A Study on Source Device Attribution Using Still Images

Surbhi Gupta, Neeraj Mohan & Munish Kumar

Archives of Computational Methods in Engineering
State of the Art Reviews

ISSN 1134-3060

Arch Computat Methods Eng
DOI 10.1007/s11831-020-09452-y

Springer

Archives of Computational Methods in Engineering
https://doi.org/10.1007/s11831-020-09452-y

ORIGINAL PAPER

A Study on Source Device Attribution Using Still Images

Surbhi Gupta[1] · **Neeraj Mohan**[2] · **Munish Kumar**[3]

Received: 24 November 2019 / Accepted: 1 June 2020

Abstract
Images are acquired and stored digitally these days. Image forensics is a science which is concerned with revealing the underlying facts about an image. The universal approaches provide a general strategy to perform image forensics irrespective of the type of manipulation. Identification of acquisition device is one of the significant universal approach. This review paper aims at analyzing the different types of device identification approaches. All research papers aiming camera and mobile detection using image analysis were acquired and then finally 60 most suitable papers were included. Out of these, 32 states of art papers were critically analyzed and compared. As every research starts with the literature review such analysis is significant. This is the first attempt for source camera and source mobile detection evaluation as per the authors knowledge. The authors have concluded that the Accuracy rate of Lens Aberration based detection techniques deteriorates when the different source camera from same brand were under consideration. The performance of color filter array Based Detection techniques dropped when the post processing operation were used on images. These techniques were vulnerable to high compression rate for JPEG images.

1 Introduction to Image Forgery and Forensics

An image is a grouping of pixels. These pixels are arranged in rows and column to depict an image in a 2-dimensional structure. Each pixel has some area and intensity value associated with it as exhibited in Fig. 1. Intensity values at respective areas constitute an image. An image processing operation will result in the modification of intensity value of pixels in an image. The amount of change in pixel intensity depends on the image processing procedure. For example, if the brightness of an image needs to be increased or contrast needs to be enhanced; the intensity value of the pixels needs to be altered slightly. While if one object needs to be translated or rotated in the image, then the intensity values of the pixels need to be changed altogether. An image is characterized by its color depth and resolution. The color depth of an image is controlled by the quantity of bits (k) required to represent an image pixel. Generally, a pixel is represented by 24 bits; 8-bit for each Red, Green and Blue (R, G and B) plane, thus resulting in color depth of 2^{24} colors in the image. Another significant attribute of an image is its resolution. It is equivalent to the quantity of pixels present in an image. It is determined as the product of the number of rows (m) and number of columns (n) of pixels present in an image, i.e. 'm × n'. Resolution and color depth of an image has a direct impingement on the image size. The image size is determined as 'm × n × k'. The image size increases when either number of pixels, or the color depth increases. A good quality image, having high resolution and high color depth, would have a larger image size as compared to a poor-quality image with the same visual substance. There are many file formats available for images like BMP, TIFF, PNG and JPEG. Some of them offer information preservation while others offer less memory consumption. The selection of file format depends on the usage and purpose of the image. One must consider file size, application and image quality before selecting an appropriate file format. Image formats such as BMP, PNG and TIFF use a lossless compression scheme and maintain the quality of the image; while lossy compression file formats like GIF and JPEG sacrifices image quality for

✉ Munish Kumar
munishcse@gmail.com

[1] Department of Computer Science and Engineering, Gokaraju Rangaraju Institute of Engineering and Technology, Hyderabad, Telangana, India

[2] Department of Computer Science and Engineering, I.K.G. Punjab Technical University, Mohali Campus, Mohali, Punjab, India

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

Published online: 08 June 2020

Fig. 1 Image and its representation

file size. Lossy file formats specifically discard some information from the image in such a way that no visual discrepancies appear. These lossy file formats may have different quality factors based on the amount of information discarded or quality degradation in the image. Thus, color depth, resolution, and image format are the basic characteristics of an image and are the basis for processing and manipulations in a digital image [30, 51].

Images have become indispensable in the present digital era. Earlier, images were considered as the evidence of events, but nowadays images could not be trusted blindly. Due to easy availability of image manipulation tools, the images are prone to various types of tampering and this is known as image forgery. Whenever an image is presented as facts, it must be first checked for its authenticity and originality. This is achieved by image forensics. Image forensics is a science which is concerned with revealing the underlying facts about an image. Images are acquired and stored digitally these days. Digital image forensics (DIF) achieves authentication of images by examining their digital version. DIF can validate and verify the image origin and authenticity. It can provide answers to various questions about images such as

- 'Is this image an authentic image or a composition of different images from different sources?'
- 'What was the make of camera or printer used?'
- 'What is the time, date and location for capturing?'
- 'Is it digitally tampered to mislead the viewer?'
- 'Does it hide secret messages behind it?'

Most of the accessible methods embed security features in images/documents. These methods are expensive and practically difficult to use. The need is to have easy, fast and low-cost solutions, to detect forged images/documents. A passive approach detects the image/document authenticity based on its intrinsic fingerprints. It does not use any preventive measure in advance. Passive techniques can be classified as intended or universal. Intended passive forensics (IPF) class of passive techniques aims at detecting specific type of image forgery detection. These approaches are based on two major operations i.e. copy-move and image splicing. The intended approaches have clear intensions to identify a specific type of image forgery. The universal passive forensics (UPF) class of approaches is general in nature. They can be employed to detect any type of digital forgery. These approaches look for general disturbances in images which appear due to manipulations.

2 Contribution and Motivation of this Paper

The universal passive forensics (UPF) is a much-evolved domain in image forensics. One part of UPF targets at identifying the source/acquisition device of the questioned image. Acquisition process introduces hardware-based fingerprints in the images. It is possible to identify the acquisition device using these fingerprints. Regardless of other properties of the image this technique aims at identifying the source of the image. If the characteristics of the source device of the image does not match the expected device, it gives a clue of manipulation in the image. One approach for image source identification is to verify a feature vector that can recognize the uniqueness of a digital camera, and then use those features to classify images originating from a specific camera. When a part of the image is replaced by a part of another image, acquired with a different device or settings, the regular characteristics of the image gets disturbed. The discrepancy of the intrinsic fingerprints from various regions can reveal such type of image tampering. A few approaches based on different source elements from the image acquisition pipeline exist (as depicted in Fig. 2).

Some of these approaches are based on lens aberration, sensor pattern noise, CFA pattern, demosaicing and

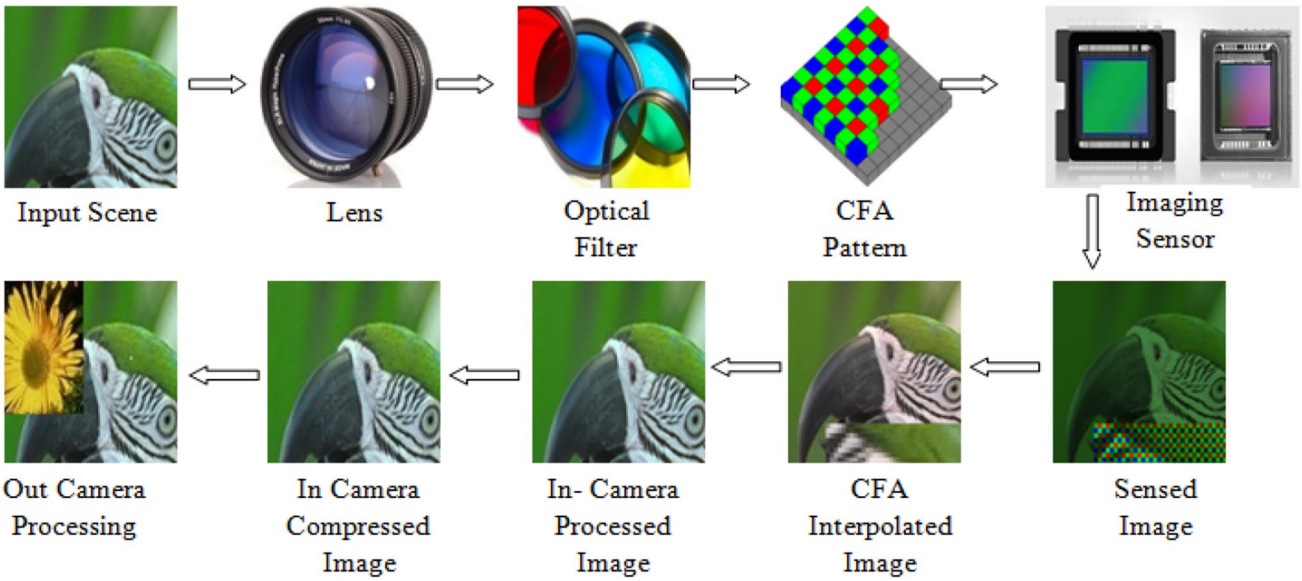

Fig. 2 Production of a digital image

gamma correction. As a lot of literature is available and the research is still on, a constructive review of this domain is very much required. A lot of analysis has been presented for copy, move, image splicing and passive forensics, but it is not there for source device attribution. The authors have presented one novel approach for printer device attribution [31] and now the attempt is camera attribution. But as the first step is review of state of art, the author fails to find a critical review for the same. This is the first attempt to analyze the existing techniques for camera device attribution to the best of our knowledge. The aim of this review is:

