Digital image forgery detection: a systematic scrutiny

Article *in* Australian Journal of Forensic Sciences · March 2018

DOI: 10.1080/00450618.2018.1424241

2 authors:

Savita Walia
Chitkara University
18 PUBLICATIONS **280** CITATIONS

SEE PROFILE

Krishan Kumar Saluja
University Institute of Engineering & Technology, Panjab University, Chndiagarh
185 PUBLICATIONS **4,810** CITATIONS

SEE PROFILE

Australian Journal of Forensic Sciences

ISSN: 0045-0618 (Print) 1834-562X (Online) Journal homepage: http://www.tandfonline.com/loi/tajf20

Digital image forgery detection: a systematic scrutiny

Savita Walia & Krishan Kumar

AUSTRALIAN JOURNAL OF FORENSIC SCIENCES, 2018
https://doi.org/10.1080/00450618.2018.1424241

Digital image forgery detection: a systematic scrutiny

Savita Walia and Krishan Kumar

University Institute of Engineering and Technology, Panjab University, Chandigarh, India

ABSTRACT

Image manipulation has eroded our trust of digital images, with more subtle forgery methods posing an ever-increasing challenge to the integrity of images and their authenticity. Over recent years, a significant research contribution has been dedicated to devising new techniques for countering various image forgery attacks. In this article, a survey of such research contributions has been conducted by following a well-defined systematic process. A total of 66 primary studies published before July 2017 was selected from five different electronic databases using a careful scrutinizing process. Four research questions have been formulated that capture various aspects of the identified primary studies. The field background required to understand the evolution of digital image forgeries is also presented. The aim of this systematic survey is to gain insights into the current research on the detection of these forgeries by comprehensively analysing the selected studies in order to answer this predefined set of research questions. This survey also discusses various challenges that need to be addressed, and has recommendations for possible future research directions.

ARTICLE HISTORY
Received 28 September 2017
Accepted 31 December 2017

KEYWORDS
Image forensics; digital image forgery; passive methods of detection; systematic survey

Introduction

Nowadays, there barely exists any platform where digital images are not used. They are used in almost every field, namely digital media, electronic media, military, law, industry, forensics, science and technology, medical sciences, glamor, social media, and so on, and all over the internet. With such vast numbers of images, the importance of their authenticity has increased enormously. We humans tend to believe in what we see rather than what we hear. So visible content becomes more important for us than verbal content. And hence we give much importance to what we see on a daily basis in newspapers, on the covers of magazines, news channels, social media such as Facebook, Instagram, Twitter and many more. Owing to their widespread use, digital images are the most commonly tampered digital media, misrepresenting their meaning with malevolent purpose.

Motivation

Digital image manipulation[1,2] is the act of distorting the contents of an image in order to fulfil some malevolent/fraudulent purposes. In digital forensics, such manipulations are

CONTACT Savita Walia savita_walia@rediffmail.com

known as forgeries. The problem of image forgeries is not new, but is as old as images themselves. Photo-manipulations have been in existence since the 1860s. There exist various cases of image forgeries in history[3] which caused clutter and affected people/organizations. Earlier photographers were habituated with using the process of photomontage, in which composites of images were created by pasting, gluing, overlapping and reordering two or more photographs to get the final print that looks like just a single photograph (Figure 1). However, due to the evolution of technology, various photo manipulation tools have been developed by researchers and programmers and made available over the internet. Various professional/amateur digital image editing tools are available, such as Affinity Photo, Paintshop, Adobe Photoshop, GIMP, Photoshop Elements, and many more. Some of them are available for free and a few are paid for but easily accessible and affordable.

It therefore becomes extremely important to find whether the image under consideration has been manipulated or not, as images are used in court of laws, in news, in sciences, for medicinal purposes and in many more fields as a proof of result. Hence, there arises the requirement for efficient and reliable image forgery detection methods that can distinguish between authentic and forged images and are able to locate the forgery in the image. Owing to the current demand, researchers are working in this field and are trying their best to develop the most reliable methods. It has been observed that a large number of research papers have been published in this research field by authors from around the world. An analysis has been done by running a query 'Image forgery detection' on IEEE (ieeexplore.org) and Elsevier (sciencedirect.com) which shows the number of publications per year in image forensics from 2000 to 2017 from two different libraries (Figure 2).

The major focus of a digital image forgery or manipulation is to contrive the illegitimate changes in an authentic image so that the image closely mimics the legitimacy of an authentic one. Thus, it becomes harder for the human visual system to differentiate between legitimate and forged/manipulated images. A mere detection of forgery is not the only objective here. Localizing the forged region affected by the various forgery operations performed by the forger is considered a more important task. Comprehensive ongoing research aims at delivering solutions to the problem of differentiating a forged image with that of an authentic image. Devising effective and real-time detection and localization methods is currently important as these forgery attacks are increasing with time[4].

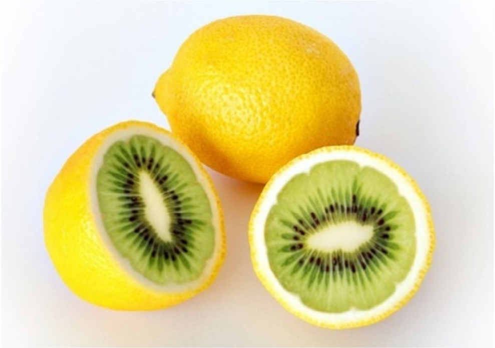

Figure 1. Photomontage of kiwi fruit and lemons digitally manipulated using GIMP (by Manuel (Diskussion) and Aka – Own work using: GIMP, Image: Lemon.jpg and Image: Kiwi_aka.jpg, CC BY-SA 2.5).

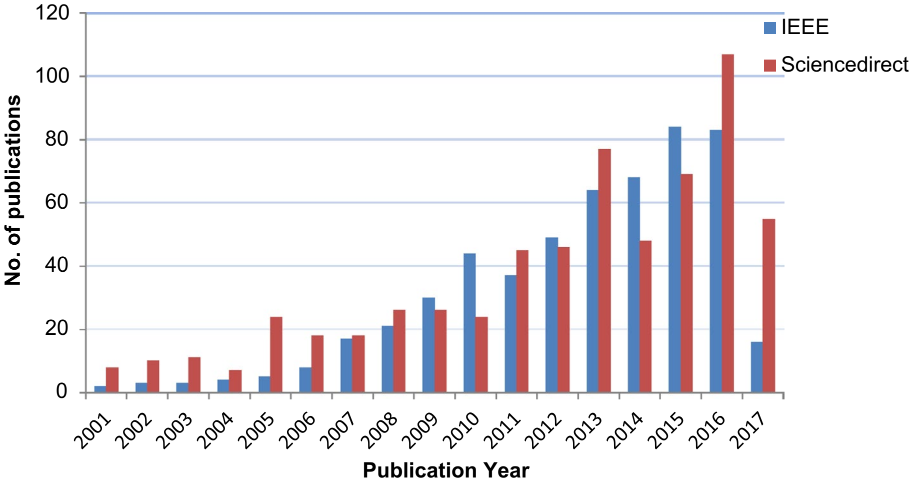

Figure 2. Number of publications over past 17 years on 'image forgery detection' in IEEE (ieeexplore.org) and Elsevier (Sciencedirect.com).

After a comprehensive consideration of the available literature, a few surveys dealing with passive methods of digital image forgery detection have been found. The survey paper[5] provided a taxonomy of various detection approaches against copy-move and image splicing and various image processing operation detection methods. The generalized structure of various detection methods is also discussed along with their drawbacks. Another effective survey paper[6] provided a complete bibliography on pixel-based methods adapted for image forgery detection, while a review[7] focused on copy-move forgery detection. This survey provided a classification of various image forgeries and their detection techniques and focused on passive detection based on pixel-based methods. Some very specific types of survey papers also came to the forefront, which focused on a particular type of detection method. Two of such surveys are given, the block based methods of copy-move forgery detection were discussed and only 18 studies were surveyed[8]. Methods based on different features were categorized and analysed[9]. The key-point based methods were divided into two categories: (1) methods based on SIFT; (2) methods based on SURF. Nineteen SIFT-based and ten SURF-based studies were considered for the review[8,9]. The latest survey paper encountered[10], in which 33 studies for copy-move and 18 studies for image splicing detection were exhaustively reviewed. Various other surveys are also available[11–14] but fail to provide a deep insight into this field and do not provide a path for future directions. In spite of analysing the pros and cons of various detection studies, such work failed to provide an in-depth and exhaustive coverage of the current literature.

Contribution

The work in this article differs from the above-mentioned existing surveys in that a systematic approach is followed to conduct an exhaustive survey, and to provide in-depth detail of literature focusing on various image forgery detection techniques. A systematic approach for surveying the literature initially gained popularity in the field of medicine, public health, etc. In computer science, such surveys are common in the field of software engineering[15,16].

A number of surveys also exist in the area of cloud computing[17–19] and network security[20,21]. This survey is the first of its kind in the field of digital image fakery detection.

The survey accomplished in this article integrates a 'systematic' methodology to formulate a significant and comprehensive record of the state-of-art literature focusing on detection of various digital image forgeries. A well-defined systematic methodology is used to recognize, investigate and understand all available indications related to an explicit research question, such that it is impartial, balanced and (to a certain level) re-iterates[22,23]. The quality assessment was performed in order to select high quality research papers for final review. The data extracted from the final set of papers selected for review were analysed in order to respond to the formulated questions. The major contributions of this study can be precisely given, as follows:

- Identification of high quality studies in the field of digital image forgeries using a systematic survey protocol.
- Provides state-of-art taxonomy of digital image forgeries and detection methods.
- Presents critical review of approaches and modelling practices followed by various detection methods.
- Signifying hopeful future research directions through a vigilant scrutiny of various limitations and challenges of existing studies.

The article is organized as follows. The section below explains in a systematic manner the steps involved in the Survey Protocol, which is implemented for the literature review. Further, a state-of-art taxonomy of various possible forgery attacks and a refined classification of various image forgery detection methods are provided. Upon critically reviewing final set of studies obtained from survey protocol, various research challenges and future scope in this field are identified. Conclusions are drawn in the final section.

Survey protocol

A sequence of methodologies followed by orderly literature evaluation assists in attaining a prevalent understanding of the problem at hand. Originating from the field of medicine, systematic surveying is considered to be a trustworthy research method[24]. It delivers a constructive medium to collect and perceive the literature relating to the problem description. It is believed to be an effective method to identify any research gaps and recognize paths for upcoming research work. Following the stipulations suggested by Kitchenham[22], a systematic approach is undertaken to implement an extensive review of the accessible literature associated with the detection of various image forgery attacks.

The validity of the survey process was verified by doing a pilot study before actually implementing the survey protocol. The theoretical view of the implemented survey protocol is shown in Figure 3[21]. The very first step of a systematic survey is to define research questions based on which the search string is formulated. A comprehensive literature search is conducted with the help of this search string that will form the base of the answers to the research questions. Several steps involved in conducting this systematic survey are explained in the subsequent subsections. The conclusion of this review would help in highlighting numerous challenges associated with the field, thereby encouraging the researchers to perform further investigations.

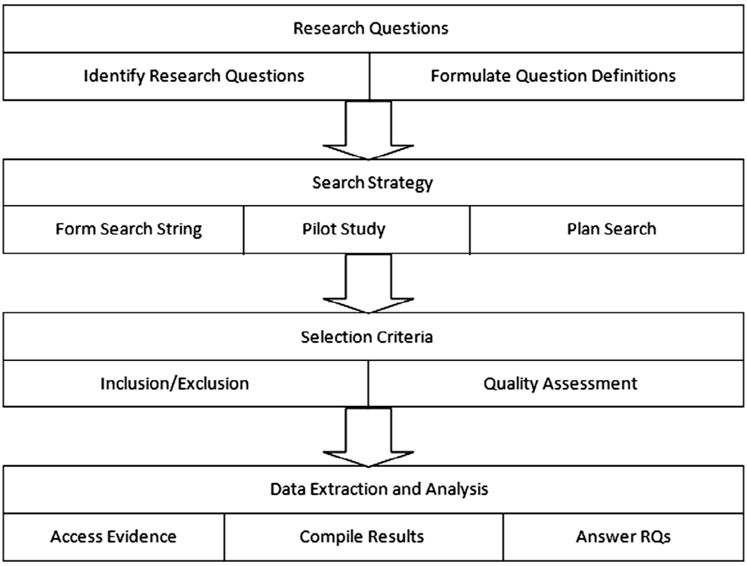

Figure 3. Survey protocol plan.

In the following subsections, the particulars of survey protocol phases linked to the research questions, search strategy, inclusion/exclusion criteria, reference checking, quality assessment, data extraction, and categorization method are explored.

Research questions

The main objective of this structured survey is to execute a detailed analysis of the literature available on detection techniques for various image forgery attacks. To achieve this objective, various research queries are formulated that are answered by scrutinizing the data mined out from the list of final competent research papers. The research queries addressed in this paper are given below.

Research queries

RQ1: What are the different types of digital image forgeries?
RQ2: What are the various approaches and modelling methods that form the basis of forgery detection and localization techniques available in literature?
RQ3: What are the strengths and shortcomings of the existing methods?
RQ4: What are the major challenges faced by the researchers in the literature?

