection. Elect. Image **5**, 543–551 (2019)
246. Aloraini, M., Sharifzadeh, M., Schonfeld, D.: Sequential and patch analyses for object removal video forgery detection and localization. IEEE Trans. Circ. Syst. Vid. Technol. **31**, 917–930 (2020)
247. Kobayashi, M., Okabe, T., Sato, Y.: Detecting forgery from static-scene video based on inconsistency in noise level functions. IEEE Trans. Inf. Forensics Sec. **5**(4), 883–892 (2010)
248. Wang, W., Farid, H.: Exposing digital forgeries in interlaced and deinterlaced video. IEEE Trans. Inf. Forensics Sec. **2**(3), 438–449 (2007)
249. Labartino, D., Bianchi, T., De Rosa, A., Fontani, M., Va´zquez-Pad´ın, D., Piva, A., Barni, M.: Localization of forgeries in mpeg-2 video through GOP size and DQ analysis. In: 2013 IEEE 15th International Workshop on Multimedia Signal Processing (MMSP). IEEE, vol. 2, pp. 494–499 (2013)
250. Subramanyam, A.V., Emmanuel, S.: Video forgery detection using hog features and compression properties. In: 2012 IEEE 14th International Workshop on Multimedia Signal Processing (MMSP). IEEE, pp. 89–94 (2012)
251. Hsu, C.C., Hung, T.Y., Lin, C.W., Hsu, C.T.: Video forgery detection using correlation of noise residue. In: 2008 IEEE 10th Workshop on Multimedia Signal Processing. IEEE, 170–174 (2008)
252. Kancherla, K., Mukkamala, S.: Novel blind video forgery detection using markov models on motion residue. In: Asian Conference on Intelligent Information and Database Systems. Springer, 308–315 (2012)
253. Fayyaz, M.A., Anjum, A., Ziauddin, S., Khan, A., Sarfaraz, A.: An improved surveillance video forgery detection technique using sensor pattern noise and correlation of noise residues. Multimed. Tools Appl. **79**(9), 5767–5788 (2020)
254. Singh, R.D., Aggarwal, N.: Detection of upscale-crop and splicing for digital video authentication. Digit. Invest. **21**, 31–52 (2017)
255. Chen, J., Kang, X., Liu, Y., Wang, Z.J.: Median filtering forensics based on convolutional neural networks. IEEE Signal Process. Lett. **22**(11), 1849–1853 (2015)
256. Hyun, D.K., Lee, M.J., Ryu, S.J., Lee, H.Y., Lee, H.K.: Forgery detection for surveillance video. In: The era of interactive media. Springer, pp. 25–36 (2013)
257. Zhang, Y., Goh, J., Win, L.L., Thing, V.L.: Image region forgery detection: A deep learning approach. In: SG-CRC, pp. 1–11 (2016)
258. Rao, Y., Ni, J.: A deep learning approach to detection of splicing and copy-move forgeries in images. In: 2016 IEEE International Workshop on Information Forensics and Security (WIFS), pp. 1–6 (2016)
259. Bondi, L., Lameri, S., Güera, D., Bestagini, P., Delp, E.J., Tubaro, S.: Tampering detection and localization through clustering of camera-based cnn features. In: 2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), pp. 1855–1864 (2017)
260. Amerini, I., Uricchio, T., Ballan, L., Caldelli, R.: Localization of jpeg double compression through multi-domain convolutional neural networks. In: 2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), pp. 1865–1871 (2017)
261. Salloum, R., Ren, Y., Jay, K.C.-C.: Image splicing localization using a multi-task fully convolutional network (MFCN). J. Vis. Commun. Image Represent. **51**, 201–209 (2018)
262. Wu, Y., Abd-Almageed, W., Natarajan, P.: Busternet: detecting copy-move image forgery with source/target localization. In: Proceedings of the European Conference on Computer Vision (ECCV), 168–184 (2018)
263. Bi, X., Wei, Y., Xiao, B., Li, W.: Rru-net: The ringed residual u-net for image splicing forgery detection. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops, (2019)
264. Wang, X., Wang, H., Niu, S., Zhang, J.: Detection and localization of image forgeries using improved mask regional convolutional neural network. Math. Biosci. Eng. **16**, 4581–4593 (2019)
265. Kumar, K., Shrimankar, D.D., Singh, N.: Event bagging: A novel event summarization approach in multiview surveillance videos. In: 2017 International Conference on Innovations in Electronics, Signal Processing and Communication (IESC), pp. 106–111 (2017)
266. Gunawardena, P., Sudarshana, H., Amila, O., Nawaratne, R., Alahakoon, D., Perera, A.S., Chitraranjan, C.: Interest-oriented video summarization with keyframe extraction. In: 2019 19th International Conference on Advances in ICT for Emerging Regions, 250:1–8 (2019)
267. Xia, G., Chen, B., Sun, H., Liu, Q.: Nonconvex low-rank kernel sparse subspace learning for keyframe extraction and motion segmentation. IEEE Trans. Neural Netw. Learn. Syst. **32**, 1–15 (2020)
268. Kumar, K., Shrimankar, D.D.: Deep event learning boost-up approach: Delta. Multimed. Tools Appl. **77**, 26635–26655 (2018)
269. Kumar, K., Shrimankar, D.D.: F-des: Fast and deep event summarization. IEEE Trans. Multimed. **20**(2), 323–334 (2018)
270. Kumar, K., Shrimankar, D.D., Singh, N.: Eratosthenes sieve based key-frame extraction technique for event summarization in videos. Multimed. Tools Appl. **77**, 7383–7404 (2018)
271. Sharma, S., Kumar, K. GUESS: Genetic uses in video encryption with secret sharing. Adv. Intell. Syst. Comput., 51–62 (2018)
272. Sharma, S., Shivhare, S.N., Singh, N., Kumar, K. Computationally efficient ANN model for small-scale problems. Mach. Intell. Signal Anal., 423–435 (2018)
273. Kumar, K.: Text query based summarized event searching interface system using deep learning over cloud. Multimed. Tools Appl. **80**(7), 11079–11094 (2021)
274. Manupriya, P., Sinha, S., Kumar, K. V⊕SEE: Video secret sharing encryption technique. In: 2017 Conference on Information and Communication Technology (CICT) (2017)

275. Koppanati, R.K., Kumar, K., Qamar, S.: E-MOC: an efficient secret Sharing Model for Multimedia on Cloud. In: Tripathi, M., Upadhyaya, S. (eds.) Conference Proceedings of ICDLAIR2019, p. 175 (2021)

276. Gadicha, A.B., Gupta, V.B., Gadicha, V.B., Kumar, K., Ghonge M.M.: Multimode approach of data encryption in images through QUANTUM STEGANOGRAPHY. In: Multidisciplinary Approach to Modern Digital Steganography, pp. 99–124 (2021)

277. Xiao, J., Zhao, R., Lam, K.-M.: Bayesian sparse hierarchical model for image de-noising. Signal Process. Image Commun. **96**, 116299 (2021)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.