International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:12, No:10, 2018

Digital Image Forensics: Discovering the History of Digital Images

Gurinder Singh, Kulbir Singh

***Abstract*—**Digital multimedia contents such as image, video, and audio can be tampered easily due to the availability of powerful editing softwares. Multimedia forensics is devoted to analyze these contents by using various digital forensic techniques in order to validate their authenticity. Digital image forensics is dedicated to investigate the reliability of digital images by analyzing the integrity of data and by reconstructing the historical information of an image related to its acquisition phase. In this paper, a survey is carried out on the forgery detection by considering the most recent and promising digital image forensic techniques.

***Keywords*—**Computer forensics, multimedia forensics, image ballistics, camera source identification, forgery detection.

I. Introduction

IN forensic science, technical and scientific approaches are applied to discover the evidences of forgery or tampering from the digital multimedia contents (image, video and audio). The digital sensors can capture the real world information such as image or audio files and transform them into digital data or information which can be stored and processed by the computers. A computer expert can easily alter or tamper the digital information. Thus, the reliability of the digital information is one of the primary concerns. Many powerful forensic tools are available for the investigators due to the dynamic growth of new applications in forensic science related to the different fields of science. Digital forensics is one of the forensics fields which relate the forensics with computer science. Subsequently, it has evolved into new fields such as Computer Forensics, Disk Forensics, Network Forensics, etc.

In the early notion of digital forensics, the Federal agents of United States first started to discover and investigate the digital evidences in the 1980s. Afterwards, in 1990s, the academia researchers realized that the digital forensics can accelerate the speed of investigation to an unexpected level. The first definition of Digital Forensic Science was given in the first Digital Forensics Research Workshop (DFRWS) in 2001 as:

> "The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations".

The rapid growth of network socialization increases the demand of multimedia social network (MSNs) services. Thus, MSNs create various security issues related to multimedia contents. The MSNs provide applications such as Facebook, Flickr, Instagram, YouTube etc. for sharing of digital image, audio and video and other multimedia contents. More than 1 billion images are shared each day just on Facebook, hence producing another issue known as Big Data. Therefore, another sector comes under the category of digital forensics named as Multimedia Forensics [1]. Multimedia forensics brings together the researchers of different groups, such as signal processing, digital imaging and computer forensics. Digital image forensics utilizes various image forensics approaches to validate the truthfulness of an image.

The remainder of this paper includes the brief survey of various recent and efficient techniques for image forgery detection.

II. Digital Image Ballistics

The recent advancements of digital image forensics make it possible to identify the camera type, model, and the sensor used for shooting the image or video. This can be accomplished by exploiting the traces or fingerprints left during the image acquisition phase. The connection between the image and device can be utilized to trace the criminal activities such as images or videos related to the child pornography or terroristic action. Hence, the information related to camera device enhances the level of investigation.

The concept of device fingerprinting can be extended to variety of other traces which are present in the digital contents. For example, when the image is processed by some particular processing suite, or when it is uploaded to some social networking site. The analysis of such traces can enable the Law Enforcement Agencies (LEAs) with new analytical tools. These tools can be effectively used against the cybercrimes.

Most of the effective image ballistics techniques are utilized for the classification of digital images i.e. the considered image is acquired with scanner devices or created by the camera or tampered with some editing software. These techniques are based on the analysis of the traces related to each of the acquisition steps such as lens aberration, color interpolation, sensor imperfections and compression formats. The acquisition pipeline for a digital image is shown in Fig. 1.

The objective of the image ballistics techniques is to classify the model and features related to the device used for shooting. This information related to the device properties

Gurinder Singh and Kulbir Singh are with the Department of Electronics and Communication Engineering Thapar University, Patiala, Punjab, India (e-mail: gurinder.singh@thapar.edu, ksingh@thapar.edu).

helps to exploit the origin of digital image. Different schemes related to the image ballistics are described in the following subsections.