- To analyze the basic model of hand crafted and deep learned approach for CDI.
- To compare and statistically analyze the different hand-crafted machine learned approaches.
- To compare and statistically analyze the deep learned approaches.
- To provide the future direction for the research in this domain.

3 Brief Overview of Universal Passive Forensics (UPF)

The universal approaches provide a general strategy to perform image forensics irrespective of the type of manipulation. These approaches are based on the acquisition, coding or editing fingerprints [48].

- Acquisition Fingerprints

A digital acquisition device has various components. These components tend to alter the input signal in some ways and leave intrinsic fingerprints in the image. Camera optical system, the image sensor and camera software have their unique fingerprints. Even if the acquisition steps remain same but still the fingerprints of sensors and camera may differ due to use of hardware from different manufacturers. The traces vary with the specific camera brand and/or model. Each hardware part will introduce some distinctive fingerprints on the image. This fingerprint is unique for every lens, camera, sensor or CFA. One can even distinguish the individual device from the same manufacturer. These features are obvious and intentional. The absence of coherence in these fingerprints can be taken as a clue of image forgery.

- Coding Fingerprints

Different coding architectures have different characteristic fingerprints. Most of the camera devices usually follow lossy compression while coding the image acquired. This compression coding leaves its characteristic fingerprints on the image. These characteristics may even reveal the processing history of a compressed image. The presence of disturbances in the coding artifacts can be taken as an evidence of tampering. JPEG image analysis is widely used for this purpose. Every manipulated image needs to be encoded. The changes and disturbances due to encoding process can provide a clue about the manipulations performed on an image. Many contributions have been made in the JPEG double compression detection for image forensics. Acceptable accuracy has been achieved using these techniques. The main challenges in the

JPEG forensic analysis are varying false rate and overall accuracy while classifying JPEG images at different compression quality factors [7, 24, 48].

- Editing Fingerprints

Editing of an image is very common as it may increase the utility of the image. The editing operation may be visible or non-visible. But every such operation disturbs the natural coherence of the image and affects its natural statistics. Editing fingerprints are statistical irregularities left in images due to manipulation activities. These fingerprints can be used to detect the tampering of images. These methods are based on the statistical analysis of various features drawn from the image characteristics. In these methods, first the image characteristics of the Spatial domain, Fourier domain, Wavelet analysis, Shape descriptors, etc. are obtained. Statistical analysis of these characteristics reveals the truthfulness of the image [49]. Most of the statistical features-based algorithms utilize specific color channels for image forensics. A color image is always processed in three separate layers. Image data are represented in the three-color channels which contain intensity values for red, green, and blue planes. Although the RGB color space is extremely powerful and perceptive, RGB information may be transformed to luminance (light intensity information) and chrominance (color information) information channels. Several color space models are available, but YCbCr is the second most popular after RGB. Use of Hue, Saturation and Value channels for feature extraction is also helpful in detecting tampering operations. The Hue is an important attribute of the color. It denotes the dominant color. Saturation is the purity of the color. It is estimated by the degree to which a pure color is mixed with white light. The Value work in conjunction with saturation and describes the brightness or intensity of the color. The luminous component (brightness) in HSV model is separated from color information (hue and saturation) [59, 60]. Other algorithms work on image quality assessment as it is assumed that whenever an image is altered the natural image statistics is disturbed. This disturbance is captured using image quality measures (IQM). Several IQMs and their variations have been proposed to detect image tampering. But high false rate has been a problem with these algorithms [1]. One another class of algorithms explores traces of re-sampling to identify tampering. Re-sampling is done to create a new image with a different number of pixels. Up-sampling is done to increase the size of an image. While down-sampling is done to reduce the image size. Geometric transformations are often required while performing image manipulations to give the image a natural appearance. These use re-sampling. Re-sampling is achieved using interpolation methods e.g., nearest neighbors, bi-linear and bi-cubic. The interpolation step can be identified by the statistical study of the image and could be a clue for image forgery. Re-sampling causes statistical association in the image pixel intensity value. This association can be detected. The periodic associations are estimated by analyzing the interpolated pixels. An association indicated a specific type of re-sampling. But such estimation is difficult for images at low quality factors (QFs) [27, 50].

4 Open Challenges with Passive Image Forensics

Every forensic technique will have some desired characteristics, and this keeps the challenges open in image forensics:

- *High accuracy* A passive forensic technique aims at classifying authentic and tampered images correctively in their respective class. If they can classify all the images correctly the accuracy rate would be 100%. Any wrong classification lowers its accuracy rate. So, high accuracy rate of classification is the most important issue for any technique. Accuracy has four parameters: true positive rate (TPR), false negative rate (FNR), false positive rate (FPR) and true negative rate (TNR). TPR and FNR denote the correct classification of authentic and tampered images in respective classes while FPR and TNR denote the wrong classification of authentic and tampered images respectively. A good classifier aims at high TPR and FNR and low FPR and TNR.
- *Low dimensionality of features* Every classification technique utilizes some features extracted from the image data for classification. Dimensionality depicts the number of features required for classification. High Dimensionality of features will result in large computation time while very low dimensionality may result in low accuracy of classification. A classification technique always aims at low dimensionality of features.
- *Robustness to noise* Another important characteristic of an efficient forensic technique is that it must be robust to the noise present in the image. It can be ensured by validating the classification results of images in the presence of noise like White Gaussian Noise, Gaussian Blur and Fast Fading. A passive forensic technique may only be efficient if it maintains the accuracy of classification in the presence of various types of noise.
- *Comparable performance for various JPEG quality images* A JPEG image may have different compression rate and thus different quality factor (QF). A high QF ensures higher data preservice in the image. Whenever a tampering operation is performed on the image, it is resaved. Re-saving of image may be done at similar or different QF. Thus, the input questionable image may be authentic or tampered at any QF. A test suite must

contain combinations of authentic and tampered images at different QF as the classification results may vary for different combinations.

- *Low computational complexity* Computation complexity is an important measure of the effort made by the classification technique in terms of time and space. Most of classification techniques are based on feature extraction from the image and a computation cost is involved with every feature. Low dimensionality of features may reduce the computational cost, but some features have high computation cost as compared to others. So, before considering any feature its computational cost must be determined first; so that it could result in an efficient classifier technique.
- *Integrated design* Most of the classifiers aims at detecting one artifact in the image e.g. Copy-move, image splicing, steganography or seam carving. While checking the authenticity of an image, the type of manipulation is almost always unknown. So, the image needs to be checked for various types of expected manipulations. An integrated classifier may solve this problem by classifying an image as tampered, irrespective of the manipulation operation. So, the focus is on identifying features which may be characteristic for various types of manipulations. Thus, designing an integrated classifier is another challenge for the researcher community.
- *Training data requirement* Another important concern of a classifier design is the quantity of data required for the testing of the classifier. Different classifier techniques require different amount of data for testing purpose. If the test data availability is limited it will make the forensics more challenging.
- *Classifier selection* Classifier selection may affect the performance of image forensic technique. A classifier is selected based on the parameters mentioned above. The challenge is to identify the right kind of classifier so that it can give maximum accuracy with limited input.