In this study, the emphasis is entirely on defining and answering the research queries, which are formulated above, and on exploring the collected works on detection of various image forgery challenges from various viewpoints. These digital image forgeries can be performed with varying semantics in efforts to outsmart various detection methods. In RQ1, we explore such different attack strategies that have been investigated in the literature. The organization of detection practices established on the basis of methodologies adopted and the localization methods used, is covered in Research Query 2. There is a widespread range of datasets that have been used for the assessment of these detection methods. Also, the evaluation of a particular method involves the usage of numerous software tools that provide a variation of investigational setups which are covered under Research Query 3 while critically analysing each method. RQ4 attempts to identify major challenges faced by the researchers.

Search strategy

A search strategy is formed to initialize the process of a systematic survey with a hunt through electronic libraries to gather the appropriate literature. The search strategy is an important point of the survey procedure. So, constructing an effective search strategy is considered as a critical pre-requisite. In this work, an automatic search was performed in two different phases. Search Phase 1 included a consideration of four digital libraries, i.e. *ACM Digital Library*, *IEEE Xplore*, *Springer* and *ScienceDirect*. Search Phase 2 was supported by scholarly search engine, *Google Scholar*. The addition of *Google Scholar* as a source helped in constructing a robust and durable base of primary studies and evaded omitting any relevant studies. The search was limited to the article title, abstract, and meta-data in *ACM Digital Library*, *IEEE Xplore* and *ScienceDirect*. Carrying out a search query on *Springer* and *Google Scholar* produced 1514 results due to the lack of customization options as in other digital libraries. Restricting the search keywords was sustained by all electronic databanks that aided in deciding a smaller search query. The common search sequence that was used with slight alterations fitting in various libraries is:

(Digital image forgery **OR** image forgery detection **OR** detecting image forgery)

The results achieved by performing this search query in selected digital libraries were narrowed down to the appropriate fields wherever possible by means of 'filtering' options. Figure 4 represents the implementation flow of the survey procedure along with the number of studies subsequent to each stage.

Pilot study

A pilot study was performed before conducting the actual process of data collection to refine the search method. A total of 20 articles were selected for this purpose from a set of pre-collected articles stored in the database. These comprised the ten most cited and ten most

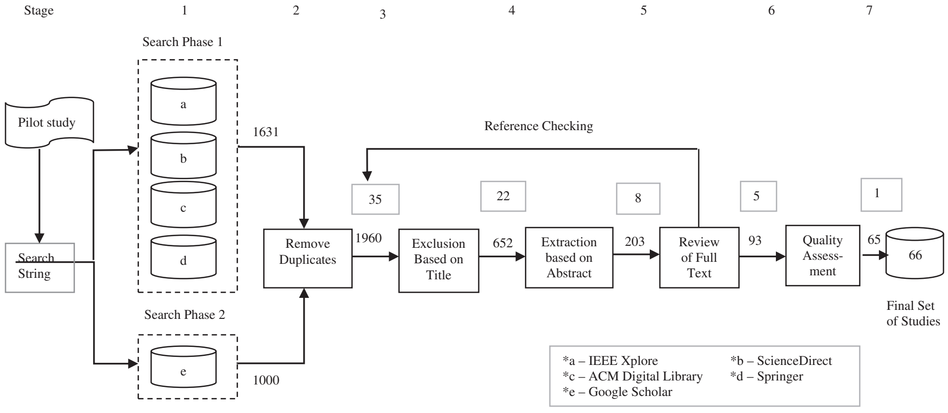

Figure 4. Various steps involved in survey protocol along with the number of studies obtained at each step.

relevant articles (published between 2015 and 2017). Following this, a pilot search was carried out on *IEEE Xplore*, targeting the studies published between 2015 and 2017. The resulting entries were passed through further stages of the survey protocol. The articles resulting from this process were then compared with the 20 selected articles. 1Seventeen out of all 20 nominated articles (85%) were found to be consistent with the pilot search results, which validates our search string and the survey process.

Study selection

In the study selection stage, the addition and elimination criteria were applied to exclude any irrelevant articles with respect to the defined research questions. Hence, only those studies that could possibly answer the research questions were added to the final list of primary studies. The study selection criteria were collectively designed, taking into consideration the defined research questions. In addition to the above-defined criteria, studies that were either identical to existing studies or which had been extended as a new and mature studies and published elsewhere were also filtered out. Only the articles that were published as extended versions of their respective previous works were selected. The studies with ambiguous exclusion decisions were retained for analysis in subsequent stages. Search Phase 1 returned 1631 entries.

Google Scholar fetched 1000 entries in Search Phase 2, making a total of 2631 studies in Stage 1. In Stage 2, 671 duplicate entries were removed from the list of total entries obtained from Stage 1. this was followed by the elimination of results based on their titles (1308 studies excluded), abstracts (449 studies excluded), and full texts (110 studies excluded) respectively in subsequent stages. Finally, a total of 93 studies were extracted after Stage 5. The inclusion and exclusion criteria used in the selection process are defined below.

The inclusion criteria checklist is as follows:

- All studies that provide a novel approach for detection of image forgeries;
- Studies that deal with differentiating between the authentic and forged image;
- Studies that comply with research questions;
- Studies that, along with the detection of any other forgery, have also considered localization of the detected forgery;
- Studies that are closely related but vary in one or more important parameters were included as individual primary studies.

The exclusion criteria checklist is as follows:

- Studies not in the English language;
- Works that have been extended and published as a new article elsewhere;
- Tutorials, editorials, covers, news, interviews, surveys, simulation studies, and summaries of workshops and symposiums;
- Works not outlining the adequate amount of information;

Reference checking

The references of 90 studies obtained from Stage 5 were also examined to avoid omitting any relevant work. The resulting list of 33 studies was passed back to Stage 3 for relevance assessment based on title and abstract. The studies not complying with study selection criteria were removed. After the full text analysis using inclusion and exclusion criteria, 11 studies were removed. Finally, a total of eight studies were obtained through reference checking.

Quality assessment

A quality assessment check was performed in Stage 6 to extract only the high quality works out of 98 studies passing Stage 5. To assess the quality of each study, the same predefined quality checklist was followed. The quality assessment of a study was conducted by assigning every checkpoint with a score value after carefully analysing the relevant credentials of that particular study. The average of these score values assigned was then calculated. A study that scored higher than 4.5 was included in the final list. Sixty-five studies from the original list and one study from the list obtained through reference checking qualified for inclusion in the final list of 66 primary studies. Thirty-two other studies were eliminated in this phase. The quality checklist comprises following checkpoints:

- Are the results of practical significance?
- Is the approach followed novel?
- Does the paper highlight implementation details?
- Is the method used to evaluate the work appropriate?
- Is the content adequate to support the research?
- Are the results explicitly stated?
- Is the study design in agreement with the research questions?
- Are conclusions drawn appropriately?
- Does the work utilize any datasets for evaluating the proposed technique?

Data extraction

To address each research question, the required data were extracted by reviewing the complete article text. A pre-designed data extraction form was initially filled with detailed information extracted from every study. The extraction form contains various entries to critically analyse the final set of papers. The fields in the critical review format include title, author, publisher and year, aim, approach, experimental setup/tools used, strengths, weaknesses and future scope. At the end, a total of 66 data extraction forms (spreadsheets) were prepared to facilitate the explanation of responses to the research questions. Table 1 shows the number of studies obtained at every stage in the survey process. Table 2 gives the percentage of the studies on the basis of the nature of publications.

Categorization method

The classifications of primary studies performed under different research questions were independently carried out. A three-phase method was followed in order to put together a consistent list of categories during the course of this survey. The first phase begins with writing down all the possible keywords which the given input set may fall under. The common keywords were selected for further exploration. Secondly, the input set was grouped

Table 1. Number of studies in each stage of the survey process.

Source	Stage 1	Stage 2	Stage 3	Stage 4	Stage 5	Stage 6
IEEE	183	175	131	73	32	23
Springer	514	443	206	41	27	21
ACM	727	452	150	10	5	2
Sciencedirect	207	200	154	47	20	16
Google Scholar	1000	690	111	32	9	3
References	–	35	22	8	5	1
Total	2631	1995	774	211	98	66

Table 2. Distribution of studies on the basis of publication types.

Publication type	No. of PRs	Percentage (%)
Journal	52	78.78
Symposium	1	1.51
Conference	7	10.61
Workshop	6	9.09

based on these keywords. The process is repeated until a coherent category structure is obtained.

Taxonomy of digital image forgeries

Image forgeries started to occur a decade after the first image was created. The forgeries done in 1860s were analogue manipulations. Before digital scanners and cameras prevailed, traditional analogue image editing was implemented with the help of tools such as airbrushing to modifying photographs with any traditional art method. In traditional analogue image editing, the images were edited during the process of photographic printing. With the advent of technology, digital images have become mainstream and analogue image editing has become obsolete[25]. Digital images can be forged in a number of ways with the help of various image manipulation software such as Adobe Photoshop Elements[26], Pixlr[27], GIMP[28], etc. Such image editing software are available on internet for almost every platform, e.g. Windows, mobile phones, tablets, etc. The image editing applications are being used by a lot of people and shared on various social media platforms. The purpose of editing an image can vary from person to person. When the malicious changes are performed on a digital image by hiding some useful information or to change the meaning of the image being viewed, then such modifications are known as digital image forgeries[29]. In this paper, a taxonomy of digital image forgeries is provided (see Figure 5). The various categories are discussed below:

Copy-move forgery

Copy-move forgery is one of the most commonly performed manipulations on digital images. In copy-move forgery[30], a region from the image is copied and pasted to another region in the same image. Copy-move forgery is performed in order to hide an existing object in the image, to create a duplicate of the object or to change the meaning of the image completely. There are various ways in which copy-move forgery can be performed. Based upon them, it is categorized further into the following four types:

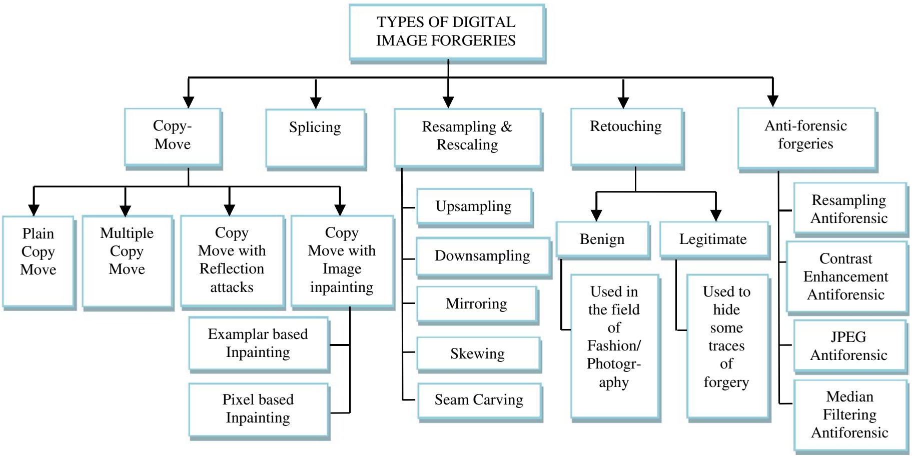
TYPES OF DIGITAL IMAGE FORGERIES
Copy-Move
Splicing
Resampling & Rescaling
Retouching
Anti-forensic forgeries
Plain Copy Move
Multiple Copy Move
Copy Move with Reflection attacks
Copy Move with Image inpainting
Examplar based Inpainting
Pixel based Inpainting
Upsampling
Downsampling
Mirroring
Skewing
Seam Carving
Benign
Legitimate
Used in the field of Fashion/ Photogr-aphy
Used to hide some traces of forgery
Resampling Antiforensic
Contrast Enhancement Antiforensic
JPEG Antiforensic
Median Filtering Antiforensic

Figure 5. Taxonomy of digital image forgeries.

(1) *Plain copy-move*: plain copy-move forgery refers to the process of copying a region of the image and pasting it onto another region in the same image without performing any manipulation on the copied region.

(2) *Multiple copy-move*: in multiple copy-move, more than one region or object may be copied and pasted into different regions of the image. There can be cases when an object is copied from the image and pasted to two locations in the image. In another case, different objects are copied and can be pasted into different locations in the same image.

(3) *Copy-move with reflection attacks*: in this type of copy-move forgery, the duplicated region is obtained by altering the copied region with a rotation of 180° such that it creates the same object but with a different orientation. In most of the cases, object created using reflection attack is pasted along with the copied region such that it matches the characteristics of the copied object and escapes the detection methods.

(4) *Copy-move with image inpainting*: earlier image inpainting was used for reconstructing the deteriorated portions of the image by considering neighbouring areas of the distorted regions. But the forgers are trying their finest to attempt a kind of forgery such that it seems real. Using image inpainting to perform manipulations on the image is one such technique. It modifies the image in undetectable form. One of the most common methods of image inpainting is exemplar based inpainting. In copy-move with exemplar based image inpainting, several small regions of the image are taken in order to hide an object in the image.

Now, the region to be copied can be anything, depending upon the image[7]. If the image is of document type, then the manipulations can be such that the content of the document is changed by altering the text in the image. Such a kind of forgery is used to alter the documents such as certificates, testimonials, legal and confidential papers, etc. The region to be copied can be background area, objects or text.

Image splicing

Image splicing[31] is the process of merging two or more images. Splicing is similar to copy-move forgery to some extent. In copy-move, the region copied is from the same image whereas the region to be pasted in the spliced image is taken from some other image. Splicing is a major step in digital photomontage, which refers to the paste-up produced by combining images with the help of digital software tools such as Photoshop, GIMP, etc. Image splicing is also known as image compositing. Various examples of image composites can be witnessed in numerous infamous news reportage cases involving the use of forged images.