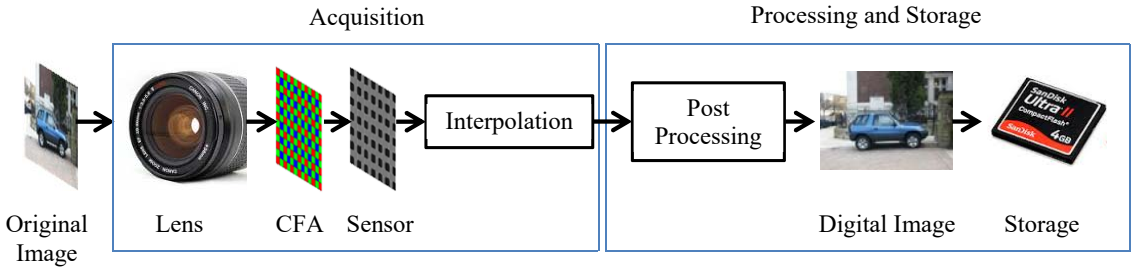


Fig. 1 Acquisition pipeline of a digital image

A. Lens Aberration Methods

Many different kinds of imperfections are introduced during the manufacturing process of lenses that may be due to the material impurities, machinery defects etc. These imperfections result in the creation of different kinds of aberrations in the digital images. The radial and chromatic distortions are the two main aberrations which are analyzed to solve the identification problem of source camera [2]-[4]. The radial distortions are introduced due to the spherical surfaces of lens used in the digital cameras. The manufacturers of the camera lenses are making the spherical surfaces to decrease the production cost. The straight lines in the object space caused by the radial distortion of the spherical lenses rendered as curved lines on the camera sensor. This happens when there is a change in transverse magnification with increasing distance from the optical axis. The degree of such distortion varies according to the different camera models and different manufacturers.

A method is proposed in [2] to analyze the distortion parameters providing the fingerprint for the identification of camera source. This method is established by considering the technique based on the Devernay's straight line proposed in [5]. But, this technique does not provide satisfactory results when there is an absence of straight lines in the considered image and when the two cameras of same models are compared. Besides, the problem of radial distortion can be solved by operating the software correction.

The chromatic aberration occurs when the light of different wavelengths fails to meet at the same point of the focal plane. There are two types of chromatic distortions i.e. longitudinal and lateral distortion. In the case of longitudinal distortion, different wavelengths are focused at different distances from the lens. Secondly, the lateral distortion corresponds to the different positions on the sensor. The chromatic aberration produces various types of color imperfections on the resultant image. The lateral chromatic distortion is considered in the work [3] to identify the source of cell phone devices by employing the SVM classifier.

B. CFA Interpolation Schemes

The fingerprints left by the interpolation process during the image acquisition phase can be utilized to localize the altered regions. In the image acquisition process, color filter array (CFA) is used to filter the light coming from the real world. Afterwards, the filtered light falls on the charge couple device (CCD) sensor such that only one particular color is available for each pixel. Hence the interpolation process is used to acquire the other two colors for each pixel. The artifacts left during the interpolation process can be explored to find the digital forgeries.

The image coming from the digital camera shows demosaicing artifacts on every cluster of pixels corresponding to a CFA component. When this image is forged or tampered, the demosaicing artifacts become inconsistent. Therefore, during the digital investigation, the occurrence of demosaicing inconsistencies reveals that the considered image is a doctored one.

The camera source identification techniques are concentrated on the detection of the CFA pattern and the color interpolation algorithm engaged during the internal processing steps of digital camera used to capture an image [6]. In [7], a camera identification scheme is proposed by Swaminathan et al. based on the estimation of CFA pattern and interpolation kernel. In this technique, linear approximation is used to evaluate the coefficients of color interpolation for the CFA pattern in various kinds of texture of the image such as smooth, horizontal and vertical gradient image regions.

C. Sensor Imperfections Methods

The systematic errors are introduced in the digital image due to the sensor imperfections. These errors are exploited by the various sensor imperfections based techniques for the camera source identification. The sensor imperfections can be analyzed by capturing an image of an absolutely evenly lit scene. The resultant image reveals small fluctuations in intensity among distinct pixels. The sensor's pixel defects and a noise pattern are included in these errors. The noise pattern can be categorized into two components i.e. fixed pattern noise and photo response non-uniformity noise (PRNU).

Multiple images obtained from the same camera are analyzed to estimate the widespread noise in low-cost digital cameras. Lukas et al. [8] proposed a technique to compute the reference pattern noise for each camera under investigation and this pattern noise exploits the unique identification

fingerprint. The reference pattern noise is considered as a spread-spectrum watermark in an image which is detected by the correlation detector to identify the camera from a given image.

The number of images from a particular camera and image content make it difficult to calculate the PRNU. Thus, a sharpening scheme is suggested in [9] by Lawgaly et al. to magnify the PRNU components for enhanced estimation, which results in better performance of camera source identification. In [10], Debiasi et al. proposed a PRNU enhancing technique in which the enhancement of PRNU is parameterized based on image contents.