5 Acquisition of an Image

The production of a digital image comprises the acquisition, coding and editing as three main phases, as shown in Fig. 2. During acquisition, the light emitted from an object or scene is focused by the lenses on the camera sensor. Camera sensor could be a charge-coupled device (CCD) or a Complementary metal-oxide semiconductor (CMOS). The captured light is filtered by the color filter array (CFA). CFA is a thin film which allows only a part of light to surpass it. Only Red color out of Red, Green, or Blue is captured. Then CFA interpolates the other two colors for each pixel [48].

Additional camera processing operations like color processing, smoothening, sharpening and enhancement etc. may be applied on the image. This is called image acquisition. Then the image coding is done, and the coded image is stored into the camera memory. While coding, the image is compressed and then saved to memory storage. Most of the cameras use JPEG coding format to achieve compression as it is lossy and retain good image quality. The coded image is post-processed to enhance its usability. After the image is coded image editing may be performed as desired. Image editing operations like rotation, scaling, re-sampling, blurring, sharpening, morphing, seam carving, in-painting, copy-move or image splicing could be performed to enhance or change the image contents. After these changes the image is re-saved; hence re-compressed in JPEG format. At every stage, i.e. acquisition, coding and editing, some inherent traces are left behind in a digital image. These traces can be mined and examined to verify the authenticity of the image.

6 Survey Design

A structured survey of Source Device Attribution is reported in this section. For more optimization different steps have been followed that included in the survey are development of a survey protocol, conducting the survey, analyzing the results, reporting the results and discussion of findings. A sequence of techniques followed by orderly literature assessment helps in accomplishing a comprehension of the current problem. An efficient surveying is a trustworthy research technique. It is believed to be a powerful technique to distinguish any research gaps and perceive ways for upcoming research work. A complete literature search is conducted with the assistance of search strings that will form the base of the responses to the research questions. The conclusion of this review would help in highlighting numerous challenges related to the field, along these lines encouraging the researchers to perform further investigations. Survey Protocol characterize the comprehensive layout, framework or an analogy to explore the plan regarding the inventory and monitoring tasks. The protocol also depicts the set of rules and guidelines for performing the survey on the literature work on the source device authentication process. It provides help to the novice researchers in this field with sufficient details regarding source device authentication. The principal goal of this organized survey is to execute a detailed analysis of the literature available on detection techniques for various image forgery attacks. A search strategy is framed to initialize the process of a systematic survey with a hunt through electronic libraries to accumulate the appropriate literature. The search strategy is significant purpose of the overview method. So, constructing an effective search strategy is considered as a critical pre-requisite. In this work, an automatic search was included a consideration of four digital libraries, i.e. ACM Digital Library, IEEE

Xplore, Springer and ScienceDirect. The search was limited to the article title, abstract, and meta-data in ACM Digital Library, IEEE Xplore and ScienceDirect. Completing a pursuit query on Springer and Google Scholar delivered lot of results because of the absence of customization choices as in other digital libraries. Restricting the search keywords was sustained by all electronic databanks that aided in deciding a smaller search query.

7 Handcrafted Techniques for Camera Device Attribution

Whenever an image needs to be matched to its source, it requires some unique features of the source acquisition device. These features may be module imperfections, defects or faults. The deviation produced by a lens, noise in an imaging sensor, dust spots on a lens will introduce unique artifacts in images. Imaging sensors in source devices have various defects which may result in disturbances in the pixel intensity values. The sensor noise could be present due to pixel defects, fixed pattern noise (FPN) or photo response non uniformity (PRNU) [5, 6]. Some of the other methods involve the study of hardware utilized during image or document acquisition and scanning etc. Usually optical or sensor irregularities of the devices are studied for the purpose of image classification. The main challenge is to quantify small deviations/traces in an image. It is not easy as these noise pixels may be obscured by the image content itself. But they may not always give a meaningful classification due to varying operating conditions. Figure 3 show the general framework for Machine Learning based CDA. In this approach, different image features as per different acquisition device characteristics are extracted. These features are fed to the classifier for training and a classifier model is obtained which is further tested for model verification.

The following sections analyses various hand-crafted machine learning based techniques for source camera detection.

- Lens Aberration-Based Detection

These techniques aim at analysis of aberrations introduced by the lens system during the image production phase. Choi [14] claimed that lens radial distortion is the most suitable and robust method for camera identification. The unique pattern of radial distortion was explored for the identification of device camera. Van et al. [58] proposed lateral chromatic aberration to perform cell phone identification. Different experiments using manipulated and original images with random crops regions were performed. But the accuracy of the technique declined when it is experimented with different camera models from the same brand.

- Color Filter Array (CFA) Based Detection

Most of the digital cameras are equipped with a CCD or CMOS sensors. These sensors have CFA which senses the color scene at various pixel locations. It is done only for one primary color i.e. Red. The remaining Blue and Green colors of the RGB color channels are obtained by interpolation process. Popescu and Farid [50] proposed CFA based source detection for digital image forensics. An image tampering localization scheme based on an expectation maximization

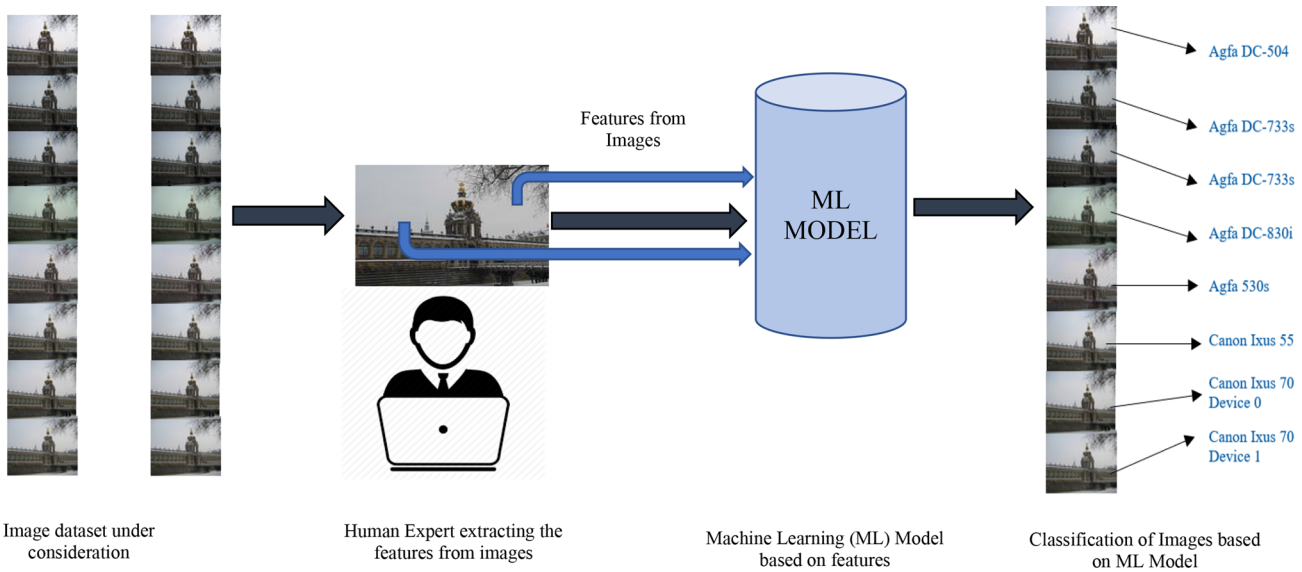

Fig. 3 Machine learning based CDA

(EM) algorithm was also implemented. The proposed model was used for lossless and lossy compressed image forensics. CFA interpolation was used to fill the missing pixel intensity values in the pixel neighborhood during image acquisition. This method required the knowledge of CFA pattern of the respective acquisition device and the interpolation technique used. The technique failed for new capturing devices as these devices did not use CFA interpolation. The detection accuracy for evaluation of eight CFA interpolation algorithms was approximately 100% for high-quality images but it dropped for low quality images. Long and Huang [37] proposed a decision mechanism using 3-layer feed-forward neural network. They designed a majority-voting scheme for detecting demosaicing in images. The spatial periodic inter-pixel correlation due to CFA interpolation was represented in a quadratic form. The principal components of the coefficient matrix of every color channel were extracted and fed into the neural network for camera identification. Experiments demonstrate that presented method was efficient and robust as well. Gallagher and Chen [28] developed a similar technique to detect and locate the image tampering. Demosaicing was stated as a type of passive watermark whose traces were found in the image signal. The demosaicing artifact was detected using Fourier analysis. The periodicities in the variance signal were detected to indicate demosaicing and, hence tampering. A standard test set of 1600 images were used and accuracy of approximately 95% was reported. The algorithm was also applied for localizing forged image regions. It was demonstrated that demosaicing parameter evaluation was not required to authenticate images. The detection of their presence was enough to indicate a forgery. Swaminathan et al. [54] presented techniques to identify the inherent fingerprints of the source device for image forensics. Intrinsic fingerprints were classified into two categories i.e. in-camera and post camera. The intrinsic fingerprints were estimated using an imaging model. Estimation of camera outputs was performed to obtain the post-camera fingerprints/traces. The non-appearance of in-camera traces indicated that the test image was not a camera output and was possibly generated by the other image production process. The appearance of new post-camera traces indicated that the image has undergone post-camera processing.