Resampling and resizing

Resampling[32] is the process of transforming a sampled image to another coordinate system. It is the method of geometrically transforming the images by changing the number of pixels in an image. Most people confuse image resizing and image resampling. Image resizing is simply changing the size of the images without changing the number of pixels. Changing the document size of the image is known as resizing and changing the number of pixels is known as resampling. In image forgery, there may be cases when an object needs to be resized in order to match the relative object in the image while performing forgery. The process of resampling involves sampling of the original image on top of a different sampling mesh which introduces particular correlations between adjoining pixels. Resampling can be performed in the following different ways in order to achieve goals according the requirements:

(1) *Up-sampling*: when the number of pixels of the image is increased, it is called up-sampling.
(2) *Down-sampling*: when the number of pixels of the image is decreased, it is called down-sampling.
(3) *Mirroring*: in mirroring, the whole image is flipped horizontally or vertically. This type of forgery is difficult to detect as it does not change any intrinsic characteristics of the image.
(4) *Skewing*: skewing in digital images can be performed using software tools such as Photoshop, GIMP, etc., by dragging the corner points of an image.

Retouching

Retouching refers to the process of removing image flaws, skin blemishes, scratches, etc. It is used to eradicate disturbing elements by improving the images according to the individual requirements. Digital image processing offers several options for image retouching[33] and is preferably suited for fashion photography as well as beauty and product images. Retouching can also be done in an illegitimate way in order to hide the traces of forgery operations already attempted on the image.

Anti-forensic forgeries

Anti-forensic forgeries are those forgeries that are targeted at escaping the forgery detection methods[34]. Those forgers who have deep knowledge of digital image processing methods and forensic methods, are working towards finding ways to perform a forgery such that the detection methods become incapable of detecting them. Anti-forensic forgeries[35] are mostly applied by forensic teams so that they can find loopholes in their detection methods and can develop counter anti-forensic methods. But some farsighted forgers also take advantage of anti-forensics so that the forensic methods cannot detect the forgeries performed. Anti-forensic forgeries have the capability to effectively eliminate imprints left by a particular image forgery. But such operations leave different imprints of their own, which can be detected by using counter anti-forensics methods.

Apart from the above-mentioned types of digital image forgeries, various other post processing operations can also be applied by the forger in smarter ways, such that it may not be noticed by human vision. Such post-processing operations can be applied in various combinations. A forger may attempt a forgery with a number of post-processing operations. Some commonly used post-processing methods are noise addition, compression, blurring, geometrical operations such as rotation, flipping, skewing, scaling, mirroring, etc., and quality improvement operations like change in brightness or contrast.

Classification of digital image forgery detection methods

In a world packed with technology, we simply cannot trust what we see. As the software tools for image manipulations are so easily available on the internet, image authenticity and integrity needs to be checked. Digital images are increasingly communicated over various non-secure channels. Therefore, the images used in medical, military, law, science, journalism and other images of utmost importance must be checked before they are believed to be true. The manipulation tools undermine the trustworthiness of digital images shown in the news or as proof in a court cases, since it may not be possible to distinguish between the authentic image and a forged one. Hence, the authenticity and the integrity of digital images cannot be taken for granted. Image forensics, from this perspective, is apprehensive about determining the source and authenticity of a digital image. To check the authenticity and integrity of digital images, digital image forensics[29] moved toward expansion (see Figure 6). Digital image forensics is broadly classified into three categories, namely source camera identification, discrimination and image forgery detection. A detailed classification of image forensics is provided in this section. Earlier, only a classification of forgery detection methods[5] was given. The major aim of this paper is to explore digital image forgery detection methods, so the other two fields are only briefly described.

Source camera identification

Identification of the source camera is a significant branch of digital image forensics which is used to determine the origin of the image. Source camera identification techniques extract and recognize features of devices used in the process of image acquisition. The techniques that are used to classify the acquisition devices (such as digital camera, smartphone camera) are based on the difference in processing elements and technologies. Reliable classification of the source camera depends on the classification of various model dependent characteristics. Source camera identification methods can be further based on various device characteristics, such as lens aberration, sensor imperfections, colour filter array (CFA) interpolation and image features. Lens aberration is the result of imperfections and artefacts caused by

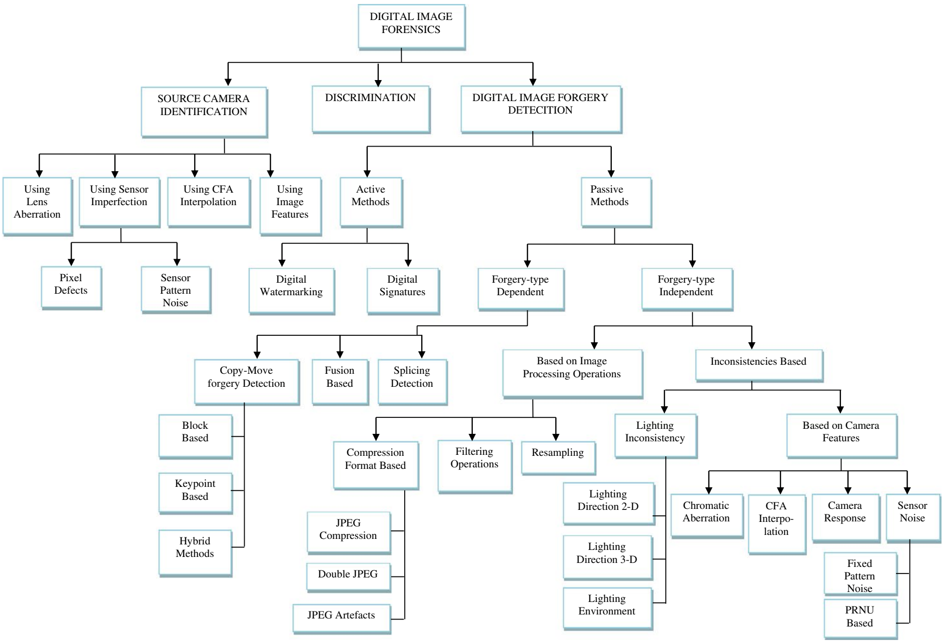

Figure 6. Hierarchical structure of Digital Image Forensics.

the optical lens of the digital camera. Choi, Lam, and Wong[36] proposed lens radial distortion as a characteristic to recognize source camera. Due to radial distortion, the straight lines give the impression of the curved lines on the resulting images. A unique radial distortion pattern is expressed by each camera model, which helps to identify it. The second category under source camera identification uses sensor imperfections. Sensor imperfections can be characterized using pixel defects and sensor pattern noise. Geradts et al[37] examined the imperfections of Charged Coupled Device (CCD) pixels and used them to match objected images with source digital camera. Lukas, Fridrich, and Goljan[38] proposed a method based on pixel non-uniformity (PNU). PNU refers to the different light sensitivities of different pixels sensitivities due to inadequacies in sensor manufacturing processes, which is a major source of pattern noise. This makes PNU an accepted feature for exclusively identifying sensors. In CFA interpolation[39], the colour filter array (CFA) is examined. The methods based on CFA interpolation use the correlation patterns of each colour band for image classification. The last category in source camera identification is the use of image features for recognizing the acquisition device. Various image features[40] are proposed to categorize a camera model. These features are categorized into three major groups: Colour Features, Wavelet Domain Statistics and Image Quality Metrics. The methods based on image features do not work well with images from a camera having similar CCD and are not suitable for detecting the correct source camera model.

Discrimination

With technology, computer graphics have attained new heights and become capable of producing extremely photorealistic images, which results in stimulating legal situations.

Such technological advances have led to exaggerated releases that distort the line between reality and imagination. There are various situations in which it is necessary to discriminate between computer generated images and natural photographic images. To distinguish the computer generated (CG) images from photorealistic images, various computational techniques are proposed[41–44]. These techniques use low-level statistical measures of the images. Such statistical measures suffer from various issues, for example their susceptibility to deviations in colour, compression quality, image quality, signal-to-noise ratio (SNR), resolution, etc.

Digital image forgery detection

Forgery detection methods have become a requirement of the present time as image forgeries are increasing day by day. *Image forgery* refers to the deliberate manipulation of a digital image, for the only purpose of amending the semantic of the visual message comprised in that image. Digital image forgery detection mechanisms aim to detect such manipulations. They can be grouped into two different categories, active methods and passive methods.

Active methods

The methods used in the active methods[45] exploit certain information inserted inside the digital image by the imaging device during image acquisition or before the distribution of the image to the public. The embedded data in the image is used to detect the source of such an image or to perceive an alteration in that image. Digital watermarking[46] and digital signatures[47] are examples of active techniques. In digital watermarking[48], a specific message digest is inserted in an image at the time of capturing. The digest can be taken out from the image at further stages in order to verify the legitimacy. The extracted digest is then compared, if it is found to be different from the original digest then it indicates that the image was modified after the acquisition process. In watermarking techniques, there are two phases when watermarking is used. Initially, when the image is generated the watermark is inserted. Then, after the image reaches the destination, the watermark is extracted and is matched with the obtained watermark[49–51]. Watermarking is a vigorous mechanism to safeguard the digital image integrity, but there are various challenges that make its use impractical. The primary reason is that there are only a few devices or cameras that have the feature of embedding a watermark in image acquisition. Second, the available devices, such as the Canon EOS-1D or Nikon D2Xs, having this embedding feature are very expensive. Another drawback of this technique is that it is incapable of distinguishing the illegitimate and legitimate manipulations on an image. Legitimate manipulations are the changes done for quality improvement of the image, such as contrast enhancement, sharpening, etc. The actual limitation of watermarking approaches is that specialized hardware or software is required in order to embed the digest in the image. In Tafti et al work[52], the spatial data are embedded in the image, i.e. the statistical measures. Initially, the image is divided into regions based on similar region properties. Then, four statistical measures, i.e. mean, median, mode and the range of pixel values are embedded in the image with encryption. If the image has been tampered with, regions can be identified with the help of embedded statistical information.

Passive methods

In disparity with active methods, passive or blind methods[53,54] of forgery detection take advantage of the traces left by the image processing operations performed in various phases while acquiring and storing the digital images. Such traces can be considered as a thumbprint of the image source device. Passive methods work in the absence of prior knowledge about the image, such as watermarks or signatures. There is nothing inserted in the image before its distribution. Passive methods make use of the available image only and a certainty that the manipulation operations alter the statistics of the image, which can help in its detection when the image is tampered with. The binary information of the image is analysed using various techniques to detect the forgery traces if present. Original images are supposed to have consistent characteristics, such as noise variation, lighting, shadows, and so on. Manipulating the contents of the image results in altering these characteristics, which make them inconsistent. Such inconsistencies in the statistics of the image can then be calculated in order to detect forgery. Passive methods are the only solution to decide the trustworthiness of a digital image when digital watermarks or signatures are not available. Some image manipulation operations may be more confusing for such methods, taking compression-based forgery into account. Image forgery detection based on compression in some cases may not give enough evidence of forgery. Instead, we doubt the integrity of that image, hence we need further analysis. Passive methods are broadly classified as forgery-type dependent and forgery-type independent.

Forgery-type dependent

Forgery type dependent methods target the two major types of forgeries described in Section 2. They are based on copy-move forgery and image splicing.

Copy-move forgery detection methods follow a general sequence which includes three major steps shown in Figure 7: (i) dividing the image into overlapping/non-overlapping blocks; (ii) implementing the feature extraction algorithm on each block; (iii) feature matching.

In copy-move forgery detection methods[7,55], the major goal is to match the regions in the image, which are similar and can distinguish between the copied and the pasted region. The problem of copy-move forgery has engrossed various researchers and there are numerous research papers available in the literature focusing only on copy-move forgery detection. Copy-move forgery can be easy to perform but it is difficult to detect as the regions are from the same image, so most of the characteristics, such as colour temperature, noise and illumination conditions are mostly well-matched among the copied and the pasted region. Hence, it can be undetectable by human vision. Further, integrating it with other operations like splicing can make it more complex to detect. Therefore, detection of copy-move forgery is essential. Various copy-move forgery detection methods are divided into two categories: block based and key-point based methods. A third category is formed by combining the block-based and key-point based methods. In block-based methods, feature extraction algorithms are implemented on the segmented image. The segmented image can have

Block Segmentation
Feature Extraction
Feature Matching

Figure 7. General methodology for copy-move forgery detection.

overlapping blocks or non-overlapping blocks. The feature extraction algorithms used in these methods are discussed in the next section. Feature vectors are obtained from feature extraction algorithms and are matched using block-based matching algorithms. Various block-based matching algorithms used in literature are:

- Sorting: lexicographic sorting, KD-tree, radix sort
- Hash: counting bloom filters, locality-sensitive hashing
- Phase correlation
- Euclidean distance
- Others: sum of difference between DCT coefficients and sequential clustering

In the case of key-point based methods, the segmentation into blocks is removed from the pre-processing step. The key-points are extracted using key-point feature extraction algorithms. They extract the distinctive local features such as corners, edges, and blobs from the image. Each feature is defined with a set of descriptors extracted from a region around the features. Both the descriptors and features are matched to find the copied region. Key-point based methods are computationally less complex, but they do suffer from issues. The issues are concerned with images having smooth surfaces, where fewer key-points are extracted and the forged region can escape the detection methods. Some forgers inject key-points in order to perform an anti-forensic forgery in the image. Key-point based feature extraction algorithms are divided into three categories: SIFT, SURF and Harris corner points, which are discussed briefly in next section. Key-point based matching algorithms are divided into following types:

- Nearest neighbour: 2NN, g2NN, best bin first, others
- Clustering: Hierarchical Agglomerative Clustering (HAC), Weight Centre of Mass Distance (WPGMC)

To overcome the drawbacks of block-based and key-point based methods, both are fused[56,57] together to make a hybrid method. The hybrid method helps in reducing the overall complexity of the method, which was due to the block matching step. In key-point based methods, segmentation can be performed before extracting key-points in order to extract key-points from the whole image.