D. JPEG Analysis Based Techniques

The JPEG format becomes a virtual standard and therefore, most of the camera devices and softwares utilize the JPEG format for the encoding purposes. The JPEG compression is lossy in nature and the image can be compressed at different quality factors. Different models of camera devices have different setting related to the compression parameter i.e. quantization matrix.

The source of an image is identified by analyzing the difference of compression parameter between the two images taken from two different cameras. Farid et al. [11] proposed the first technique on image ballistics considering the analysis of JPEG quantization tables. Afterwards, the efficacy of the notion was confirmed in the subsequent works [12], [13].

The first quantization matrix is always lost in the case of multiple compressed JPEG images. The estimation of first quantization matrix can boost the investigation of digital images. Moreover, the identification of the acquisition device can be done through the estimation of first quantization matrix from the multiple compressed JPEG images [14], [15].

The social networking sites such as Facebook, Instagram etc. provide the users an interface to upload and share the large amounts of images. These social platforms alter the digital images for bandwidth, storage and layout reasons. Thus, these alterations are responsible to make the existing techniques of camera identification less reliable.

The processing of social platforms modifies the digital information of an image to great extent and leaves fingerprints on the JPEG image format [16], [17]. These fingerprints can be exploited to understand if the image has been actually uploaded to a specific social platform.

The meta-data stored on the JPEG files can be exploited by using various techniques based on the JPEG standard. Most of the digital cameras encapsulate meta-data in JPEG files in EXIF format [18], [19]. The EXIF data information saved by the acquisition device includes information related to producer, camera model, date and time of image formation, GPS coordinates, information related to characteristics of the image such as pixel resolution, dpi, color depth, etc., shooting settings and others. The EXIF information can be manipulated easily. Therefore, image ballistics based on this EXIF information is weak because there is no guarantee that whether all the information recovered is genuine. An image authentication technique is proposed based on the analysis of EXIF information by Kee et al. [12] for the image forgery detection.

E. Discussion

The consideration of forensics fingerprinting techniques is a challenging task in the real world investigation scenarios due to various concerns. The lack of robustness in the realistic operating circumstances is the first concern. The existing state-of-the-art approaches provide better results when tested under the controlled conditions. However, the application of these techniques is problematic in the realistic settings. The accuracy of these techniques drops dramatically under the realistic conditions [20]. This is particularly happens in the case of videos because the adoption of video compression techniques generally constrains the extraction of fingerprints [21], [22]. This problem becomes major issue when the evidences gathered by the forensic tools are presented as a proof in court.

The necessity of processing the large amount of data is the second concern which is essential in numerous investigation scenarios. For instance, large number of images and videos extracted from the seized hard drives must be processed in a timely fashion in the case of child abuse or terrorism. A few schemes are available in the literature allowing the extraction and analysis of device fingerprints contained in large amount of images [23]. However, these methods have not been extensively authenticated on the real world data. There are many issues related to these techniques such as their scalability to large amount of images and their robustness to simple processing operations [24].

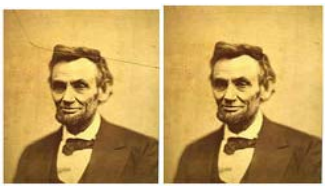
The real world investigations are characterized by the necessity to analyze the heterogeneous data originated from different sources. The textual metadata related to multimedia contents such as file headers, annotations or accompanying text etc. can be utilized to complement the information inferable from the digital media itself. This task is difficult to perform because it involves the techniques related to multi-clue and complex data fusion [25], [26]. Moreover, the provided information is incomplete and unreliable in nature. For example, as opposed to laboratory conditions, the class of device used for shooting is not fully known [27]-[29]. Therefore, proper tools are developed to combine the evidences acquired through different means and with different reliability.

Most of the forensics techniques can be fooled by the adoption of simple counter-forensics techniques [30]. The criminals can create the fake evidences by attaining sufficient information about the forensic tools. This creates many problems during the use of forensic evidence in court. Anti-counter-forensics techniques are developed to do the forensics of multimedia contents after the application of Anti-forensic techniques. The Anti-counter-forensics techniques developed so far are usually limited to one attack at a time. The researchers are interested and motivated by these concerns related to the integrity and security of the multimedia contents [31].