Fan et al. [23] proposed demosaicing detection using a neural network framework. Computational rules used in demosaicing were simulated through bias and weight value adjustment. Inverse operation against interpolation was applied through the knowledge of demosaicing inter-pixel correlation. A neural network was used to represent the difficult computational rules for interpolation algorithms. This framework revealed a series of traces present due to demosaicing. 4-layer feed-forward, back propagation NNs was used. The transfer function of the output layer was linear. Three independent classifiers were used for classification decision. The decision was made based on majority voting scheme which integrated the decision of the three classifiers. An image was classified as demosaiced/non-demosaiced based on the consensus of these classifiers. Kirchner [36] determined the pattern of the CFA in demosaiced digital images. The proposed method was based on a CFA synthesis procedure to determine the most likely raw sensor output for a given full-color image. Linear filter was used to evaluate the legitimacy of digital images. The analysis of small sub-blocks diminished the effects of large local errors. This technique achieved low accuracy, especially in case of image JPEG compression. Ho et al. [32] proposed four algorithms which are based on aspects of inter-channel correlation. Bilinear, edge-directed with constant hue, projection-onto convex-sets and adaptive filtering algorithms were used to calculate variance maps (v-maps). 50 images from four cameras of three different brands were used for experimentation. 50% on the images were used for training and remaining were used for testing purpose. The inter-channel correlation was found to be complementary as it deals with pixel-correlations resulted due to demosaicing, in a much better way.

Takamatsu et al. [55] described a method for estimating demosaicing from image noise variance. It was observed that the noise variance in interpolated pixels was low. The obtained CFA pattern estimation accuracy for high quality images was 95.8 and 98.4% for multiple and single image, respectively. But this accuracy decreased after the application of post processing operation on demosaiced image. Chang et al. [15] proposed photographic image (PIM) detection and device categorization method. The periodicity event caused by color filter arrays (CFAs) and the demosaicking process was used. The proposed scheme exploited the prediction error statistics and local peak identification. The phenomenon for PIM detection was analyzed. Device classification was performed by analyzing local peaks in the Fourier spectrum. A hierarchical model was used for the same. PIMs and photo realistic computer graphics (PRCG) images were generated for method evaluation. The accuracy for 5805 images was 95.56%. The precision of the proposed method was 93% for different camera images for device class identification. Chen and Stamm [16] proposed an integrated model from submodels for SCI. Demosaicing errors based on image and interpolated image were calculated. Each submodel contains partial information about the demosaicing algorithm in a camera. Integration of sub-models was used to design a multi-class ensemble classifier. The proposed model identified the correct make and model of the source camera with an average accuracy of 99.2%.

Some author explored CFA based techniques for source mobile detection too. Celiktutan et al. [13] proposed using bit plane similarity as a measure to identify the source mobile camera. A few binary similarity measures were used as metrics. The features based on hese binary similarity

measures and image quality measures were classified with a KNN classifier. The major limitation was that the performance deteriorates whenever highly compressed images were subjected to analysis. Cao and Kot [11] introduced an image classification algorithm based on image demosaicing regularity. Partial derivative correlation models were proposed. The source mobile cameras were identified using demosaicing features extracted from the image. Eigen feature regularization and feature reduction were used. 14 commercial cameras of different models were used for experimentation. The detection accuracies were 97.5% and 99.1% for different models and 10 RAW-tools, respectively. The results were obtained using the SVM classifier. Cao and Kot [12] utilized the statistics of the CFA matrix interpolation for source identification. Three sets of demosaicing features which included weights, error cumulants (EC) and normalized group sizes (NGS) were used. A total of 432 features were extracted. eigenfeature regularization (ERE) is performed to decrease the number of features. Finally, a set of 20 Eigen features based on demosaicing features were used with PSVM classifier to identify 15 source devices i.e. mobile cameras. Zhao and Stamm [64] proposed a computationally effective approach for source mobile identification. The technique improved the approach proposed by Swaminathan et al. [54] for identification of an image's source camera, in terms of accuracy and computation. The basic approach used least squares estimates of its demosaicing filter. Different experiments were performed to evaluate the performance of proposed method for obtaining demosaicing filter estimates. It was compared with window-based approach. Self-captured pictures from 13 different camera models were used. The length of the data matrix was taken as representative for the computational cost. The proposed approach allowed the size of the data matrix to be directly specified and hence predicted the computational cost. A support vector machine was used to perform camera model identification using these demosaicing filter estimates using fivefold cross validation.

- Sensor Noise Based Detection

The various components of source devices including imaging sensors may result in different types of defects and noise in the image. The three main components of sensor noise are i.e. Pixel Defects, fixed pattern noise (FPN), and photo response non-uniformity (PRNU). Bayram et al. [5] implemented the source camera identification of images based on fingerprints of the pixel interpolation using RGB color channels. Integrated model based on demosaicing artifacts and noise characteristics of the imaging sensor was proposed to fix the source camera. Bayram et al. [6] determined the camera model using demosaicing artifacts. Noise characteristics of the imaging sensor of the camera were used. Author has used integrated feature set of 78D, comprising demosaicing characteristics and sensor noise properties. SVM classifier was used to classify 5 categories of source cameras. Lukas et al. [42] proposed image tamper detection by identifying source camera using sensor pattern noise (SPN). It was assumed that either the camera or images taken by that camera were available. The camera pattern noise was a unique feature of imaging sensors present in every region of the image. The region with absence of pattern noise was termed as forged region. The presence of the noise was recognized using correlation. Two different approaches were proposed. First approach required region of interest (ROI) selection by user and second approach does ROI selection automatically. The methods were tested for lossy compression and filtering operations. Although these methods were able to verify the image integrity, but they fail to correctly classify the regions where the pattern noise was naturally low. Dirik et al. [22] used sensor dust characteristics for source camera identification. The sensor dust problem arose due to unchangeable lenses in camera. The dust particles that settle in front of the imaging sensor created a persistent pattern in all captured images. A novel detection based on matching of dust-spot characteristics in the images were proposed. A Gaussian intensity loss model was proposed for the detection of dust spots. Average identification accuracy of 99% was achieved. Chen et al. [17] estimated PRNU of camera sensor pattern noise (SPN) using the maximum-likelihood principle. The proposed method was efficient against most of the image processing operations like enhancement and filtering. The correlation coefficient was used for sensing the similarity between the image noise residue and the camera SPN. It was noted that the periodic structure artifacts of the SPN due to color interpolation, on-sensor signal transfer and sensor design were not unique for one specific camera. The cameras of the same brand or having the same sensor design may share these details. The zero-mean operation was performed to the camera SPN to lessen these effects. The Fourier magnitude of SPN was filtered to lessen the JPEG compression artifacts. Fridrich [26] estimated and detected image PRNU to identify the image origin and truthfulness. The proposed technique used maximum likelihood principle derived from a simple sensor output model. The model was then used to perform fingerprint detection from the image. The image noise residual was examined to check if it contained the camera fingerprints. Use of the peak to correlation energy (PCE) measure was suggested. It was proved to be a more stable measure as compared to the normalized cross correlation for images which may have undergone geometrical manipulations. The proposed measure was capable to deal with the interpolated noise.

Li and Li [39] proposed a novel method to extract camera PRNU. It was called colour-decoupled PRNU (CD-PRNU).