Splicing-based methods: image splicing is another commonly used forgery operation in images. It is therefore necessary to detect image splicing. For splicing, copy-move based techniques cannot be used as those techniques are based on finding a matching region in the image, whereas, in splicing, the forged region is copied from another image. Hence, the forged region will have different characteristics as compared with the rest of the image. Splicing-based methods use a variety of features such as Bi-coherence features, camera response function, DCT and DWT coefficients, invariant image moments, Weber local descriptors, etc. Bi-coherence was initially used for detection of forgeries in speech[58]. Soon after, Ng and Chang[59] used magnitude and phase features of bi-coherence in order to detect splicing in digital images. A method was proposed[60] that calculated the response functions of the capturing device by choosing different patches from the image. The inconsistency or abnormalcy in the patches was then used to detect splicing. The splicing based methods are dependent on the intrinsic characteristics of the devices rather than the actual characteristics of the capturing devices.

Fusion-based methods: fusion-based methods[56,57] target both copy-move forgery and image splicing. Information fusion techniques are used to develop the fusion rules to follow. Relying on only the decisions from one forensic tool is no longer a well-grounded approach. In order to improve the reliability and performance of detection approaches, various forensic tools are combined by using appropriate decision fusion rules. So that the final decision rule for authenticity of the image is dependent on decisions of all the tools in use rather than on the decision of a single forensic tool. In fusion, the final decision about the problem is taken by analysing the outputs from different tools. It can be performed in three ways, namely Fusion at Feature Level, Fusion at Measurement Level and Fusion at Abstract Level[61,62]. In fusion at feature level, the features are extracted from various tools and are fused together to make new features. These features are then further used to train a universal classifier. The second method is fusion at measurement level, which fuses the scalar outputs from various tools. In fusion at abstract level, the outputs from various forensic tools are converted to binary outputs and decision rules are made based on the binary outputs.

Forgery-type independent

Forgery-type independent methods do not target any specific forgery, such as copy-move or splicing. Rather, these methods look for some intrinsic changes in the image characteristics. These methods have limited applications. In case of the compression-based method, they can be implemented only on images that are compressed in a certain format. For uncompressed images, compression-based methods cannot be implemented.

Based on image processing operations, the blind methods of forgery detection utilize the statistical features of the image, and such imperceptible features can be exploited by various image processing operations such as image filtering, resampling, jpeg compression and contrast enhancements. Detection of these operations can provide a clue that the image has been tampered with. Resampling[32,63,64] can be detected either in pixel domain or in frequency domain. After resampling, median filtering[65] is the most popular tool for noise removal and image enhancement. Numerous works are proposed for detection of median filtering[66,67,68]. The perfect performance was detected in these methods when the images under consideration are large and uncompressed. But in real scenarios, the images are mostly compressed using JPEG compression format. So the detection methods need to be resistant to various compression quality factors. Sometimes the traces left by median filtering are too weak to detect, which remains a challenge for median filtering forensics. Forgers also use JPEG compression as a tool to hide the hints of the tampering. Consider, for example, the case in which a manipulator alters the contents of the already compressed image by resaving the image again with the same compression format, say JPEG. The unaltered portion of the image is therefore compressed twice whereas the altered region appears to be compressed only once because the JPEG artefacts introduced by initial compression were destroyed by the manipulation. So the major goal in JPEG-based forgery detection[69–71] is to find the areas with differing numbers of JPEG compression, and discover such an abnormality. The standard approach for JPEG-based methods is to use blocking artefacts introduced by JPEG compression. Such inconsistencies help to detect the forgery and, moreover, they shed light on what kind of forgery has been performed. There are numerous techniques that are based on such inconsistencies and detect resampling, scene lighting and copy-move.

Inconsistency-based: inconsistency-based methods are further categorized as Lighting inconsistency based and methods using camera features. Lighting inconsistency based methods further include 2-D lighting, 3-D lighting, lighting environment and the shadow of objects in an image. These methods assume that the manipulations performed on an image will change the geometrical or physical aspects of the image, which can be used as evidence to detect tampering. Lighting-based forgery detection has been addressed[72–74] with simple light direction, two-dimensional complex lighting and three-dimensional complex lighting respectively. The second category is the detection using camera-based features. There are various features of a camera that are used in image forgery detection, such as chromatic aberration, camera response function, colour filter array interpolation and sensor noise. All these features are related to the optical and sensor system of the camera. The interpolation introduced by the acquisition process causes some specific correlations between the samples of a colour image. When a digital forgery is attempted on the image, these correlations may be damaged or altered.

Critical review of final set of studies

A critical analysis of the final set of studies (obtained after Section 2) was performed. The final set of studies included 66 research papers published in the period 2015 to 2017. These methods are categorized as broadly based on the techniques used in the detection methods. The critical analysis was done by preparing 66 different spreadsheets which included fields: Date of review, Title, Author, Publisher and Publication year, Aim, Approach, Experimental setup/Tools used, Strengths, Weaknesses and Future Scope. The data from these spreadsheets were extracted and was put into different tables. The table attributes contain some important aspects of the methods, namely features used, feature dimension, classifier/model used, dataset used and the performance metrics with their value obtained in respective methods. In the final set, 30 studies were based on copy-move forgery detection, and these are further divided into key-point based, block based and hybrid methods, 13 were based on splicing detection and two were based on a fusion of copy-move and splicing detection, 10 on deep learning based studies and 11 other studies, which are discussed in this section.

Key-point based methods: in Silva et al work[75], multi-scale analysis is performed on the extracted key-points using Speeded Up Robust Features (SURF). The image is analysed by examining its various scales in a Gaussian pyramidal decomposition that generates a new Partial Detection Map (PDM), which is a detection map for an image at given pyramid level. In each PDM, a region gathering procedure is performed in which a cloning candidate region is joined from a subgroup by merging in a unique region using a Minimum Bounding Rectangle (MBR) algorithm. Therefore, a larger area of a subgroup becomes a potentially cloned region. Then the regions which are classified as duplicated in the majority of the pyramid levels are referred to as forged. The method proves to be more robust against rotation, scaling and their combination. It suffers from a lack of key-points extraction in the case of small and homogeneous forged regions. To overcome the problem of fewer key-points, a dense-field approach is proposed[76] in which a fast approximate nearest neighbour Patch-Match algorithm is used, especially suited for computation of dense-fields over the images. Dense field techniques give better performance as compared with key-point based methods but at the cost of higher processing time. Another method is proposed[77] to extract sufficient amount of key-points in the image especially in the case of smooth regions. Two-stage feature point detection is proposed in which fusion of features is used, one feature for textured areas and another one for smooth areas. Furthermore, g2NN is used for feature matching. The method is not robust against geometrical attacks and post-processing operations. The point density can be automatically adjusted over the image in order to concentrate more on the suspected regions[78]. The points of interest are extracted and Polar Cosine Transform (PCT) is used for descriptors. Adaptive matching is utilized and falsely matched descriptors are discarded by effective the filtering process using SLIC and RANSAC algorithms. A rotation robust method is proposed[79] in which the segmented image undergoes angular radial partitioning and then Harris key-points are extracted. The method detects different rotations up to 360 degrees with approximation of rotation angles between duplicated regions.

The method uses a non linear scale space based AKAZE features as key-point extraction method. The drawback of this method is that AKAZE features are slower than most of the key-point algorithms. The small smooth regions are targeted as most of the times such regions escape from the key-point based methods[81]. The Entropy Rate Superpixel (ERS) algorithm is adapted for segmentation, the probability density-based SURF detector is used for key-point extraction and R2gNN is implemented for matching key-points. This approach is computationally more expensive. The problem of fewer key-point extractions is addressed to improve the contrast in images using the Contrast Limited Adaptive Histogram Equalization (CLAHE) algorithm[82]. It operates in small regions and, after CLAHE, key-points are extracted using SURF. To extract sufficient and efficient key-points, a set of hybrid features using SIFT and KAZE is proposed[83]. The hybrid features utilize the strengths of both the features. A neglected attack, i.e. reflection attack is targeted using mirror-SIFT feature extraction and SIFT-symmetry as a matching algorithm[84]. The method has a drawback that it may interpret an original symmetric image as forged. The method uses Multi-Level Dense Descriptor (MLDD) extraction, which included Colour texture descriptor and Invariant moment descriptor to mine dense features instead of existing sparse features[85]. Multiple levels are used in the MLDD method to extract the dense feature descriptors but it is a lengthy and complex method. It can be seen in Table 3 that Wang, Li, and Liu obtained the highest F-score of 0.9680 with SURF features on IMD and GRIP datasets[81].

The main advantages of key-point based CMFD methods are their remarkable performance with respect to computational cost, memory requirement and invariance under rotation and scaling operations, but they still struggle to reduce the false matches in flat regions. Another problem for key-point based methods is extraction of fewer key-points in case of smooth/flat and homogeneous regions.

Block-based copy-move forgery detection methods: a block-based method based on the histogram of oriented gradient is proposed[86] in which the image is divided into overlapping blocks. HOG features are extracted from each block and Euclidean distance matching is performed. The method detects multiple instances of copy-move in a single image but it is not rotation and scale invariant. Another method based on histograms is proposed in which uses a Histogram of Oriented Gabor Magnitude (HOGM)[87]. The method has lower computational complexity and is effective for high resolution images. Image inpainting leaves no traces of tampering as it preserves the texture and structure continuity. It is targeted[88] by using Central Pixel Mapping (CPM) to search for suspicious blocks, greatest zero-connectivity component labelling (GZCL) is used to mark the tampered pixels and finally Fragment

Table 3. Key-point based CMFD methods.

Paper	Features used	Feature dimension	classifier/ matching	Dataset	Performance metric
[75]	SURF	128	Nearest Neighbour Distance Ratio	CMH database (own), CMFD, IFC-TC	TPR = 71.92% FPR = 1.22% Accuracy = 85.35%
[76]	Zernike moments, PCT, FMT	10, 12, 25	Dense Linear Fitting	Image Manipulation Data-set FAU, GRIP	F-score image= 95.92% pixel = 93.72%
[77]	MROGH, Combination of MROGH and HH	192	g2NN	CMFD, MICC-F2000	Precision = 94.0% Recall = 97.9% Fscore = 95.9%
[78]	PCT	_____	RANSAC	IMD, SBU-CM161	Precision, Recall, Fscore
[79]	Harris corner points	______	Euclidean distance matching	CMFD, MICC-F220	Precision = 90% Recall=85% TPR=96% FPR = 2.89% time = 4s
[80]	AKAZE	486	Hamming Distance matching	Google image search, CoMoFoD	TPR = 80% FPR = 2%
[81]	SURF	_____	Rg2NN	IMD FAU, GRIP	F1 score = 0.9680
[82]	SURF	64	g2NN	CMFD	Precision = 93.3% Recall = 87.5% F1 score = 90.3%
[83]	SIFT, KAZE	128, 64	2NN followed by SLIC	CMFD	Precision = 95.45% Recall = 87.25% F-score = 91.11%
[84]	Mirror-SIFT	128	g2NN/ Symmetry matching	CASIA v2.0	F-score = 0.894
[85]	Colour texture, PCET	-,8	Hierarchical Feature Matching	CMFD, CMFDPM	Precision = 91.37% recall = 84..64% Fscore = 87.88%

Splicing detection (FSD) is used for distinguishing the tampered and the non-tampered pixels. A threshold free algorithm[89] detects copy-move forgery in images under various JPEG compression, Gaussian noise and blurring attacks using FFT, SVD and PCA features and they are matched in a cascading manner. The method[90] makes use of cellular automata along with LBP. The method provides lower feature vector complexity and gives a powerful pattern description. Most of the forgery detection methods convert a RGB image into a grey scale image, which discards the colour information of the image. To utilize the colour information, colour moments are used to cluster the blocks[91] according to their colour similarity. The extracted features are fed to Compositional Pattern Producing Network (CPPN) for a deep learning purpose. While Neural Networks can have only a certain type of sigmoidal or radial basis function, CPPN can have a mixture of such functions. The method is not rotation invariant.

To target larger rotations, multi-radius rotation invariant PCET features[92] are used. GPU acceleration is used in order to lower the computational time. The mismatching rate is higher when a JPEG compressed image is blurred. Another method[93] targets multiple copy-move forgery by using fractal coding features which are robust against blur and affine transforms. The method is incapable of extracting features from images with highly uniform areas. To improve the robustness against noise, low frequency components and high frequency components of Zernike moments are used[94] through non-sampling wavelet transform. To deal with the problem of false positives and susceptibility to various image processing operations, invariant quaternion moments[95] are used. Exact Euclidean Locality Sensitive Hashing (E2LSH) is used to adaptively match the features. Finally, false positives are removed using a Random Sample Consensus (RANSAC) algorithm. The method cannot be effectively used in real-time applications as it is computationally more demanding. Another method[96] makes use of colour information of an image by exploiting Colour moments and Colour Layout Descriptors (CLDs). CLDs are extracted for each block and utilize a spatial distribution of the colour in an image irrespective of the resolution. Similar regions are handled by separate threads concurrently to decrease the processing time of the matching process. Blocks are converted into YCbCr colour space first and then corresponding CLD feature vectors are fabricated for each channel. Similarity CLDs are considered as a clue about possible forgery in blocks. The downside of this method is that the execution time increases with an increase in resolution of the image. It has been observed that the major drawback of block-based methods is their computational complexity and there is a need to propose more robust feature extraction methods. The summary of these studies is provided in Table 4. Among all the block-based methods discussed[89], an accuracy of 98% can be obtained by using three different methods in a cascading manner.