III. Image Integrity and Authentication

(a) (b)

Fig. 2 (a) Original image of Ann-Margret (b) This doctored photograph belongs to the talk-show host Oprah Winfrey and was displayed by the cover of TV Guide in 1989. The head of Winfrey was spliced on the body of Ann-Margret, taken from the photo captured in 1979



(a) (b)

Fig. 3 (a) Abraham Lincoln photograph taken by Alexander Gardner in 1865 (b) Image after inpainting

(a) (b)

Fig. 4 (a) Original image of actress Minnie Driver (b) Image after skin features enhancement

(a) (b)

Fig. 5 (a) Original image (b) Image after retouching: The Iran Army released this doctored picture in which four missiles are shown in place of three to exaggerate the power of their army

The image forgery creation is a difficult task to perform in back 1946 and it requires a collection of tools, an enormously steady hand, and a very sharp eye. Nowadays, digital image manipulation and retouching can be performed easily by using image processing software's such as GIMP, Adobe Photoshop etc. Moreover, image tampering can be done immediately by using camera applications in mobile phones that are embedded with the capabilities of image filtering, enhancing and editing. The image can be modified by applying the operations like splicing, inpainting, enhancement and retouching as shown in Figs. 2-5.

An image can be considered as forgery depending upon the situation in which it is used. The image can be changed just to enhance a bad image. Therefore, it is possible to agree that all the photo editing operations which are utilized to enhance the image appearance cannot be considered as forgery.

Hitler had removed his loyal colleague Joseph Goebbels from his photo as shown in Fig. 6. The missing person Joseph Goebbels is one of the top propagandist and architects of the holocaust. Furthermore, the Honorable Prime Minister of India, Mr. Narendra Modi doing an aerial survey of the flood-hit areas of Chennai somewhere in between 8th November 2015 to 14th December 2015. This photograph was posted by Press Information Bureau (PIB) on their website, and it took twitter by storm. This photograph was actually doctored by PIB and was conclusively removed as shown in Fig. 7.

(a) (b)

Fig. 6 (a) Original image (b) Doctored image

(a) (b)

Fig. 7 (a) Original image (b) Doctored image

There are two types of image authentication approaches i.e. active and passive approaches. To achieve the authentication of the image, the active approaches introduce or attach supplementary data on images. On the other hand, the passive approaches exploit the intrinsic information of images for the detection of image forgeries.

A. Active Image Authentication Schemes

The active image authentication schemes are based on conventional cryptography, watermarking and digital fingerprints based on image contents. A hash function is used to calculate a message verification code from the images by the image validation techniques based on cryptography. The resultant hash is encoded with the help of a special confidential key of the sender and then added to an image. The techniques considering the hash computation of an image lines

and columns are called as line-column hash functions. In this approach, hashes corresponding to every line and column of an image are obtained. These hashes are stored and compared subsequently with those obtained from the image to be tested. If the hashes are found to be changed then the considered image is manipulated and the tampered region is detected, otherwise the image is declared authentic [32].

The authentication methods based on watermarking involve in computing a portion of data or information and hiding it in the image. The authentication is performed by extracting the hidden data. The watermarking techniques are based on the concept that a watermark is generated and it is inserted into the image in such a way that any alteration made to an image is also reflected on the watermark. Thus, the image integrity confirmation and localization of altered regions can be done by merely confirming the existence of inserted watermark.

The watermarking is considered to be fragile in the case when it cannot tolerate any image distortion. Therefore, if all the pixels of an image remain unchanged then the considered image is genuine. The first fragile watermarking algorithm is based on the set of image pixels selected with the help of secret key.

An image authentication technique based on fragile watermarking was recommended by Walton in [33] considering only the image data to produce the watermark. This method is based on the insertion in the least significant bits (LSB). The grey level of the seven most significant bits (MSB) of pseudo-randomly nominated pixels is considered to calculate the checksum. This technique can detect and localize the tampered regions but have no restoration abilities. But this approach fails to detect the manipulations in the case when the blocks from the similar location of two different images, which are secured with the identical key were exchanged. To resolve this issue, many improvements were made to this technique based on the extraction of more robust bits [34]. The other active approaches exploit the image high level features like SIFT that can be encoded in a codebook and attached to an image. Therefore, the recipient can confirm the integrity of the receiving image by extracting the features and compare them to the original attached codebook. A robust image alignment tool based on SIFT is proposed by Battiato et al. in [35] for the forgery detection.

B. Passive Image Authentication Schemes

The passive authentication techniques can detect the image manipulations or tampering without any need of additional data. In the case of skilled forgery, many post-processing approaches are available that can be applied to conceal the artificial traces and thus making the forensics techniques less effective. Therefore, the enhancement of forensics techniques has become an important subject for the researchers.