The physical and simulated colour components of the image were distinguished. The device identification accuracy of 99% was achieved. But it decreased for small image size. Typical identification rate for 768×1024 and 192×256 image size was 94.33% and 60.67%, respectively. Liu et al. [40] detected the presence of PRNU in the image by using binary hypothesis testing scheme. The noise like nature of PRNU was studied. It was discussed that the amount of PRNU carried by an image was small and it was also affected by the content of the image. Image with highly saturated colors carried less PRNU. Other noise components go above the amount of PRNU noise. These other noise components were required to be removed first without affecting the PRNU signals. Thus, the signal detection task was analyzed as it decreased the detection accuracy. The significant regions from the noise residual were extracted and used for the detection of the source device. The deteriorated regions were discarded. The significance of a region was estimated by its signal-to-noise ratio (SNR). The term signal referred to the PRNU, while the noise referred to the other unwanted noise components in the proposed work. Goljan and Fridrich [29] proposed a method based on sensor fingerprint (PRNU) for camera identification of images having lens distortion. A detection reliability of 91% and 99.8% were obtained using camera fingerprints for Panasonic and Canon camera respectively. Kang et al. [34] used circular correlation norm (CCN) as the statistic device to lower the false positive rate to 50% of that with Peak to Correlation Energy (PCE). The proposed method removed the interference and raised the CCN value for a positive sample. It achieved greater camera identification performance. The efficiency of the method was proved based on theoretical analysis and extensive experimentation. The method achieved best ROC performance among similar camera identification methods. True positive rate (TPR) of the proposed method was 99.9% with zero false positive rate (FPR). Cooper [19] suggested a simpler space variant filtering approach for estimating the PRNU. This model was based on spatial domain filtering combined with other enhancement procedures. The proposed model had a significantly higher discrimination rate. Author pointed that although the wavelet-based Mihcak's filter was commonly accepted in the literature for estimating the noise residue, it may spread the details and edges of an image. Various disturbing signals would appear around such regions. It resulted in lower correlation between the noise residue and the correct PRNU. A PRNU estimation technique using a combination of adaptive wiener and median filtering in the pixel domain was proposed. An enhancement strategy was used. Only the pixels with high probabilities of significant noise residue bias were preserved.

Chierchia et al. [18] explored absence of PRNU signatures in doubtful images. Assuming image forgery as Bayesian estimation, a Markov Random Field was used to model the strong spatial dependencies of the source. The overall decision was based on the whole image analysis rather than pixel regions. A globally optimal solution using convex optimization technique was proposed. PRNU estimation was performed by non-local filtering. Extensive experiments illustrated that the technique was successful for a wide range of practical problems. Various forms of image distortion and JPEG compression were focused. The receiver operating curve (ROC) was obtained using the original boxcar and guided filtering. The grayscale image, the RGB image, and the vectorially image were used to design the correlation predictor. 200 uncompressed 768×1024-pixel images were used. Comparisons were carried out for very-small, small, medium and large forgeries. A huge performance improvement was observed for small forgeries. The performance gain was much limited for medium and almost negligible large sized forgeries, respectively. Marra et al. [44] proposed passive camera identification algorithm. PRNU noise was estimated from image residuals. PRNU identification was based on the correct clustering of residuals obtained from the same camera images. The proposed strategy consisted of two steps. First, the image residuals were classified by correlation grouping. Then, the basic clusters were grouped together with ad-hoc enhancement algorithm. The Dresden database was used for experimentation. The evaluation proved that the technique was very efficient. Bouman et al. [10] observed that severely tampered images could be recognized using camera's defects known as noise pattern. The source camera was identified based on these processed images. The noise patterns of images were detected using denoising filter. The average of the noise pattern was termed as reference pattern. The same pattern was found in different images of the same device. This intrinsic fingerprint of the camera was used to correlate noise pattern of an image with its source device. If similar patterns were found and the correlation was above a certain threshold, the camera was categorized as the source device. Each camera's noise pattern was compared to four camera reference noise patterns for decision making. Costa et al. [20] proposed a scheme to combat a situation where one may not have access to all the possible image source mobile devices and cameras. Three main phases of the proposed scheme were the identification of regions of interest, extracting features and identification of device. Nine different region of interests (ROI) instead of the central region of the image were considered as it is assumed that it will complement the useful information. Then, the Sensor Pattern Noise for each of the R, G, B and Y (luminance) channels was used to obtain 36 features for each image. Costa et al. [21] extended this approach by experimenting on 13,210 images of 400 cameras. Out of these 25 cameras were physically available. Rest of the camera were experimented based on their clicked images. An average of 96% was achieved for the experimentation.

- Image Feature Based Detection

Many contributors studied the image quality for the purpose of device detection. Most of them considered color, textural and statistical quality features for source attribution. Kharrazi et al. [35] used IQM's introduced by Avcibas et al. [2]. The same set of IQM's was used by to identify the source camera of a digital image. The variation between the filtered and tampered image was characterized using IQMs. A set of 13 IQM's was proposed. The IQMs used were based on pixel difference, correlation and the spectral distance. It was stated that the examination of first, second and higher order statistics of the digital images was needed to obtain the color characteristics for different cameras. Proposed measures were average pixel value, RGB pair correlation, neighbor distribution center of mass, RGB pair energy ratio and wavelet domain statistics. The classifier accuracy of 98.73% was obtained from a database of 300 images using LIBSVM classifier. Farid [25] proposed use of quantization tables to distinguish between original and tampered images. It was observed that different cameras employ different quantization tables for JPEG compression. Image quantization scheme of given image was compared to a database of known cameras to detect the source camera. Quantization table from 204 images were considered from different cameras in their highest quality setting. Most part of these quantization tables were found different from each other. Overlapping was found in the case of cameras from the same manufacturer. It was also observed that the quantization tables used by the digital cameras and Adobe Photoshop were different.

Wang et al. [59, 60] proposed wavelet statistics for feature extraction. These features were classified using SVM. A 35-dimensional set consisting of 216 wavelet and 135 textural features were obtained. The sequential forward featured selection (SFFS) algorithm was used to reduce the dimensionality. Hu et al. [33] identified the image source device using similar image features. Different combination of wavelet, color, and statistical quality measures-based features were explored for the source device classification. 300 images from each camera with 50–50 ratio for training and testing was considered. The experiments were conducted to analyze the performance of the features for images with different JPEG compression, cropping regions and scaling factors. But the performance of the different feature combinations varied with different type of manipulations. Ozparlak and Avcibas [47] proposed ridgelets and contourlets sub-bands based statistical models for source detection. SFFS algorithm was used for feature reduction. Ridgelets based model used 48 features, and contourlets based model used 768 features. Both these were found to be effective in classification of camera models as well as in differentiating natural and computer-generated images. These were also able to differentiate between images from scanners of the same maker. Marra et al. [43] used passive forensics based on the analysis of image residuals. The proposed features were extracted locally based on textural features. These features are based on co-occurrence matrices and classified using SVM classifier. The experiments were conducted on images from Dresden database and a good classification rate was obtained. Xu et al. [61] performed source camera identification using image texture features. These features were extracted from chosen color model and channel. The proposed techniques distinguished images even belonged to sources of the same brand and model. The technique was robust to harmful retouching or geometric distortions, such as JEPG compression and noise addition. The experimental results demonstrated that the performance of the proposed method was very encouraging. The proposed method had a high detection accuracy and robustness.

Marra et al. [45] proposed the analysis of the image residuals of different color bands for feature extraction. Image residuals are collected using co-occurrence matrices of selected neighbors and then used for training a classifier model. Dresden Image Database was considered for experimentation. All the cases including partially corrupted and cropped images were experimented. The performance degraded in cases where the training and test set were not aligned. That means if a system was trained on original images but tested on JPEG compressed images then the detection accuracy was lower. This remains as an open problem for all such classification and detection problem. Many authors used image features to identify source camera for mobile devices also. Tsai et al. [56] used color features, image quality metrics and frequency domain to identify source device. Wavelet domain statistics were classified using a Support Vector Machine. Both type of devices i.e. digital cameras and mobile devices were used for experimentation. Author extended this experiment and included mobiles, phones, cameras, scanners and computers for identification. Image acquisition process features were explored to make two different groups named as color interpolation coefficients and noise features. Mckay et al. [46] used signal processing features to identify the source device. They explored the color interpolation coefficients for each device. Further, the noise features were added to identify the device accurately. This technique was efficient in classifying the images produced by cameras, cell phone cameras, scanners, and computer graphics. Different set of experiments were conducted to identify the brand and model of the device too. An overall accuracy of 93.75% was obtained. It was claimed that the proposed features were robust to JPEG compression.