Hybrid methods for Copy-move forgery detection: the traditional key-point based methods are improved by employing some properties of block-based methods. Hybrid methods (summarized in Table 5) are used to lower the running time of key-point based methods along with the accuracy of block-based methods. One such method is proposed[97] in which the key-points are extracted using the SIFT algorithm by first segmenting the test image into semantically independent patches using SLIC segmentation with no less than 100 patches so as to cover all the possible forged regions. K-nearest neighbour is used for matching the patches. The EM-based algorithm is then used in order to refine the matching. To overcome the drawbacks of block based methods, adaptive over-segmentation is used[98] to divide the image into blocks and extract key-points from each block using SIFT features. The

Table 4. Block based copy-move forgery detection methods.

Paper	Features used	Feature dimension	classifier/ matching	Dataset	Performance metric
[86]	HOG	4	Euclidean distance matching	CoMoFoD, Google image search	Correct detection ratio, False detection ratio
[87]	Histogram of Oriented Gabor magnitude (HOGM)	12	Euclidean distance matching	CoMoFoD, Image Manipulation Data-set	Correct detection ratio = 98.8% False detection ratio = 2.8%
[88]	Hash values	——	GZCL	2 Databases from literature	Recall = 96.67 Precision = 93.13 ABPT = 468
[89]	FFT, SVD, PCA	9	Cascading matching using Euclidean distances	CASIA v1.0	Accuracy rate = 98% False negative rate = 8%
[90]	Cellular Automata and LBP	128	FLANN	CoMoFoD	Precision = 61.7 Recall = 5.2 F-measure = 67.4
[91]	Colour moments, CLD, CEDD, FCTH, SCD, EHD	50	CPNN	CoMoFoD	Accuracy False negative ratio
[92]	PCET	——	radius ratio	Image manipulation data-set (IMD), Kodak lossless true colour suite	——
[93]	Fractal coding features	4	feature vector matching	MICC F220, MICC F2000, CMFD	Precision Recall
[94]	Wavelet transform, Zernike moments	——	Block feature matching algorithm	CASIA TIDEV1.0	Accuracy = 95.70% False Positive Rate = 4.43% False negative rate = 6.43%
[95]	Invariant quaternion exponent moments (QEMs)	——	E2LSH-based image block matching	CMFD	Precision = 92.45% Recall = 93.67% F-score = 93.06%
[96]	CLD features	64	Euclidean distance matching	CoMoFoD	Accuracy = 0.94

Table 5. Hybrid methods for copy-move forgery detection.

Paper	Features used	Feature dimension	Classifier / matching	Dataset	Performance metric
[97]	SIFT	128	Expectation-Maximization	CMFD, MICC-F600	Precision = 86% Recall = 88%, F-score = 87%
[98]	SIFT	128	Block feature matching algorithm	Image Manipulation Data-set	Precision = 97.22%, Recall = 83.73%, F-score = 89.97%
[99]	SIFT, SURF, Harris	128, 128	Mean Vertex Descriptor	Own database, CMFD	Precision = 61.7 Recall = 5.2 Link precision = 67.4
[100]	RORHFM	____	Pearson Phase correlation	100 images from internet	TPR FPR
[101]	Hue moments, SIFT	______	Nearest Neighbour classifier	MICC F220, MICC F2000	Precision (P) = 97.68 Recall(R) = 96.04 F1 score = 96.85 Accuracy = 92.48
[102]	DSWT and MDS	8	feature vector matching	Kodak truecolor dataset, CoMoFoD	Accuracy Rate = 0.99 False Positive rate = 0
[103]	Behaviour knowledge space	______	fusion of classifier	CMFD	F-measure = 84.14%,
[56]	SIFT, Zernike moments	128, 12	g2NN	CMFD	Precision = 0.7759 Recall = 0.9375 F-score = 0.8491 Running time(s) = 862.5

forgery region extraction method is used to detect the forged regions, which greatly reduces the chances of forgery being undetected and thus improves the recall. Key-points are extracted using three common detectors, namely, SIFT, SURF and Harris corner points[99]. The triangulation is built onto the extracted key-points. The image is divided into triangles, which include pixels with very similar features. In the regions where no key-points are extracted, uniformly arbitrary points are added onto the boundary of the image which helps in subdividing the parts of the image into triangles that have no key-points. The triangles are matched using two characteristics, the dominant and the angles and the areas in the triangle. They are matched using a Mean Vertex Descriptor (MVD). The method is two orders of magnitude faster than block-based methods. In the case of complex scenes, the high number of triangles influences the matching process resulting in worse performance. To improve performance against various operations such as rotation, scaling, translation etc., the Radon odd radial harmonic Fourier moments method[100] is applied with a circle template to extract the geometric inherent features. Radon transform is capable of detecting linear trends and capturing directional properties of these trends. The kernel representation is more complex in RORHFM, which leads to computational complexity because computational complexity and cost of the method is mainly dependent on kernel function.

In another method[101], SIFT and Hue Moments Features are fused together to form a feature. Hue moments are used to acquire the global features, invariant image features are extracted using magnitude coefficients of moments and a SIFT descriptor is used to extract distinct key-points which act as local features. Searching for its nearest neighbour is used as feature vector matching. Another non-intrusive image forgery detection method[102] exists in which DSWT is applied on a pre-processed image and then the LL sub-band is extracted. To decrease feature dimensions, multi-dimensional scaling is performed. The method performs well for small forged regions but the performance degrades for low intensity level changes. Multiscale behaviour knowledge space[103] can also be used to combine the two techniques, i.e. block based and key-point based. The output arrangements of different techniques are encoded as a priori probabilities in multiple scales of the training data. The method is slightly slower than other existing standalone methods. An effective fusion technique is applied to combine key-point and block-based methods[56]. The method first adaptively divides the image into non-overlapped sections with the help of a simple linear iterative clustering (SLIC) algorithm. Then, the SIFT key-point detector is implemented on the entire image. The ratio of the number of key-points extracted to the number of pixels is calculated, and if it is less than a threshold value, a region is categorized as a smooth region or a key-points region. After that, a key-points matching procedure is implemented in key-points regions to check whether the candidate region is forged. Further, the RANSAC algorithm is used to clip outliers. In case there are more than two smooth regions in the image, Zernike moments are used as block features to detect forgery in smooth regions. The detection speed is improved greatly as the block-based method is selectively applied to smooth regions only. It is observed from Table 5 that it obtained the highest F-score of 96.85 by using Hue moments as block features and SIFT for key-point extraction[101].

The drawback of combining block-based methods and key-point based methods is that if the first one is unsuccessful at identifying the forgery and the image is too smooth to have enough key-points, then the fusion approach cannot give accurate results.

Splicing detection methods

Markov features are one of the most effective features for splicing detection. Zhao, Wang, Li, and Li[104] model the adjacent coefficient difference array in two different domains, i.e. BDCT domain and DWT domain as an observation for a 2-D Markov model. The entire feature set is then divided randomly into two sets: one for training and other for testing. The training set finds the optimal hyperplane and the testing set is used to test the effectiveness of the method. The method has high complexity but provides better robustness to JPEG compression and median filtering as compared with methods available in the literature. To hide the traces of splicing, blurring is the commonly performed operation. Local blur-type features are proposed[105], generated by partitioning the image into blocks using a Generalized Gaussian Distribution (GGD). Second, a classifier is formulated to classify the image blocks into out-of-focus or motion blur based on the proposed features. Then, splicing localization is performed. The drawback of this method is that a human decision is needed to indicate the spliced region based on some inconsistencies in the blur type and the semantics of the image. An image is segmented into pixel-centred overlapping image blocks[106]. Each block is resampled by the self-similarity pixel strategy (SSS). Then, the local minimum eigenvalues (LME) of the sample matrix calculated by PCA are analysed. A threshold is set to separate the LMEs into two clusters. The threshold can be obtained by the frequency histogram. In the literature, some methods select a few reference blocks and approximate their illuminants. The reference blocks are compared with a suspicious block to find out the angular error between them. If this value is more than the threshold value, the corresponding block is said to be manipulated. Such methods rely largely on user's perception and interaction capabilities to choose the correct reference blocks. If the reference blocks are not chosen correctly, the performance of the methods is strongly compromised. The method has been proposed to work on this goal[107]. It uses algorithms to estimate IMs, transformed representation of input image, extracting image visuals such as colour, texture and shape and forming feature vectors form the extracted information. In order to classify each new image feature vector, Face Pair classification is performed to learn inter- and intra-class patterns of images. Then, forgery classification and detection is performed.

Image residuals are computed through high-pass filtering, and then they are quantized and truncated[108]. The residuals are then analysed in sliding-window modality, taking square patches with a stride in both directions. Co-occurrences of small patterns along the vertical and horizontal direction are computed within each patch. The histogram of co-occurrences is processed and normalized to form a length-K feature. A simple feedforward autoencoder with a single hidden layer is used and features are fed as input. The method focuses on single image splicing localization. Noise is the most common characteristic of an image and images consists of some type and level of noise, which is produced during the process of acquisition of the image until it is displayed by the device. So, the forgery detection based on noise estimation is proposed[109] in which outlier detection is performed using noise level function. The standard deviation of noise as a function of brightness is known as the noise level function. It depicts the relationship between local noise and brightness. Standard deviation of the noise in each segment is calculated in local noise estimation. A Weiner filter is used for noise level estimation. After calculating the average brightness and noise level of each segment, the data can be projected in a 2-D coordinate representing the correlation among noise and the brightness in the image. The outliers can be easily separated after computing the noise level function. Multi-scale analysis helps in providing visually distinguishable results to observers. Other than noise discrepancy, other detection methods may also be extended to multi-scales for improved performance. Two successive Maximal Entropy Random Walks[66] aim to identify important regions of the input map, and improve visual organization of the output map, respectively. The method considerably improves the localization performance both in terms of ROCs and scores and can be adapted to existing methods for localization as a post-processing step. An efficient splicing detection scheme is proposed using maximization and threshold expansion to construct Markov states for feature extraction[110]. Local statistics in DCT and DWT domain are used[111]. A Local Ternary Pattern (LTP) operator is employed to capture the statistical changes of DCT and DWT coefficients caused by image splicing.

A Sharp transition is introduced by splicing operation in the form of lines, corners, edges, etc. Such sharp transitions are characterized by high frequency components. To detect such transitions, wavelet coefficients can be analysed in order to measure local sharpness or smoothness. So a method[112] based on wavelet transform is proposed using DWT and LBP. Low level coefficients are obtained using Single level discrete wavelet transform. Then, local binary patterns are used to extract the texture of these [LL, LH, HL, HH] components. A histogram of these texture images is considered for effective training and testing of features. The concatenation of LBP histograms is performed and fed to the SVM classifier for training. The method has low computational complexity and is invariant to monotonic illumination changes. But the performance of the method degrades when the size of the image is too small. In another method[113], the colour components are utilized and information pertaining to colour is obtained from blocks of images to construct quaternion. Then QDCT is applied and its coefficients related to the blocks of images are extracted. The expanded Markov features generated from the transition probability matrices in QDCT domain can capture inter-block correlation between its coefficients along with the intra-block QDCT coefficients. Finally, the distinction between authentic and spliced images is made using the feature vector obtained with Primal SVM as a classifier. The L1 norm is used to increase the robustness of the method efficiently[114]. A summary of splicing-based detection methods is given in Table 6, in which it obtained the highest accuracy, of 94.09%[113].

Fusion-based method: fusion methods are used to get good localization for detection results of different approaches. Two forensic approaches are used for forgery localization[115], one is a statistical feature-based approach, the other is a copy-move forgery detection technique. The maps of tampering possibility for each approach is produced which are used for fusion in further steps. The final localization results are obtained by concatenating the possibility maps obtained in the previous step. In the Statistical feature approach, a feature set (Spatial and Colour Rich Model, SCRM) is used. For colour images, the model separates SRM features from the R, B and G channels, puts them together and then adds a subset of features to it which consists of co-occurrence matrices calculated from the image residuals of these three colour channels. This approach is implemented using a sliding window technique. In second approach, a PatchMatch algorithm is used to find out the similar patches in the different areas of images and obtain offset fields for such similar patches. Six different fusion methods are implemented to fuse the two techniques. In some cases, it cannot be distinguished between a source region and a tampered region, so copy move detection fails. If the possibility map of feature-based detection is combined, such a limitation can be improved. The method is complex and has very large dimensionality of features. A

Table 6. Splicing Detection Methods.