Majority of work has been concentrated on copy-move forgery detection and splicing detection. The forgery detection scheme [36] is based on the image pixel blocks and analyzing the specific and deterministic transformation such as translations, rotations and scale transformations to identify the tampered region. The approaches based on the features extraction from different color spaces and then exploited by the SVM classifier provide better results [37]. In [38], splicing detection technique is proposed based on the analysis of incoherences in frequency domain. This technique exploits a shift-invariant version of the discrete wavelet transform for the data analysis. Furthermore, the splicing detection technique based on the study of intrinsic noise of an image proposed in [39] provides better results in the detection of tampered regions. Tables I and II provide the comparative analysis of various copy-move forgery and splicing detection techniques respectively.

TABLE I
COMPARATIVE ANALYSIS OF COPY-MOVE FORGERY DETECTION TECHNIQUES

Technique	Extracted Feature	Classifier	Detection Error
Lin et al. [54]	Average intensity of image blocks	Radix sort and Shift vector	2.00%
Basher et al. [55]	DWT & KPCA	Point based tampering detection procedure	4.45% (DWT) 9.06% (KCPA)
Sutthiwan et al. [56]	Image luminance using RAKE model & Image chroma using edge statistics	SVM	1.00%
Xunyu & Siwei [57]	Matched SIFT Keypoints	K-mean Clustering	0.92%
Muhammad et al. [58]	Dyadic wavelet transform	Thresholding Classification	1.66%
Zhao & Guo [59]	DCT & SVD	Lexicographical sorting of blocks	3.90%

TABLE II
COMPARATIVE ANALYSIS OF SPLICING DETECTION TECHNIQUES

Technique	Extracted Feature	Classifier	Detection Error
Fu et al. [60]	Hilbert-Huang Transform & Wavelet decomposition based features	SVM	19.85%
Chen et al. [61]	Moments of wavelet characteristics & 2D phase congruency	SVM	17.68%
Zhang et al. [62]	Moment features from multi size block features (MBDCT) & Image quality Metrics	SVM	12.90%
Zhen Hua et al. [63]	Edge sharpness measure and visual saliency	SVM	3.67%
Fang et al. [64]	Color edges sharpness	LDA	10.00%
Zhao et al. [37]	Grey level run length number vectors	SVM	5.30%

The forgery detection in digital images becomes a challenging task, when multiple post-processing operations are applied on images. In the case of complex editing, forgery detection can be performed by analyzing the geometry and physical features in the contents of the images. An approach is proposed for the detection of forged images in [40] based on scene illumination by exploring the contents of images. In [41], an image falsification detection scheme is proposed based on the analysis of image edges distribution. Furthermore, forgery detection techniques are proposed in [42]-[45] exploiting the SVM classifiers based on the comparison of high level features such as SIFT and SURF of genuine images with the tampered ones. The median or blurring filters are applied on digital images in order to conceal the image tampering. In this case, forgeries can be detected by using the automatic detection techniques proposed in [46], [47].

The JPEG format provides useful information for image ballistics as well as for the forgery detection. The image falsification detection approaches based on the analysis of JPEG blocking artifacts are proposed in [48], [49]. In [12], a forgery detection approach is proposed based on the investigation of JPEG headers. The forgery detection methods based on the analysis of thumbnails and EXIF are proposed in [50], [51] respectively. Moreover, in [19], [52], [53], tampering detection methods are proposed based on the analysis of DCT coefficients.

IV. Conclusions

Multimedia forensics finds its significance in today's scenarios where a bulk of information is being shared in the form of digital images, videos and audios. In this paper, a brief survey is conducted on the digital image forensics considering the image ballistics and image authentication techniques. Through reconstruction of digital image life cycle, various fingerprints left in the image can be extracted and can be tested for inconsistencies. These inconsistencies would ultimately help for the detection as well as localization of tampering in the image. No doubt that image forgery techniques are becoming more and more sophisticated with the advent of technology, but there are certain issues which are needed to be resolved. It can be observed from the literature that limited work has been devoted to the characterization of traces or artifacts from the chain of acquisition stages. So, there is a scope to consider the whole acquisition system to design the algorithms for the real application scenarios. Furthermore, the positive decision of one forgery detection algorithm may inherently imply the negative decision of another algorithm. This happens because both the algorithms search for mutually excluding traces. Thus, it is not a trivial task to take a decision on the integrity of an image based on the output of a set of forensic tools.