Liu et al. [41] proposed a method using the marginal density discrete cosine transform (DCT) coefficients in low-frequency coordinates and neighboring joint density features from the DCT domain. Furthermore, hierarchical clustering and SVM is used to detect the source of acquisition of the images. Sandoval Orozco et al. [52] proposed Sensor

Imperfections and Wavelet Transforms to detect the acquisition mobile device. This method extracts the sensor noise patterns of images. 25 features including first-order, higher-order and Quadratic Mirror Filters features were used. Sandoval Orozco et al. [53] experimented classification of brand and model using image features with support vector machines. 36 experiments in 5 sets were carried for different configurations including the identification of mobile device images in a set of scanned and computer-generated images. Noise, color, Image Quality Measures and Wavelets based image features were used. Some modification was proposed to suit the experiment for mobile devices and improvement of the results. A combination of the different feature sets, different crop sizes, positions, and wavelet functions were explored for experimentation. Zeng [63] proposed a method based on traces left by anti-forensic methods. It was an extension which could be used with the existing camera source identification method. Author analyzed that the removed/embedded signature is not dependent on the target image which resulted as a limitation of denoising filter used for estimating device signatures. This caused higher noise levels in forged images. This noise level estimation was used to counter anti-forensics and exposed the fingerprints left by signature removal or replacement. This may be used as preliminary judgment before CSI investigation. Experiment were conducted on proposed anti-forensic schemes on JPEG images with QF = 100 [38].

8 Deep Learning Approaches

Now a days, CNN and deep learned features are explored for many image related applications. A large dataset for training is a crucial requirement for such frameworks. It has been established that if large datasets are available, the deep learning features can outperform the hand-crafted features considerably. On similar lines various authors explored CNN based framework for image analysis to identify the source camera. Figure 4 show the general framework for Deep Learning based CDA. In this approach, the CNN consisting convolution, pooling and fully connected layer is used. Layers are used for feature extraction as well as classification. But it can be intervened by human expertise to enhance the outcome.

Bondi et al. [8] made a first attempt for the identification of different camera models using a convolutional neural network (CNN). Author extracted device features from image subregions. Dresden and Flickr Image Database was used to validate the results. Efficient model was proposed using simple CNN structures. Bondi et al. [9] explored usage of CNNs for camera model identification. Author used CNN for feature extraction and a set of SVMs for classification. Various CNN architectures were experimented to manage accuracy and computational complexity. The performance dependency with respect to accuracy, training set size, and training–testing strategy was explored. High detection accuracy of 96% was obtained for four convolutional layers network for a set of 18 camera models. Small accuracy increment was claimed for complex CNN structures. Tuama et al. [57] used similar CNNs for source camera model identification. Author tuned the existing AlexNet model for camera detection. It was computed with GoogleNet and found to be slightly less efficiency. The role of preprocessing filters was found to be crucial. A slight performance drip was observed with increase in number of models under classification.

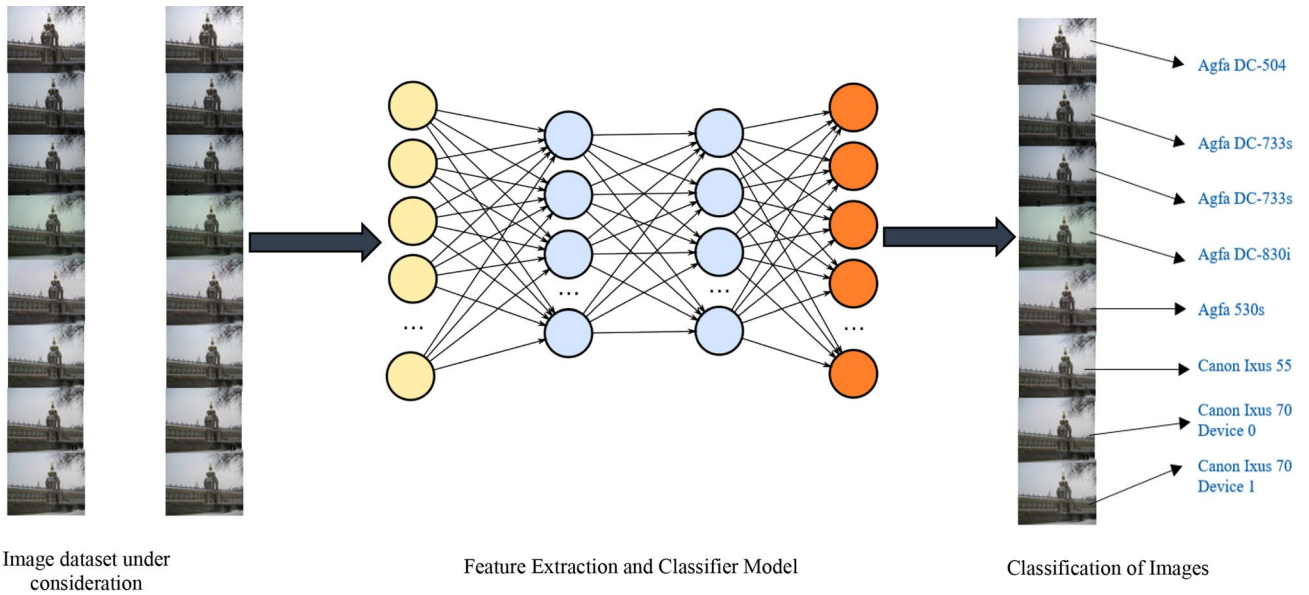

Fig. 4 Deep learning based CDA

Increasing the number of layers improved the accuracy and hence bigger networks with more layer were claimed to be more efficient. Yang et al. [62] identified the source camera using small-size images. A content-adaptive convolutional neural networks (CA-CNN) was proposed. Three parallel CNNs i.e. CA3-CNN, CA5-CNN, CA7-CNN were used. The convolutional kernel size of these preprocessing layers differed. Effective results were obtained for the identification of the camera brand and model even using small-size images. A classical problem in source identification is when the questionable image does not belong to the dataset of the known camera models. This is known as the open set problem. Two different approaches were proposed to address this issue in Bayar and Stamm [4]. Their approach categorized the sources as known or unknown. In first experiment, deep learned features were mapped into a confidence score. Then, thresholding was on confidence score used to identify unknown models. In another experiment, a set of 'known unknown' devices were used to train a new classifier to identify unknown camera models. Experiments demonstrated an accuracy of 97.74%. Recently, Al Banna et al. [3] performed Mobile Model Identification using Deep CNN and Transfer Learning Approach. Author proposed a transfer learning approach with Machine learning classifiers The MobileNet from ImageNet was explored as a transfer learning model. Machine learning classifiers i.e. Random Forest. -Logistic Regression and SVM were explored in integration with MobileNet. The accuracy decreased in case the data for a particular device is less. Highest accuracy was obtained for SVM and logistic regression. But SVM took the highest training time. Kaggle dataset with ten mobile classes was used for experimentation.

9 Synthesis Analysis of Work

In this review paper, all research papers aiming camera and mobile detection using image analysis were acquired and then finally 60 most suitable papers were considered to be included. Out of these, 32 states of art papers were critically analyzed and compared. Table 1 shows a critical evaluation of existing machine learning based device detection techniques. After the evaluation many important observations have been made which one must analyze before reaching conclusion.