Paper	Features used	Feature dimension	classifier/ decision model / matching	Dataset	Performance metric
[104]	Markov based features	14,240	LibSVM	Columbia Image Splicing Detection Data-set (DVMM), UCID, IFC-TC	True positive Rate = 92.99% True Negative Rate = 93.75% Accuracy = 93.36%
[105]	Local Blur kernels	_____	Expectation-Maximization	Own database, Collected from Flickr	True Positive Rate = 93.2% False Positive Rate = 92.4% Accuracy = 92.8%
[106]	Local minimum eigenvalues	_____	Threshold clustering	Columbia	AUC = 0.7193
[107]	Illuminant maps	_____	fusion of classifier, SVM	DSO-1, DSI-1, a set of famous forgery cases from internet	accuracy = 94.0%
[108]	Image residuals	_______	Auto encoder network	acquired from 7 devices, 6 smartphones, DSO-1	f-measure = 0.418
[109]	Local noise estimation	_____	Clustering	Dataset from Y.F. Hsu et. al, 2006	Precision = 81.14% Recall = 94.84%
[112]	DWT and LBP	1024	SVM	CASIA V1, V2, Columbia compressed and uncompressed	accuracy = 94.09%
[110]	Markov based features	972	PrimalSVM	CASIA TIDE V1.0, CASIA TIDE V2.0	Accuracy = 92.38%
[114]	AC filters	64	k-means clustering	Columbia, CASIA v2.0	True positive rate = 91.8% Probability of False acceptance = 10.36%
[113]	Markov based features	95, 170, 85	SVM	CASIA v1.0, CASIA v2.0, Columbia gray DVMM	Accuracy DVMM = 91.83% CASIA v1 = 97.86% CASIA v2 = 93.47%
[111]	LTP	4608	LibSVM	Columbia image Splicing detection data-set	TPR = 92.18% FNR = 92.42% AR = 92.30%

multi-scale analysis approach[116] is investigated which joins a number of candidate tampering maps obtained from scrutiny with various windows to get a reliable, singular tampering map with a more desirable localization resolution. The proposed fusion mechanisms are based on energy minimization (EM fusion) and iterative top-down and bottom-up improvements (TD/BU fusion). An attempt to automatically learn the dependencies between different scales of analysis, is successful to some extent, but is ultimately crippled by the lack of flexibility (Table 7).

Deep learning based: median filtering has been utilized by anti-forensics methods because it has the properties of nonlinearity and conserving edge information of an image, e.g. removing statistical traces of blocking artefacts left by the JPEG compression, or abolishing linear correlations between adjacent pixels for concealing the evidence of re-sampling. So the method[117] aims to use CNN in order to improve performance and to automate the task of feature extraction. The extracted features are fed to two fully connected layers of the CNN and then the output is fed to a softmax function in third fully connected layer. The method fails because the MFR features obtained from the various filtered images may confuse the CNN model, since the differences are perceptibly fewer in them than those in the frequency domain. It has been observed from the literature that with a certain feature, only a particular type of forgery is detected. So there is still a need to develop features that can be used for multiple types of forgeries. A step towards this has been taken[118] in which a new form of convolutional layer is proposed that will force the CNN to learn manipulation detection features. There is no need of preliminary extraction of features or pre-processing. JPEG compression is another issue in image manipulation. A method is proposed[119] that defines a set of noteworthy features that are unaffected by recompression and a one-dimensional CNN is designed to absorb and categorize these features. Computational complexity of the model is considerably high, which generates a trade-off between localization accuracy capability and computational effort required. A deep learning based approach[120] is proposed which has two stages to learn features in order to detect tampered images in different image file formats. For the first stage, a SAE model is utilized to learn the complex feature for individual patches. In the second step, the contextual information of patches is integrated to conduct an accurate detection. The method is applicable to both JPEG and TIFF images but training time was around 13 h, which is a major drawback of the method. Identification of smooth filtering is implemented[121] that can provide trivial information pertaining to forensic analysis by showing the manipulation history. An advanced CNN model, T-CNN, adds a transform layer in advance. In order to capture discernible frequency-domain patterns, the transformation layer is appended ahead of the conventional framework. It is a union of two units: DFT and log-scale transformation. The learned features in this method give better

Table 7. Fusion based methods for copy-move and splicing detection.

Paper	Features used	Feature dimension	Classifier	Dataset	Performance metric
[115]	spatial and colour rich model (SCRM),	18,157	SVM, Patch Match, Fusion decisions	IFS-TC Image Forensics Challenge	F1 score = 0.4925
[116]	mode-based first digit features (MBFDF)	____	SVM	BOSSbase, CMFD	Avg F score = 0.855

performance than manually extracted features. It gives better performance for small sized images and JPEG compression.

The method[122] is based on countering anti-forensic methods using Convolutional Neural Networks. The model is proposed to find highly correlated information, which comprises several layers, such as pooling layers, convolution layers, and fully-connected layers. The outcome of the convolutional layer can be seen as a 3D volume holding neurons. Most of the existing counter anti-forensic methods separate feature extraction and classification, and this model can extract features and form classifications jointly. Another method[123] focuses on various post-processing operations that are used in order to hide the traces of the forgeries. The proposed scheme is able to detect all combinations of median filtering, blurring and Gaussian noise. In this architecture, two convolutional layers and one pooling layer are repeated three times. By stacking these two types of layers, the networks can learn from low-level features to high-level features. There are three fully-connected layers at the end of this CNN architecture. Finally, the network determines whether the image has been manipulated or not by a softmax activation function. The drawback of the method is that false detection is predominant in highly textured regions, very dark regions, and defocused regions. A CNN-based model[124] is obtained on the patch samples from training images. The altered regions in forged images, i.e. boundaries of patches and spliced portions show an elaborately drawn positive patch sample, whereas, the negative ones are sampled randomly. The patch-based features are then extracted for an image using the pre-trained CNN. This is done by using a sliding window of the size of the patch and scanning the whole image. The features based on the patch are concatenated using feature fusion to get a discriminate feature for the image; this is further used to train SVM for forgery detections. The method targets both copy-move and splicing techniques. Thirty basic high-pass filters are used to facilitate the accelerated convergence of the network, instead of using a random weight initializing strategy. In Table 8[118], an accuracy of 99.10% was achieved in comparison to the other deep learning based methods discussed so far.

Traditional techniques for machine learning have a restricted ability of processing raw data, whereas CNN can be useful in that case. A strong universal set of features needs to be developed that does not require any human analysis or a pre-determined model of data. It does not require handcrafted feature extraction. It is able to capture the representation learning automatically. Deep learning based methods such as CNN models can be modified and used for other forensic methods.

Other methods: digital image forgery detection based on shadow consistency is proposed[126]. The fact that the ratio between HSV components on neighbouring surfaces with and without shadows is similar for one image is used for forgery detection. The region with shadow and its neighbouring area is selected. The image is segmented into shadow and non-shadow based on the V component of HSV colour model. Then, the average value for shadow and non-shadow pixels is calculated for both regions of all HSV components. Characteristics are calculated and compared with all other characteristics. The decision whether the region is forged or not is based on the threshold value. The method is simple and rotation invariant but the region has to be selected manually. A method is proposed[127] to find whether image is compressed or decompressed with the help of quantization noise. The method is not complicated and very productive in deciding whether the image under consideration has been JPEG compressed. It is based on the variance of forward quantization noise. The limitation of this method is that it can only distinguish uncompressed images

Table 8. Deep learning based methods.

Paper	Type of forgery targeted	Features used	No. of layers	Model	Dataset	Performance metric
[117]	Median filtering, Cut and Paste	Median Filter Residuals	9	CNN		Detection Accuracy = 85.14%
[118]	Median filtering, Gaussian blurring, AWGN, Resampling	Prediction error filters	8	CNN	Collected from different cameras	Accuracy = 99.10%
[125]	copy move, splicing	residual-based feature	_____	CNN-SVM	from nine devices and four smartphones	accuracy = 99%
[119]	Double JPEG compression	AC coefficients of DCT	7	CNN	UCID, Dresden image database	AUC High resol = 0.86 AUC low resol. = 0.84
[120]	Splicing, copy-move	450 dimensional-3 Level 2D Daubechies Wavelet decomposition	– -	Stacked AutoEncoders (SAE)	Columbia Image Splicing Database, CASIA V1.0, CASIA V2.0	Fall-out = 4.31% Accuracy = 91.09% Precision = 57.67%
[121]	Median Filtering, Gaussian LowPass filtering and Average filtering	DFT and log-scale transformation	7	CNN	UCID, Dresden Image Database, BOSSbase	Accuracy = 97.86
[122]	JPEG antiforensic, Median filtering, Resampling antiforensic, CE antiforensic	Antiforensic features	10	CNN-Cross entropy scheme	BOSSbase, UCID	Detection accuracy (Bossbase) = 96.9% Detection accuracy (UCID) = 94.7%
[123]	Gaussian blurring, Median filtering, Gamma correction	deep learning based	___	CNN	BOSS RAW database, Dresden Image Database	Average Acc = 87.31%
[124]	Splicing, copy-move	Deep learning based	10	CNN-SVM	CASIA v1.0, CASIA v2.0, Columbia DVMM	Acc CASIA v1.0 = 98.04% CASIA v2.0 = 97.83% DVMM = 96.38

from decompressed ones that have not experienced post-processing. The method finds the correlation patterns of CFA to detect the traces of forgeries[128]. The correlation pattern is defined with the posterior probability map. Gaussian models are built based on the residual distribution, which can be automatically reformed to the compression level, to describe the interpolated and un-interpolated pixels. Finally, 2D-DFT is employed on the posterior probability map. The method is robust in order to measure the trace of CFA. These traces are very sensitive as they can be easily destroyed with any kind of modification. The authors[129] developed a technique to detect a forgery either through shadows or reflections using a features-enabled neural network. The training process of the neural network is amended with the projected learning algorithm, called ABCLM, where the Levenberg Marquardt algorithm (LM) and Artificial Bee colony (ABC) algorithms are efficiently incorporated.

The forgeries with geometric distortions[130] are targeted by detecting interpolation signals generated by applying a geometric transform to a digital image, to analyse the tampered direction and position. A modified version of an interpolation signal detection algorithm that uses a re-interpolation technique is implemented. The technique applies a minimum frequency transform to a digital image with a geometric transform to analyse the flow of the overall interpolation signals based on a detection map. Another method[131] targets multiple forgeries and uses Spatial Rich Models in combination with textural features, i.e. the local binary pattern (LBP). Different sub-model selection strategies are implemented and analysed to investigate the performance-to-model dimensionality trade-off. The method[132] focuses on detection of seam carving and seam insertions. The statistical calculation of the blocking effect is performed and stored in a matrix. Twenty-two feature vectors from the BACM are calculated by identifying the symmetry of the matrix. To perform classification, SVM is used. For localization of seam carving, the method takes into account the original image for comparison, otherwise it is hard to find the forged regions. Another method[133] explored a seam carved forgery by using the correlation of adjacent DCT coefficients. A novel image resampling detection algorithm based on blind deconvolution is proposed[64] that can recover the image editing history. The algorithm mainly consists of two stages: kernel extraction with prior knowledge refinement and hierarchical decision fusion. It classifies different types of resampling algorithms, which can be used for copy-move detection and splicing detection but it cannot effectively detect blurred images or flat images. Moreover, the method is time consuming. An Extreme Machine Learning (ELM) based method is proposed[134] based on a local texture descriptor. In this method, the image is first split into its three colour components, i.e. red, green and blue. Next, each colour component is split into blocks without any overlapping, and a LBP histogram is derived from all blocks. Further, all individual histograms are concatenated to obtain the feature vector of the image. Finally, a decision is obtained by feeding the features to an ELM classifier. A summary of these methods is provided in Table 9.

Research challenges and future scope: after critically reviewing the literature collected in a systematic manner, it has been observed that a lot still needs to be done in this field and there are various challenges that need to be dealt with. The future work can be proposed based on these challenges. Some of the most common challenges are:

(1) Feature dimensionality and computational complexity[99,104,115,100,81,92,103,95,64,116,110,134]
(2) Robustness against a high degree of post-processing operations and invariance against geometrical transformations[86,75,76,87,90,135,91,79,114]

Table 9. Other methods for image forgery detection.

Paper	Features used	Feature dimension	classifier/ decision model / matching	Dataset	Performance metric
[126]	Difference of Shadow mask	———	Threshold based classification	Database from Literature	No numerical measurements
[127]	Quantization noise	——	——	BOSSbase 1.01, NRCS photo gallery, UCID, BOWS2, REWIND SYNTHESIS	Accuracy = 99.99%
[128]	Correlation patterns of CFA	———	Gaussian models	UCID, Columbia's ADVENT, CG images from various 3D artists	Accuracy = 97.31% Precision = 87.43% Recall = 88.17%
[129]	Texture consistency, strength consistency	18	FFNN	collected from public resources	Accuracy = 80.49% TPR = 85.16% FPR = below 19% MSE = 0.0010
[130]	Frequency transform	——	———	No benchmark data-set used	——
[131]	LBP with SRM	256	Ensemble multiclass classifier	IFS-TC	Avg. accuracy = 98.4%
[135]	LBP	24	LibSVM	UCID	Accuracy = 85.50%
[132]	BACM features	22	SVM	UCID, UCUS	Accuracy =
[136]	log DFT	——	R-L restoration	from photo sharing apps	accuracy
[133]	Correlation of DCT coefficients	——	Ensemble learning with FLD	2500 images each from 4 different camera	accuracy = 99%
[137]	TF-GLCM	96	LIBSVM	CASIA v 1.0, CASIA v 2.0	Accuracy CASIA v1 = 98.54% CASIA v2 = 97.73%
[134]	LBP	——	ELM	CASIA v 1.0, CASIA v 2.0	Accuracy CASIA V1 = 95.67% CASIA V2 = 97.2%

(3) Slow feature learning rate[120,122,121,119]
(4) Accurate localization of the forgery[127,135,128,124,132,122,123102]
(5) Development of robust statistical features[135,118,80,93]
(6) Lack of dataset that covers all the possible forgery attacks[117,135,126]
(7) Human interpretation needed[105,115,84]

To reduce the feature dimensionality, effective feature reduction methods need to be developed which can preserve the characteristics of the features even when reduced to a certain dimension. Robust statistical features are required in order to make them robust against various post-processing operations and geometrical transformations. To improve the learning rate and learn the features automatically, deep learning based methods may be considered. In order to increase the detection speed, parallel programming or GPU acceleration can be used. Multi-scale analysis can be extended to various forensic methods in order to improve the localization of the forged regions.