Acknowledgment

This work was supported by the Department of Electronics and Information Technology, Ministry of Communications and Information Technology, Government of India (grant PhD-MLA/4(33)/2015-16/01).

References

[1] K. J. R. Liu, "Multimedia Forensics: Where Sherlock Holmes Meets Signal Processing," Invited talk @ ICME 2006.
[2] K. S. Choi, E. Y. Lam, and K. K. Y. Wong, "Source camera identification using footprints from lens aberration," in Proc. of SPIE conference on Digital Photography II, vol. 6069, 2006.
[3] L. T. Van and S. Emmanuel, "Identifying source cell phone using chromatic aberration," in Proc. of IEEE International Conference on Multimedia and Expo, 2007.
[4] M. K. Johnson and H. Farid, "Exposing digital forgeries through chromatic aberration," in Proc. of the 8th ACM workshop on Multimedia & Security, 2006.
[5] F. Devernay and O. Faugeras, "Automatic calibration and removal of distortion from scenes of structured environments," in Proc. of SPIE conference on Investigative and Trial Image Processing, vol. 2567, pp. 62–67, 1995.
[6] S. Bayram, H. Sencar, N. Memon, and I. Avcibas, "Source camera identification based on CFA interpolation," in Proc. of IEEE international conference on Image processing, 2005.
[7] M. A. Swaminathan and K. J. R. Liu, "Non-intrusive forensics analysis of visual sensors using output images," in Proc. of IEEE international conference on Image processing, 2006.
[8] J. Lukas, J. Fridrich, and M. Goljan, "Digital camera identification from sensor pattern noise," IEEE Transactions on Information Forensics and Security, vol. 1, no. 2, pp. 205 – 214, June 2006.
[9] A. Lawgaly, F. Khelifi, and A. Bouridane, "Image Sharpening for Efficient Source Camera Identification Based on Sensor Pattern Noise Estimation," in Proc. of IEEE international conference on Emerging Security Technologies, pp. 113 - 116, September 2013.
[10] L. Debiasi and A. Uhl, "Blind biometric source sensor recognition using advanced PRNU fingerprints," in Proc. of IEEE conference on Signal Processing, 2015.
[11] H. Farid, "Digital image ballistics from JPEG quantization," Technical Report, Department of Computer Science, Dartmouth College, 2006.
[12] E. Kee, M. K. Johnson, and H. Farid, "Digital image authentication from JPEG headers," IEEE Transactions on Information Forensics and Security, vol. 6, no. 3, pp. 1066-1075, 2011.
[13] J. D. Kornblum, "Using JPEG quantization tables to identify imagery processed by software," in Proc. of Digital Investigation 5, pp. S21-S25, 2008.
[14] W. Luo, J. Huang, and G. Qiu, "JPEG error analysis and its applications to digital image forensics," IEEE Transactions on Information Forensics and Security, vol. 5, no. 3, pp. 480-491, 2010.
[15] F. Galvan, G. Puglisi, A. R. Bruna, and S. Battiato, "First quantization matrix estimation from double compressed JPEG images," IEEE Transactions on Information Forensics and Security, vol. 9, no. 8, pp. 1299-1310, 2014.
[16] M. Moltisanti, A. Paratore, S. Battiato, and L. Saravo, "Image Manipulation on Facebook for Forensics Evidence," in Proc. International Conference on Image Analysis and Processing, pp. 506-517, 2015.
[17] A. Castiglione, G. Cattaneo, and A. D. Santis, "A Forensic Analysis of Images on Online Social Networks," in Proc. International Conference on Intelligent Networking and Collaborative Systems, pp. 679-684, 2011.
[18] CIPA DC-008, "Exchangeable image file format for digital still cameras: EXIF Version 2.3," 2012.
[19] S. Battiato, M. Mancuso, and A. Bosco, "Psychovisual and statistical optimization of quantization tables for DCT compression engines," in Proc. of IEEE international conference on Image Analysis and Processing, pp. 602-606, 2001.
[20] T. Gloe, M. Kirchner, A. Winkler, and R. Böhme, "Can we trust digital image forensics?," in Proc. of the 15th ACM international conference on Multimedia, pp. 78-86, 2007.
[21] P. Bestagini, A. Allam, S. Milani, M. Tagliasacchi, and S. Tubaro, "Video codec identification," in Proc. of IEEE International Conference on Acoustics, Speech and Signal Processing, pp. 2257-2260, 2012.
[22] P. Bestagini, S. Milani, M. Tagliasacchi, and S. Tubaro, "Local tampering detection in video sequences," in Proc. of IEEE International Workshop on Multimedia Signal Processing, pp. 488-493, 2013.