All the analyzed techniques are categorized on the basis of 'Technique used for Feature Extraction' as in 1st column. As different techniques aim at identification of different devices, we divided the techniques as camera or mobile detection in the 2nd column. The name of author and year is mentioned in the 3rd column. The feature dimensionality is listed in column 4. The number Models/Makers considered in study was listed in column 5. Column 6 and 7 lists the classifier used and the accuracy range achieved in the study. Some information which is not mentioned in particular paper is termed as NA means Not Available. Some observation during evaluation are:

- Different dataset was used for experimentation. Different source devices were used by different contributors, it is difficult to find coherence while making comparison.
- Different device Brands are analyzed for study. All the models of that brand were not analyzed. Only some of them were used to make conclusion.
- Images obtained for study are self-clicked with different crop size and compression quality. Only Dresden dataset is used for analysis by some contributors but they only considered some models from the dataset.
- SVM is widely used as classifier. The success rate for different classifiers such as decision tree, random forest and Multi-layer perceptron is hardly evaluated.
- In CNN based techniques only some models from Dresden were studied for device detection

While analyzing the contributions as per different techniques following observations are made:

- The Accuracy rate of Lens Aberration based detection techniques deteriorates when the different source camera from same brand were under consideration.
- The performance of color filter array (CFA) Based Detection techniques dropped when the post processing operation were used on images. These techniques were vulnerable to high compression rate for JPEG images.
- Sensor Noise Based Detection techniques performed poorly when pattern noise in images was low. The performance of these techniques is also subjected to JPEG compression rate. But these techniques were robust to even small manipulations in the image.
- The performance of Image feature based detection techniques was found to be varying with different JPEG compression rate, cropping regions and scaling factor. The accuracy decreased in case if there is difference in image compression rate for testing and training images.
- The deep learning based techniques were found to be more promising even with small convolutional neural networks. The only limitation is that these techniques require large dataset for feature extraction. The accuracy may be increased with addition of more layers but leading to complexity.
- One open issue for all the techniques is that the model identification for the same brand is still a challenge.
- Another open problem is the attribution when the device or device images are not available or unknown.

Table 1 Evaluation of digital camera and mobile phone device detection techniques

Technique used for feature extraction	Device identified	Author	No. of features	No. of models/makers	Classifiers	Best success rate
Lens aberration based detection	Digital camera	Choi [14]	36	3/3	SVM	87.38–91.53%
	Mobile phone	Van et al. [58]	6	3/3	SVM	72.75–92.22%
Color filter array (CFA) based detection	Digital camera	Ho et al. [32]	NA	4/3	NN	94.5%
		Chang et al. [15]	4	3	NN	95.16%
		Chen and stamm [16]	1372	12	Ensembled classifier	99.2%
	Mobile phone	Celiktutan et al. [13]	118	9/3	SVM	62.3–98.7%
		Cao and Kot [12]	20	4/11	PSVM and NN	94.8–99.4%
		Zhao and Stamm [64]	9n	13	SVM	71.3%
Sensor noise based detection	Digital camera	Bayram et al. [6]	78	5	SVM	84.8%
		Chen et al. [17]	15	6	Algorithm	75%
		Goljan and Fridrich [29]	ND	3	Algorithm	95%
		Marra et al. [44]	1875	25	Algorithm	98.72
		Bouman et al. [10]	NA	4	NA	ND
	Mobile phone	Costa et al. [20]	36	25/9	SVM	94.49–98.10%
		Costa et al. [21]	Different set of features	25/9	SVM	96.56–97.34%
Image features based detection	Digital camera	Kharrazi et al. [35]	34	5	SVM	88.02%
		Wang et al. [59, 60]	351	6/4	SVM	98
		Hu et al. [33]	102	10/4	SVM	47–92
		Marra et al. [43]	338	10 from Dresden	SVM	98.99%
		Xu et al. [61]	944	14 from Dresden	SVM	65–75%
		Marra et al. [45]	500	26 from Dresden		98%
	Both	Tsai et al. [56]	33	2/7	SVM	61.7–99.72%
		Mckay et al. [46]	60	5/5	SVM	97.7%
	Mobile phone	Liu et al. [41]	45	5/6	SVM	86.36–99.91%
		Sandoval Orozco et al. [52]	25	10/6	SVM	89.45%
		Sandoval Orozco et al. [53]	NA	12	SVM	80.69%
Deep learning based detection	Digital camera	Bondi et al. [8]	128	18 from Dresden, 10 from Flickr	CNN	99%
		Bondi et al. [9]	128	18 from Dresden	CNN	96%
		Tuama et al. [57]	AlexNet	33 from Dresden and self-clicked	AlexNet	98%
		Yang et al. [62]	CNN	13 Models from Dresden	CNN	87%
		Bayer and Stamm [4]	CNN	15 from Dresden	CNN	98%
	Mobile phone	Al Banna et al. [3]	Deep CNN-mobilenet	10 from Kaggle	Random forest, logistic regression, SVM	98.54–100%

10 Conclusion

Images authentication is the need of the hour in this digital era. Identification of acquisition device is one of the significant universal approach which is used to identify the authorship of an image. This review paper aims at analyzing the different types of device identification approaches. All research papers aiming camera and mobile detection using image analysis were acquired and then finally 60 most suitable papers were considered to be included. Out of these, 32 states of art papers were critically analyzed and compared. This is the first attempt for source camera and source mobile detection evaluation as per author knowledge.

A much needed background for device attribution is provided. The entire image acquisition process is explained. Different artifacts present sue to acquisition are discussed. The research work based on these artifacts is analyzed and presented for comparison. As mentioned, the performance for most of techniques varies with JPEG compression quality, cropping and scaling. Additionally, the model identification for the same brand is still challenge. Another open problem is the attribution when the device or device images are not available or unknown.

Compliance with Ethical Standards

Conflict of interest The authors declare that they have no conflict of interest.

References

1. Avcibas I, Bayram S, Memon N, Ramkumar M, Sankur B (2004) A classifier design for detecting image manipulations. In: 2004 International conference on image processing, vol 4, pp 2645–2648
2. Avcibas I, Memon N, Sankur B (2003) Steganalysis using image quality metrics. IEEE Trans Image Process 12(2):221–229
3. Al Banna MH, Haider MA, Al Nahian MJ, Islam MM, Taher KA and Kaiser MS (2019) Camera model identification using deep CNN and transfer learning approach. In: 2019 International conference on robotics, electrical and signal processing techniques (ICREST). IEEE, pp. 626–630
4. Bayar B and Stamm MC (2018) Towards open set camera model identification using a deep learning framework. In: 2018 IEEE international conference on acoustics, speech and signal processing (ICASSP), 2007–2011
5. Bayram S, Sencar HT, Memon N, Avcibas I (2005) Source camera identification based on CFA interpolation. In: International conference on image processing, vol 3, pp 69–78
6. Bayram S, Sencar HT, Memon N (2008) Classification of digital camera-models based on demosaicing artifacts. Digit Investig 5(1):49–59
7. Bianchi T, Piva A (2012) Image forgery localization via block-grained analysis of JPEG artifacts. Inf Forensics Secur 7(3):1003–1017
8. Bondi L, Baroffio L, Güera D, Bestagini P, Delp EJ, Tubaro S (2016) First steps toward camera model identification with convolutional neural networks. IEEE Signal Process Lett 24(3):259–263
9. Bondi L, Güera D, Baroffio L, Bestagini P, Delp EJ, Tubaro S (2017) A preliminary study on convolutional neural networks for camera model identification. Electron Imaging 7:67–76
10. Bouman KL, Khanna N, Delp EJ (2016) Digital image forensics through the use of noise reference patterns. In: International sustainable remediation forum conference, pp 1–7
11. Cao H, Kot AC (2009) Accurate detection of demosaicing regularity for digital image forensics. IEEE Trans Inf Forensics Secur 4(4):899–910
12. Cao H, Kot AC (2010) Mobile camera identification using demosaicing features. In: IEEE international symposium on circuits and systems (ISCAS), pp 1683–1686
13. Celiktutan O, Avcibas I, Sankur B, Ayerden NP, Capar C (2006) Source cell-phone identification. In: IEEE 14th signal processing and communications applications, pp 1–3. https://doi.org/10.1109/siu.2006.1659882
14. Choi KS (2006) Source camera identification using footprints from lens aberration. In: Proceedings on digital photography II, no. 852 in 6069: 60,690 J–60,690 J–8
15. Chang TY, Tai SC, Lin GS (2014) A passive multi-purpose scheme based on periodicity analysis of CFA artifacts for image forensics. J Vis Commun Image Represent 25(6):1289–1298
16. Chen C, Stamm MC (2015) Camera model identification framework using an ensemble of demosaicing features. In: 2015 IEEE international workshop on information forensics and security (WIFS), pp 1–6
17. Chen M, Fridrich J, Goljan M, Lukas J (2008) Determining image origin and integrity using sensor noise. IEEE Trans Inf Forensics Secur 3(1):74–90
18. Chierchia G, Poggi G, Sansone C, Verdoliva L (2014) A Bayesian-MRF approach for PRNU-based image forgery detection. IEEE Trans Inf Forensics Secur 9(4):554–567
19. Cooper AJ (2013) Improved photo response non-uniformity (PRNU) based source camera identification. Forensic Sci Int 226(1):132–141
20. Costa FDO, Eckmann M, Scheirer WJ, Rocha A (2012) Open set source camera attribution. In Proceedings of the 25th conference on graphics, patterns and images, pp 71–78
21. Costa FDO, Silva E, Eckmann M, Scheirer WJ, Rocha A (2014) Open set source camera attribution and device linking. Pattern Recognit Lett 39:92–101
22. Dirik AE, Sencar HT, Memon N (2008) Digital single lens reflex camera identification from traces of sensor dust. IEEE Trans Inf Forensics Secur 3(3):539–552
23. Fan N, Jin C, Huang Y (2009) A pixel-based digital photo authentication framework via demosaicking inter-pixel correlation. In: 11th ACM workshop on multimedia and security, New Jersey, USA, pp 125–130
24. Fan Z, De Queiroz RL (2003) Identification of bitmap compression history: JPEG detection and quantizer estimation. IEEE Trans Image Process 12(2):230–235
25. Farid H (2006) Digital image ballistics from JPEG quantization. Technical Report TR2006-583, Department of Computer Science, Dartmouth College
26. Fridrich J (2009) Digital image forensics. IEEE Signal Process Mag 26(2):1–11
27. Gallagher AC (2005) Detection of linear and cubic interpolation in JPEG compressed images. In: 2nd canadian conference on computer and robot vision, pp 65–72
28. Gallagher AC, Chen T (2008) Image authentication by detecting traces of demosaicing. In: IEEE conference on computer vision and pattern recognition workshops, pp 1–8