Conclusion

A thoughtful systematic survey of the available literature on detection of various image forgery attacks has been conducted, aiming to provide the current state-of-the-art, supported by the classification of various research landscapes and identification of potential challenges. A brief introduction is provided on digital image forgery that allows the reader to gain a better understanding of the behaviours and operations of such forgeries. Subsequently, the systematic review protocol that was used to conduct this survey has been conferred. The research questions defined in this work aim to comprehensively embrace all potential facets of the selected primary studies. These facets include various forgeries, detection features, detection approaches, modelling methods, datasets used and software tools employed.

The search was conducted in two phases using a systematic approach to obtain the relevant research literature. Five different electronic databases, namely *ACM Digital Library*, *IEEE Xplore*, *ScienceDirect*, *Springer* and *Google Scholar* were used. The search string was validated using a pilot study to ensure comprehensive literature coverage resulting from the execution of the search process. Moreover, the reference checking stage also amalgamated the survey process. Out of 2631 search results, a total of 66 studies qualified our study selection and quality criteria. These 66 studies were then thoroughly examined to answer the research questions. The final list of primary studies considered by this survey comprised studies that were published before July 2017.

In summary, this work contributes toward the area of detection of digital image forgeries in a number of ways. Through a detailed study of all high quality works following a systematic approach, a state-of-the-art taxonomy is provided to represent various image forgeries followed by a comprehensive examination of the detection features. The detection methods are also categorized on the basis of approaches and modelling methods. Further, various datasets related to the field of image forensics used in various primary studies are also explored. It is anticipated that the readers of this survey paper will be able to acquire a detailed understanding of various fundamentals related to the detection of digital image forgeries. In addition, the limitations and challenges listed in this paper are expected to provide researchers with promising future directions.

Disclosure statement

No potential conflict of interest was reported by the authors.

ORCID

Savita Walia http://orcid.org/0000-0002-8755-2873
Krishan Kumar http://orcid.org/0000-0001-9877-0238

References

1. Farid H. Image forgery detection. IEEE Signal Process Mag. 2009;26(2):16–25.
2. Reis G. Digital image integrity. San Jose, CA; 1999.
3. Photo Tampering throughout history. Fourandsix Technologies, Inc. [Online]. [cited 2017 Aug 18]. Available from: http://pth.izitru.com/
4. Mhiripiri NA, Chari T. Media law, ethics, and policy in the digital age. United States of America: IGI Global; 2017.
5. Birajdar GK, Mankar VH. Digital image forgery detection using passive techniques : a survey. Digit Investig. 2013;10(3):226–245.
6. Ali M, Deriche M. A bibliography of pixel-based blind image forgery detection techniques. Signal Process Image Commun. 2015;39:46–74.
7. Abd Warif NB, Abdul Wahab AW, Idna Idris MY, Ramli R, Salleh R, Shamshirband S, Choo KR. Copy-move forgery detection : survey, challenges and future directions. J Netw Comput Appl. 2016;75:259–278.
8. Mahmood T, Nawaz T, Ashraf R, Shah M, Khan Z, Irtaza A, Mehmood Z. A survey on block based copy move image forgery detection techniques. International Conference on Emerging Technologies (ICET), 2015.
9. Dada A, Dharaskar RV, Thakare VM. A survey on keypoint based copy-paste forgery detection techniques. Procedia Comput Sci 78 December 2015: 61–67, 2016.
10. Asghar K, Hussain M. Copy-move and splicing image forgery detection and localization techniques : a review. Aust J Forensic Sci. 2017;49(3):281–307.
11. Anoop AM. Image forgery and its detection : a survey. In: International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), 2015, pp. 1–9.
12. Bharti CN. A survey of image forgery detection techniques. In: *International Conference onWireless Communications, Signal Processing and Networking (WiSPNET)*, 2016, pp. 877–881.
13. Nirmalkar N. A Review of Image Forgery Techniques and their Detection. In: *International Conference onInnovations in Information, Embedded and Communication Systems (ICIIECS)*, 2015.
14. Khapare AP, Phalke DA. Approaches for camera source identification : a review. Int J Enginnering Comput Sci. 2017;6(1):19977–19979.
15. Babar MA, Zhang H. Systematic literature reviews in software engineering: preliminary results from interviews with researchers. In Int Symp Empirical Softw Eng Meas, 2009, pp. 346–355.
16. Kitchenham B, Pretorius R, Budgen D, Brereton OP, Turner M, Niazi M, Linkman S. Systematic literature reviews in software engineering - a tertiary study. Inform Softw Technol. 2010;52(8):792–805.
17. Abdelmaboud A, Jawawi DNA, Ghani I, Elsafi A, Kitchenham B. Quality of service approaches in cloud computing: a systematic mapping study. J Syst Softw. 2015;101:159–179.
18. Iankoulova I, Daneva M. Cloud computing security requirements: a systematic review. Int Conf Research Challenges Inform Sci. 2012:1–7.
19. Jula A, Sundararajan E, Othman Z. Cloud computing service composition: a systematic literature review. Expert Syst Appl. 2014;41(8):3809–3824.
20. Singh K, Singh P, Kumar K. A systematic review of IP traceback schemes for denial of service attacks. Comput Secur. 2016;56:111–139.

21. Singh K, Singh P, Kumar K. Application layer HTTP-GET flood DDoS attacks: research landscape and challenges. Comput Secur. 2017;65:344–372.
22. Kitchenham BA. Systematic review in software engineering: where we are and where we should be going. Int Workshop Evidential Assess Softw Technol. 2012:1–2.
23. Brereton MOP, Kitchenham BA, Budgen D, Turner M, Khalil M. Lessons from applying the systematic literature review process within the software engineering domain". J Syst Softw. 2007;80(4):571–583.
24. Mallett R, Hagen-Zanker J, Slater R, Duvendack M. The benefits and challenges of using systematic reviews in international development research. J Dev Eff. 2012;4(3):445–455.
25. Farid H. Digital doctoring: Can we trust photographs? Decept From Anc Empires to Internet Dating. 2009:95–108
26. Adobe Photoshop elements. Adobe Syst; 2016. [Online]. [cited 2017 Sep 9]. Available from: http://www.adobe.com/in/products/photoshop-elements.
27. PIXLR. [Online]. [cited 2017 Sep 9]. Available from: https://pixlr.com/.
28. GNU image manipulation program (GIMP); 2017. [cited 2017 Sep 9]. Available from: https://www.gimp.org/.
29. Piva A. An Overview on Image Forensics. ISRN Signal Process. 2013;2013:1–22.
30. Fridrich J L J, Soukal D. Detection of copy-move forgery in digital images. Digit Forensic Res Workshop. 2003:55–61.
31. Zhang Z, Zhou Y. Study of image splicing detection. Adv Intell Comput Theor Appl Asp Theor Methodol Issues. 2008;5226:1103–1110.
32. Nguyen HC, Katzenbeisser S. Robust resampling detection in digital images. in International Conference on Communications and Multimedia Security; 2012, pp. 3–15.
33. Lyu S, Farid H. How realistic is photorealistic? IEEE Trans Signal Process. 2005;53(2):845–850.
34. Gloe T, Kirchner M, Winkler A, Böhme R. Can we trust digital image forensics? in 15th Int. Conf. Multimedia; 2007, pp. 78–86.
35. Stamm MC, Liu KJR. Anti-forensics of digital image compression. IEEE Trans Inf Forensics Secur. 2011;6(3):1050–1065.
36. Choi KS, Lam EY, WongKKY. Source camera identification using footprints from lens aberration. Proceedings Volume 6069, Digital Photography II; 60690J. 2006. https://doi.org/10.1117/12.649775.
37. Geradts ZJ, Bijhold J, Kieft M, Kurosawa K, Kuroki K, Saitoh N. Methods for identification of images acquired with digital cameras in Proc. of SPIE, Enabling Technologies for Law Enforcement and Security; 2001.
38. Lukas J, Fridrich J, Goljan M. Digital camera identification from sensor pattern noise. IEEE Trans Inf Forensics Secur. 2006;2(1):205–214.
39. Bayram S, Sencar HT, Memon N, Avcibas I. Source camera identification based on CFA interpolation. in IEEE International Conference on Image Processing (ICIP); 2005.
40. Kharrazi M, Sencar HT, and Memon N. Blind source camera identification. in IEEE International Conference on Image Processing (ICIP); 2004.
41. Farid H, Bravo MJ. Perceptual discrimination of computer generated and photographic faces. Digit Investig. 2012;8(3):226–236.
42. Wang Y, Moulin P. On discrimination between photorealistic and photographic images. in IEEE International Conference on Acoustics, Speech and Signal Processing; 2006.
43. Dehnie S, Sencar HT, Memon N. Digital image forensics for identifying computer generated and digital camera images. in IEEE International Conference on Image Processing; 2006, pp. 2313–2316.
44. Khanna N, Chiu GT-C, Allebach JP, Delp EJ. Forensic techniques for classifying scanner, computer generated and digital camera images. in IEEE International Conference on Acoustics, Speech, and Signal Processing; 2008, pp. 1653–1656.
45. Haouzia A, Noumeir R. Methods for image authentication: a survey. Multimed Tools Appl. 2008;39(1):1–46.
46. Singh P, Chadha RS. A survey of digital watermarking techniques, applications and attacks. Int J Eng Innov Technol. 2013;2(9):165–175.

47. Wang X, Xue J, Zheng Z, Liu Z, Li N. Image forensic signature for content authenticity analysis. J Vis Comun Image Represent. Jul. 2012;23(5):782–797.
48. Cox I, Miller ML, Bloom JA. Digital watermarking. San Francisco, CA, USA: Morgan Kaufmann Publishers Inc.; 2002.
49. Friedman GL. The trustworthy digital camera: restoring credibility to the photographic image. IEEE Trans Consum Electron. 1993;39(4):905–910.
50. Rey C, Dugelay J-L. A survey of watermarking algorithms for image authentication. EURASIP J Adv Signal Proc. 2002;2002(6):613–621.
51. Langelaar GC, Setyawan I, Lagendijk RL. Watermarking digital image and video data. a state-of-the-art overview. IEEE Signal Proc Mag. 2000;17(5):20–46.
52. Tafti AP, Malakooti MV, Ashourian M, Janosepah S. Digital image forgery detection through data embedding in spatial domain and cellular automata. 7th International Conference on Digital Content, Multimedia Technology and its Applications (IDCTA); 2011:11–15.
53. Elwin JGR, Aditya TS, Shankar SM. Survey on passive methods of image tampering detection. Proceedings of the International Conference on Communication and Computational Intelligence; 2010 Dec 27–29; Perundurai, Erode: Kongu Engineering College; 2003. p. 431–436.
54. Qazi T, Hayat K, Khan SU, Madani SA, Khan IA, Kolodziej J, Li H, Lin W, Yow KC, et al. Survey on blind image forgery detection. IET Image Proc. 2013;7(7):660–670.
55. Christlein CRV, Jordan J, Riess C, Angelopoulou E. An evaluation of popular copy-move forgery detection approaches. IEEE Trans Inf Forensics Secur. 2012;7(6):1841–1854.
56. 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. 2016;27(4):989–1005.
57. Sreelakshmy IJ, Anver J. An improved method for copy-move forgery detection in digital forensic. in Online International Conference on Green Engineering and Technologies (IC-GET); 2016.
58. Farid H. Detecting digital forgeries using bispectral analysis. in AI Lab, Massachusetts Institute of Technology; 1999, p. Tech. Rep. AIM-1657.
59. Ng TT, Chang SF. A model for image splicing. in International Conference on Image Processing (ICIP); 2004.
60. Lin Z, Wang R, Tang X, Shum H-Y. Detecting doctored images using camera response normality and consistency. Recognition, IEEE conference on computer vision and pattern (CVPR); 2005, pp. 1087–1092.
61. Fontani M, Bianchi T, De Rosa A, Piva A, Barni M. A framework for decision fusion in image forensics based on Dempster Shafer theory of evidence. IEEE Trans. Inf. Forensics Secur. 2013;8(4):593–607.
62. Kharrazi M, Sencar HT, Memon ND. Improving steganalysis by fusion techniques: a case study with image steganography. Trans Data Hiding Multimed Secur. 2006;4300:123–137.
63. Kirchner M, Gloe T. "On resampling detection in re-compressed images", in First IEEE International Workshop on Information Forensics and Security, 2009. WIFS. 2009;2009:21–25.
64. JVCIR, Su Y, Jin X, Zhang C, Chen Y. Hierarchical image resampling detection based on blind deconvolution q. J Vis Commun Image Represent. 2017;48:480–490.
65. Kirchner M, Fridrich J. On detection of median filtering in digital images. Proceedings of the SPIE, Electronic Imaging, Media Forensics and Security XII, San Jose, CA, USA; January 2010. 2010.
66. Kang X, Stamm MC, Peng A, Liu KJR. Robust median filtering forensics using an autoregressive model. IEEE Trans. Inf. Forensics Secur. 2013;8(9):1456–1468.
67. Chen C, Ni J, Huang R, Huang J. Blind median filtering detection using statistics in difference domain. In 14th international conference on Information Hiding; 2012, pp. 1–15.
68. Yuan H. Blind forensics of median filtering in digital images. IEEE Trans Inf Forensics Secur. 2011;6(4):1335–1345.
69. Garg A, Hailu A, Sridharan R. Image forgery identification using jpeg intrinsic fingerprints. 2008:1–6.
70. Zach F, Riess C, Angelopoulou E. "Automated image forgery detection through classification of JPEG Ghosts", DAGM/OAGM 2012. Pattern Recognit. 2012;7476:185–194.
71. Bianchi T, Piva A. Detection of non-aligned double JPEG compression based on integer periodicity maps. IEEE Trans Inf Forensics Secur. 2012;7(2):842–848.