[23] M. Goljan, J. Fridrich, and T. Filler, "Managing a large database of camera fingerprints," in Proc. of SPIE conference on Media Forensics and Security II, pp. 754108-754108, 2010.
[24] D. Valsesia, G. Coluccia, T. Bianchi, and E. Magli, "Compressed fingerprint matching and camera identification via random projections," IEEE Transactions on Information Forensics and Security, vol. 10, no. 7, pp. 1472-1485, 2015.
[25] M. Fontani, T. Bianchi, A. De Rosa, A. Piva, and M. Barni, "A framework for decision fusion in image forensics based on Dempster–Shafer theory of evidence," IEEE Transactions on Information Forensics and Security, vol. 8, no. 4, pp. 593-607, 2013.
[26] D. Cozzolino, D. Gragnaniello, and L. Verdoliva, "Image forgery localization through the fusion of camera-based, feature-based and pixel-based techniques," in Proc. of IEEE International Conference on Image Processing, pp. 5302-5306, 2014.
[27] F. D. O. Costa, E. Silva, M. Eckmann, W. J. Scheirer, and A. Rocha, "Open set source camera attribution and device linking," Pattern Recognition Letters, vol. 39, pp. 92-101, 2014.
[28] I. Amerini, R. Caldelli, P. Crescenzi, A. Del Mastio, and A. Marino, "Blind image clustering based on the normalized cuts criterion for camera identification," Signal Processing: Image Communication, vol. 29, no. 8, pp. 831-843, 2014.
[29] Y. Huang, J. Zhang, and H. Huang, "Camera Model Identification With Unknown Models," IEEE Transactions on Information Forensics and Security, vol. 10, no. 12, pp. 2692-2704, 2015.
[30] R. Böhme and M. Kirchner, "Counter-forensics: Attacking image forensics," Digital Image Forensics, pp. 327-366, 2013.
[31] M. Barni and F. Pérez-González, "Coping with the enemy: Advances in adversary-aware signal processing," in Proc. of IEEE International Conference on Acoustics, Speech and Signal Processing, pp. 8682-8686, 2013.
[32] A. Haouzia and R. Noumeir, "Methods for image authentication: a survey," Multimedia tools and applications, vol. 39, no. 1, pp. 1-46, 2008.
[33] S. Walton, "Image Authentication for a Slippery New Age," Dr. Dobb's Journal, pp. 18-26, 1995.
[34] I. J. Cox and M. G. Linnartz, "Public watermarks and resistance to tampering," in Proc. IEEE conference on image processing, 1997.
[35] S. Battiato, G. M. Farinella, E. Messina, and G. Puglisi, "Robust image alignment for tampering detection," IEEE Transactions on Information Forensics and Security, vol. 7, no. 4, pp. 1105-1117, 2012
[36] S. B. Solorio and A. K. Nandi, "Automated detection and localisation of duplicated regions affected by reflection, rotation and scaling in image forensics," Signal Processing, vol. 91, no. 8, pp. 1759-1770, 2011.
[37] X. Zhao, J. Li, S. Li, and S. Wang, "Detecting digital image splicing in chroma spaces," in Proc. of International Workshop on Digital Watermarking, pp. 12-22, 2010.
[38] G. Muhammad, M. Hussain, K. Khawaji, and G. Bebis, "Blind copy move image forgery detection using dyadic undecimated wavelet transform," in Proc. of International Conference on Digital Signal Processing, pp. 1-6, 2011.
[39] X. Pan, X. Zhang, and S. Lyu, "Exposing image forgery with blind noise estimation," in Proc. of 13th ACM multimedia workshop on Multimedia and security, pp. 15-20, 2011.
[40] C. Riess and E. Angelopoulou, "Scene illumination as an indicator of image manipulation," in Proc. of International Workshop on Information Hiding, pp. 66-80, 2010.
[41] G. Cao, Y. Zhao, and R. Ni, "Edge-based blur metric for tamper detection," Journal of Information Hiding and Multimedia Signal Processing, vol. 1, no. 1, pp. 20-27, 2010.
[42] B. L. Shivakumar and L. D. S. S. Baboo, "Detection of region duplication forgery in digital images using SURF," International Journal of Computer Science Issues, vol. 8, no. 4, pp. 199-205, 2011.
[43] X. Bo, W. Junwen, L. Guangjie, and D. Yuewei, "Image copymove forgery detection based on SURF," in Proc. of International Conference on Multimedia Information Networking and Security, pp. 889-892, 2010.