29. Goljan M, Fridrich J (2012) Sensor-fingerprint based identification of images corrected for lens distortion. Media Watermarking Secur Forensics Int Soc Opt Photon 8303:1–13
30. Gonzalez W, Woods RE (2004) Eddins digital image processing using MATLAB. Prentice Hall, Upper Saddle River
31. Gupta S, Kumar M (2019) Forensic document examination system using boosting and bagging methodologies. Soft Comput. https://doi.org/10.1007/s00500-019-04297-5
32. Ho JS, Au OC, Zhou J, Guo Y (2010) Inter-channel demosaicking traces for digital image forensics. In: 2010 IEEE international conference on multimedia and expo (ICME), pp 1475–1480. https://doi.org/10.1109/icme.2010.5582951
33. Hu Y, Li CT, Zhou C (2010) Selecting forensic features for robust source camera identification. In: International computer symposium (ICS), 2010, pp 506–511. http://doi.org/10.1109/COMPSYM.2010.5685458
34. Kang X, Li Y, Qu Z, Huang J (2011) Enhancing source camera identification performance with a camera reference phase sensor pattern noise. IEEE Trans Inf Forensics Secur 7(2):393–402
35. Kharrazi M, Sencar HT, Memon ND (2004) Blind source camera identification. In: International conference on image processing, pp 709–712
36. Kirchner M (2010) Efficient estimation of CFA pattern configuration in digital camera images. In: Media forensics and security, pp 754111–754123
37. Long Y, Huang Y (2006) Image based source camera identification using demosaicking. In: 8th IEEE workshop on multimedia signal processing, pp 419–424
38. Li CT, Chang C, Li Y (2010) On the reputability of device identification and image integrity verification using sensor pattern noise. In: Weerasinghe D (ed) ISDF2009, LNICST, vol 41, pp 19–25
39. Li CT, Li Y (2010) Digital camera identification using colour-decoupled photo response non-uniformity noise pattern. In: IEEE international symposium on circuits and systems, pp 3052–3055
40. Liu BB, Hu Y, Lee HK (2010) Source camera identification from significant noise residual regions. In: 17th IEEE international conference on image processing, pp 1749–1752
41. Liu Q, Li X, Chen L, Cho H, Cooper AP, Chen Z, Qiao M, Sung AH (2012) Identification of smart phone image source and manipulation. In: Advanced research in applied artificial intelligence, lecture notes in computer science, vol 7345. Springer, Berlin, pp 262–271. https://doi.org/10.1007/978-3-642-31087-428
42. Lukas J, Fridrich J, Goljan M (2006) Detecting digital image forgeries using sensor pattern noise. In: Security, steganography, and watermarking of multimedia contents, electronic imaging, vol 6072, pp 15–26
43. Marra F, Poggi G, Sansone C, Verdoliva L (2015) Evaluation of residual-based local features for camera model identification. In: International conference on image analysis and processing, pp 11–18
44. Marra F, Poggi G, Sansone C, Verdoliva L (2016) Correlation clustering for PRNU-based blind image source identification. In: IEEE international workshop on information forensics and security, pp 1–6
45. Marra F, Poggi G, Sansone C, Verdoliva L (2017) A study of co-occurrence based local features for camera model identification. Multimed Tools Appl 76(4):4765–4781
46. McKay C, Swaminathan A, Gou H, Wu M (2008) Image acquisition forensics: forensic analysis to identify imaging source. In 2008 IEEE international conference on acoustics, speech and signal processing, pp 1657–1660
47. Ozparlak L, Avcibas I (2011) Differentiating between images using wavelet-based transforms: a comparative study. IEEE Trans Forensics Secur 6(4):1418–1431
48. Piva A (2013) An overview on image forensics. ISRN Signal Process 496701:1–22
49. Popescu AC, Farid H (2004) Statistical tools for digital forensics. Inf Hiding 3200:395–407
50. Popescu AC, Farid H (2005) Exposing digital forgeries by detecting traces of resampling. IEEE Trans Signal Process 53(2):758–767
51. Rabbani M (2002) JPEG2000 Image compression fundamentals, standards and practice. J Electron Imaging 11(2):286–292
52. Sandoval Orozco AL, Arenas Gonzlez DM, Corripio JR, Villalba LJG, Castro JCH (2014) Source identification for mobile devices, based on wavelet transforms combined with sensor imperfections. Computing 96(9):829–841. https://doi.org/10.1007/s00607-013-0313-5
53. Sandoval Orozco AL, Corripio JR, Villalba LJG, Castro JCH (2016) Image source acquisition identification of mobile devices based on the use of features. Multimedia Tools Appl 75(12):7087–7111
54. Swaminathan A, Wu M, Liu KR (2008) Digital image forensics via intrinsic fingerprints. IEEE Trans Inf Forensics Secur 3(1):101–117
55. Takamatsu J, Matsushita Y, Ogasawara T, Ikeuchi K (2010) Estimating demosaicing algorithms using image noise variance. In: IEEE conference on computer vision and pattern recognition, pp 279–286
56. Tsai MJ, Lai CL, Liu J (2007) Camera/mobile phone source identification for digital forensics. In: 2007 IEEE international conference on acoustics, speech and signal processing—ICASSP'07, vol 2, pp II-221
57. Tuama A, Comby F, Chaumont M (2016) Camera model identification with the use of deep convolutional neural networks. In: 2016 IEEE international workshop on information forensics and security (WIFS), pp 1–6
58. Van LT, Emmanuel S, Kankanhalli M (2007) Identifying source cell phone using chromatic aberration. In: IEEE international conference on multimedia and expo, pp 883–886. https://doi.org/10.1109/ICME.2007.4284792
59. Wang B, Guo Y, Kong X, Meng F (2009) Source camera identification forensics based on wavelet features. In: International conference on intelligent information hiding and multimedia signal processing, pp 702–705
60. Wang W, Dong J, Tan T (2009) Effective image splicing detection based on image chroma. In: 16th IEEE international conference on image processing, Cairo, Egypt, pp 1257–1260
61. Xu B, Wang X, Zhou X, Xi J, Wang S (2016) Source camera identification from image texture features. Neurocomputing 207:131–140
62. Yang P, Ni R, Zhao Y, Zhao W (2019) Source camera identification based on content-adaptive fusion residual networks. Pattern Recognit Lett 119:195–204
63. Zeng H (2016) Rebuilding the credibility of sensor-based camera source identification. Multimed Tools Appl 75(21):13871–13882
64. Zhao X, Stamm MC (2016) Computationally efficient demosaicing filter estimation for forensic camera model identification. In: 2016 IEEE international conference on image processing (ICIP), pp 151–155