72. Johnson MK, Farid H. Exposing digital forgeries by detecting inconsistencies in lighting. ACM Multimedia and Security Workshop '05 New York, NY, USA. 2005:1–10.
73. Johnson MK, Farid H. Exposing digital forgeries in complex lighting environments. IEEE Trans Inf Forensics Secur. 2007;2(3):450–461.
74. Kee E, Farid H. Exposing digital forgeries from 3-D lighting environments, in IEEE Int. Forensics Security: Conf. on Inf; 2010.
75. 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. 2015;29:16–32.
76. Cozzolino D, Poggi G, Verdoliva L. Efficient dense-field copy – move forgery detection. IEEE Trans Inf Forensics Secur. 2015;10(11):2284–2297.
77. Yu L, Han Q, Niu X. Feature point-based copy-move forgery detection : covering the non-textured areas. Multimed Tools Appl. 2016;75(2):1159–1176.
78. Zandi M, Mahmoudi-aznaveh A, Talebpour A. Iterative copy-move forgery detection based on a new interest point detector. IEEE Trans Inf Forensics Secur. 2016;11(11):2499–2512.
79. Uliyan DM, Jalab HA, Wahab AWA, Sadeghi S. Image region duplication forgery detection based on angular radial partitioning and Harris key-points. Symmetry (Basel). 2016;8(7):62–81.
80. Ulutas G, Muzaffer G. A new copy move forgery detection method resistant to object removal with uniform background forgery. Math Probl Eng. 2016;2016:1–19.
81. Wang X, Li S, Liu Y. A new keypoint-based copy-move forgery detection for small smooth regions. Multimed Tools Appl. 2016;2017(22):23353–23382.
82. Zhang W, Yang Z, Niu S, Wang J. Detection of copy-move forgery in flat region based on feature enhancement. In: Shi Y, Kim H, Perez-Gonzalez F, Liu F, editors. Digital Forensics and Watermarking. IWDW 2016. Lecture Notes in Computer Science, vol 10082. Springer, Cham; 2017. 2017:159–171.
83. Yang F, Li J, Lu W, Weng J. Copy-move forgery detection based on hybrid features. Eng Appl Artif Intell. 2017;59, no. December 2016:73–83.
84. Abdul Warif NB, Abdul Wahab AW, Idna Idris MY, Fazidah Othman RS. SIFT-Symmetry : A robust detection method for copy-move forgery with reflection attack. J Vis Commun Image Represent. 2017;46:219–232.
85. Bi X, Pun CM, Yuan XC. Multi-level dense descriptor and hierarchical feature matching for copy-move forgery detection. Inf Sci (NY). 2016;345:226–242.
86. Lee J-C, Chang C-P, Chen W-K. Detection of copy-move image forgery using histogram of orientated gradients. Inf Sci (NY). 2015;321:250–262.
87. Lee J-C. Copy-move image forgery detection based on Gabor magnitude. J Vis Commun Image Represent. 2015;31:320–334.
88. Liang Z, Yang G, Ding X, Li L. An efficient forgery detection algorithm for object removal by exemplar-based image inpainting. J Vis Commun Image Represent. 2015;30:75–85.
89. Huang D, Huang C, Hu W, Chou C. Robustness of copy-move forgery detection under high JPEG compression artifacts. Multimed Tools Appl. 2017;76(1):1509–1530.
90. Tralic D, Grgic S, Sun X, Rosin PL. Combining cellular automata and local binary patterns for copy-move forgery detection. Multimed Tools Appl. 2016;75(24):16881–16903.
91. Zhou H, Shen Y, Zhu X, Liu B, Fu Z, Fan N. Digital image modification detection using color information and its histograms. Forensic Sci Int. 2016;266:379–388.
92. Wo Y, Yang K, Han G, Chen H, Wu W. Copy-move forgery detection based on multi- radius PCET. IET Image Process. 2016;11(2):99–108.
93. Jenadeleh M, Moghaddam ME. Blind detection of region duplication forgery using fractal coding and feature matching. J Forensic Sci. 2016;61(3):623–636.
94. Jinke X, Guangdong Z. Image forgery detection algorithm based on non sampling wavelet transform and Zernike moments. Int J Secur Its Appl. 2016;10(2):27–38.
95. Wang X, Liu Y, Xu H, Wang P, Yang H. Robust copy-move forgery detection using quaternion exponent moments. Pattern Anal Appl. 2016;2016:1–17. https://doi.org/10.1007/s10044-016-0588-1.
96. Ustubioglu B et al. Improved copy-move forgery detection based on the CLDs and colour moments. Imaging Sci J. 2016;64(4).

97. Li J, Li X, Yang B, Sun X. Segmentation-based image copy-move forgery detection scheme. IEEE Trans Inf Forensics Secur. 2015;10(3):507–518.
98. Pun CM, Yuan XC, Bi XL. Image forgery detection using adaptive oversegmentation and feature point matching. IEEE Trans Inf Forensics Secur. 2015;10(8):1705–1716.
99. Ardizzone E, Bruno A, Mazzola G. Copy-move forgery detection by matching triangles of keypoints. IEEE Trans Inf Forensics Secur. 2015;10(10):2084–2094.
100. Zhong J, Gan Y, Xie S. Radon odd radial harmonic Fourier moments in detecting cloned forgery image. Chaos Solitons Fractals. 2016;89:115–129.
101. Tatkare KA, History A. Fusion of sift and hue moments features for cloning tamper detection, in International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT);2015, pp. 409–414.
102. Thirunavukkarasu V, Kumar JS, Chae GS, Kishorkumar J. Non-intrusive forensic detection method using DSWT with reduced feature set for copy-move image. Wirel Pers Commun. 2017:1–19. https://doi.org/10.1007/s11277-016-3941-1.
103. Ferreira A, Felipussi SC, Alfaro C, Fonseca P, Vargas-Muñoz JE, dos Santos JA, Rocha A. Behavior knowledge space-based fusion for copy-move forgery detection. IEEE Trans Image Process. 2016;25(10):4729–4742.
104. Zhao X, Wang S, Li S, Li J. Passive image splicing detection by a 2-D Noncausal Markov Model. IEEE Trans Circuits Syst Video Technol. 2015;25(2):185–199.
105. Bahrami K, Kot AC, Li L, Li H. Blurred image splicing localization by exposing blur type inconsistency. IEEE Trans Inf Forensics Secur. 2015;10(5):999–1009.
106. Zhan L, Zhu Y, Mo Z. An image splicing detection method based on PCA minimum eigenvalues. J Inf Hiding Multimed Signal Process. 2016;7(3):610–619.
107. Carvalho T, Faria FA, Pedrin H, Torres RS, Rocha A. Illuminant-based transformed spaces for image forensics. IEEE Trans Inf FORENSICS Secur. 2016;11(4):720–733.
108. Cozzolino D, Verdoliva L. Single-image splicing localization through autoencoder-based anomaly detection, in IEEE International Workshop on Information Forensics and Security (WIFS);2016.
109. J. V. C. I. R, Pun C, Liu B, Yuan X. Multi-scale noise estimation for image splicing forgery detection. J Vis Commun Image Represent. 2016; 38:195–206.
110. Han JG, Park TH, Moon YH, Eom IK. Efficient Markov feature extraction method for image splicing detection using maximization and threshold expansion," J Electron Imaging. 2016;25(2):023031. https://doi.org/10.1117/1.JEI.25.2.023031.
111. Zhang Y, Li S, Wang S, Zhao X. Identifying image splicing based on local statistical features in DCT and DWT domain. In: Mu J, Liang Q, Wang W, Zhang B, Pi Y, editors. The proceedings of the third international conference on communications, signal processing, and systems. Lecture Notes in Electrical Engineering, vol 322. Cham: Springer, pp. 723–731.
112. Kaur M, Gupta S. A passive blind approach for image splicing detection based on DWT and LBP histograms. Int Symp Secur Comput Commun. 2016:318–327.
113. Li C. Image splicing detection based on Markov features in QDCT domain. Neurocomputing. 2017;228:29–36.
114. He X, Guan Q, Tong Y, Zhao X. a novel robust image forensics algorithm based on L1-norm estimation. International Workshop on Digital Watermarking. 2017;2:145–158.
115. Li H, Luo W, Qiu X, Huang J. Image forgery localization via integrating tampering possibility maps. IEEE Trans Inf Forensics Secur. 2017;12(5):1240–1252.
116. Korus P, Huang J. Multi-scale fusion for improved localization of malicious tampering in digital images. IEEE Trans Image Process. 2016;25(3):1312–1326.
117. Chen J, Kang X, Liu Y, Wang ZJ. Median filtering forensics based on convolutional neural networks. IEEE Signal Process. Lett. 2015;22(11):1849–1853.
118. Bayar B, Stamm MC. 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 - IH&MMSec '16; 2016, pp. 5–10.
119. Wang Q, Zhang R. Double JPEG compression forensics based on a convolutional neural network. EURASIP J Inf Secur. 2016;2016:23. https://doi.org/10.1186/s13635-016-0047-y.

120. Zhang Y, Goh J, Lei L, Thing V. Image region forgery detection : a deep learning approach. Singapore Cyber-Security Conf. 2016;14:1–11.
121. Liu A, Zhao Z, Zhang C, Su Y. Smooth filtering identification based on convolutional neural networks. Multimed Tools Appl. 2016:1–15.
122. Yu J, Zhan Y, Yang J Xiangui KB. A multi-purpose image counter-anti-forensic method using convolutional neural networks. In International Workshop on Digital Watermarking. 2017:3–15.
123. Choi, H, et al. Detecting composite image manipulation based on deep neural networks. Int. Conf. Syst. Signals Image Process; 2017.
124. Rao Y, Ni J. A deep learning approach to detection of splicing and copy-move forgeries in images. IEEE Int Work Information Forensics Secur. 2016. https://doi.org/10.1109/WIFS.2016.7823911.
125. Cozzolino D, Poggi G, Verdoliva L. "Recasting Residual-based Local Descriptors as Convolutional Neural Networks: an Application to Image Forgery Detection", in 5th ACM Workshop on Information Hiding and Multimedia. Security. 2017;159–164.
126. Tuba V, Jovanovic R, Tuba M. Digital Image Forgery Detection Based on Shadow HSV Inconsistency. In 5th International Symposium on Digital Forensic and Security (ISDFS); 2017.
127. Li B, Ng T, Li X, Tan S. Revealing the trace of high-quality JPEG compression through quantization noise analysis. IEEE Trans Inf Forensics Secur. 2015;10(3):558–573.
128. Li L, Xue J, Wang X. A robust approach to detect digital forgeries by exploring correlation patterns. Pattern Anal Appl. 2015;18(2):351–365.
129. Cristin R, Raj VC. Consistency features and fuzzy-based segmentation for shadow and reflection detection in digital image forgery. Sci China Inf Sci. 2017;2017:60, 082101. https://doi.org/10.1007/s11432-016-0478-y.
130. Hwang M, Kim S, Har D. A method of identifying digital images with geometric distortion. Aust J Forensic Sci. 2017;49(1):93–105.
131. Farooq S, Yousaf MH, Hussain F. A generic passive image forgery detection scheme using local binary pattern with rich models. Comput Electr Eng. 2017;62:459–472.
132. Wattanachote K, Shih TK, Member S, Chang W, Chang H. Tamper detection of JPEG image due to seam modifications. IEEE Trans Inf Forensics Secur. 2015;10(12):2477–2491.
133. Liu Q. An approach to detecting JPEG down-recompression and seam carving forgery under recompression anti-forensics. Pattern Recognit. 2017;65:35–46.
134. Alhussein M. Image tampering detection based on local texture descriptor and extreme learning machine. In 18th International Conference on Computer Modelling and Simulation; 2016, pp. 196–199.
135. Yin T, Yang G, Li L, Zhang D. Detecting seam carving based image resizing. Comput Secur. 2015;55:130–141.
136. Zeng F, Wang W, Tang M, Cao Z. Exposing Blurred Image Forgeries through Blind Image Restoration. In 10th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC);2015, pp. 466–469.
137. Shen X, Shi Z, Chen H. Splicing image forgery detection using textural features based on the gray level co-occurrence matrices. IET Image Process. 2017;11(1):44–53.