[44] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra, "Geometric tampering estimation by means of a SIFT-based forensic analysis," in Proc. of IEEE International Conference on Acoustics, Speech and Signal Processing, pp. 1702-1705, 2010.
[45] X. Pan and S. Lyu, "Detecting image region duplication using SIFT features," in Proc. of IEEE International Conference on Acoustics, Speech and Signal Processing, pp. 1706-1709, 2010.
[46] G. Cao, Y. Zhao, R. Ni, L. Yu, and H. Tian, "Forensic detection of median filtering in digital images," in Proc. IEEE International Conference on Multimedia and Expo, pp. 89-94, 2010.
[47] F. Peng and X. L. Wang, "Digital image forgery forensics by using blur estimation and abnormal hue detection," in Proc. of IEEE Symposium on Photonics and Optoelectronics, pp. 1-4, 2010.
[48] A. R. Bruna, G. Messina, and S. Battiato, "Crop detection through blocking artifacts analysis," in Proc of International Conference on Image Analysis and Processing, pp. 650-659, 2011.
[49] W. Luo, Z. Qu, J. Huang, and G. Qiu, "A novel method for detecting cropped and recompressed image block," in Proc. IEEE International Conference on Acoustics, Speech and Signal Processing, pp. II-217-220, 2007.
[50] E. Kee and H. Farid, "Digital image authentication from thumbnails," in Proc. of SPIE conference on Media Forensics and Security II, pp. 75410E-75410E, 2010.
[51] T. Gloe, "Forensic analysis of ordered data structures on the example of JPEG files," in Proc. of IEEE International Workshop on Information Forensics and Security, pp. 139-144, 2012.
[52] S. Battiato and M. Giuseppe, "Digital forgery estimation into DCT domain: a critical analysis," in Proc. of ACM workshop on Multimedia in forensics, 2009.
[53] G. Singh and K. Singh, "Forensics for partially double compressed doctored JPEG images," Multimedia tools and applications, vol. 75, no. 24, pp. 1-18, 2016.
[54] H. Lin, C. Wang, and Y. Kao, "An efficient method for copy-move forgery detection", in Proc. of 8th International Conference on Applied Computer and Applied Computational Science, pp. 250-253, 2009.
[55] M. Bashar, K. Noda, N. Ohnishi, and K. Mori, "Exploring duplicated regions in natural images," IEEE Transactions on Image Processing, pp. 1-40, 2010.
[56] P. Sutthiwan, Y. Q. Shi, S. Wei, and N. Tian-Tsong, "Rake transform and edge statistics for image forgery detection," in Proc. IEEE International conference on multimedia and Expo, pp. 1463-1468, 2010.
[57] P. Xunyu and L. Siwei, "Region duplication detection using image feature matching," IEEE Transactions on Information Forensics and Security, vol. 5, no. 4, pp. 857-867, 2011.
[58] G. Muhammad, M. Hussain, and G. Bebis, "Passive copy move image forgery detection using undecimated dyadic wavelet transform," Digital Investigation, vol. 9, pp. 49-57, 2012.
[59] J. Zhao and J. Guo, "Passive forensics for copy-move image forgery using a method based on DCT and SVD," Forensic Science International, vol. 233, pp 158-166, 2013.
[60] D. Fu, Y. Shi, and W. Su, "Detection of image splicing based on Hilbert-Huang transform and moments of characteristic functions with wavelet decomposition," in Proc. of International workshop on digital watermarking, pp. 177-187, 2006.
[61] W. Chen, Y. Shi, and W. Su, "Image splicing detection using 2-d phase congruency and statistical moments of characteristic function," in Proc. of SPIE electronic imaging: security, stegnography, and watermarking of multimedia contents, 2007.
[62] W. Zhang, X. Cao, Y. Qu, Y. Hou, H. Zhao, and C. Zhang, "Detecting and extracting the photo composites using planar homography and graph cut," IEEE Transactions on Information Forensics and Security, vol. 5, no. 3, pp. 544-555, 2010.
[63] Q. Zhenhua, Q. Guoping, and H. Jiwu, "Detect digital image splicing with visual cues," in Proc. of International workshop on information hiding, pp. 247-261, 2009.
[64] Z. Fang, S. Wang, and X. Zhang, "Image splicing detection using color edge inconsistency," in Proc. International Conference on Multimedia Information Networking and Security, pp. 923-926, 2010.