Source Camera Identification Techniques: a Survey

Chijioke Emeka Nwokeji, Akbar Sheikh Akbari,
Antoliya Gorbenko and Iosif Mporas

July 17, 2023

Source Camera Identification Techniques: A Survey

Chijioke Emeka Nwokeji[1], Akbar Sheikh-Akbari[2*], Anatoliy Gorbenko[3], and Iosif Mporas[4]

[1,2,3] School of Built Environment, Engineering, and Computing, Leeds Beckett University, Leeds, U.K.

[4] School of Physics, Engineering & Computer Science, University of Hertfordshire, Hertfordshire, U.K.

Abstract. Successful investigation and prosecution of major crimes like child pornography, insurance claims, movie piracy, traffic monitoring, and scientific fraud among others, largely depends on the availability of water-tight evidence to prove the case beyond any reasonable doubt. When the evidence required in investigating and prosecuting such crimes involves digital images/ videos, there is a need to prove without an iota of doubt the source camera/device of the image in question. Much research has been reported to address this need over the past decade. The proposed methods can be divided into brand or model-level identification or known imaging device matching techniques. This paper investigates the effectiveness of the existing image/video source camera identification techniques, which use both intrinsic hardware artefacts-based techniques like sensor pattern noise, and lens optical distortion, and software artefacts-based techniques like colour filter array, and auto white balancing, to determine their strengths and weaknesses. Publicly available benchmark image/video datasets and assessment criteria to quantify the performance of different methods are presented and the performance of the existing methods is compared. Finally, directions for further research on image source identification are given

Keywords: Source camera identification, camera brand source identification, camera model source identification, sensor pattern noise, image lens optical distortion, camera colour filter array.

1 Introduction

The last few years have seen a significant increase in research interest in the field of digital image forensics because the easy availability of advanced and affordable devices has made the acquisition and manipulation of digital media images which used to be a professional job very easily accessible to the public giving room for untrusted media images and videos being in circulation. According to Su, Zhang & Ji in [1], the advancement in digital technology and the increasing number of images and video-sharing websites like YouTube, Facebook, Twitter, and other social media platforms has helped the spread of various kinds of less trusted images from individual sources on the internet. It is therefore very imperative to have a technology that can effectively trace digital cameras and be able to identify digital devices that took any digital image that will aid law enforcement officers and even the prosecutors in criminal investigations relating to child pornography, insurance claims, movie piracy, traffic monitoring and financial fraud, among others. Then the question is, can we really determine that images came from a specific digital source claimed to come from? The need to resolve these issues and more gave birth to what is now known as image forensics.

Image source identification is necessary for digital forensics, Chen, Pande, Zeng & Mohapatra [2] stated that identification of the acquisition device of digital image evidence to be presented in court is as important as the digital image itself. The objective of the source camera identification is to determine whether a given image was taken with a specific camera, as well as the camera model/brand and imaging mechanism used such as cameras, scanners, computer graphics or smartphones. As opined by Thai, Retraint & Cogranne in [3] the two active approaches for source camera identification such as digital signatures and digital watermarking have several drawbacks since specialized information must be incorporated during the generation of an image. Explaining the drawback further Chio, Lam & Wong in [4] asserts that most cameras in their images include an Exchangeable Image File Format (EXIF) header which comprises information such as the digital camera type, exposure, date, and time. This information, however, could be maliciously altered and could possibly be destroyed during the process of an image being resaved or recompressed.

The drawback of active techniques to source camera identification gave rise to passive techniques which Thai et. al. in [3] argued have received a lot of attention in the last decade because they do not impose any constraints and do not require any prior knowledge of the capturing device. And according to Bernacki in [5] the internal traces or unique artefacts left by the digital camera in each digital image serves as camera fingerprints that are used in passive techniques and investigating the image acquisition pipeline can offer these internal traces.

An overview of several methods for source digital camera identification will be discussed in Section 2 and Section 3 will be the conclusion and future studies.

2 Source Camera Identification Techniques

To help with image forensic investigations, researchers have proposed different techniques for source camera identification. This section, therefore, will provide an overview of various proposed techniques for source camera identification by examining state-of-the-art source camera identification approaches, intrinsic hardware artefacts-based methods that occur due to the imperfections of the manufacturing process, as well as those that use software-related properties will be reviewed.

2.1 Analysis of Sensor Pattern Noise

The imperfection in the manufacturing process of the image sensor chip, which results in pixel sensitivity variation in the imaging sensor, is the source of Sensor Pattern Noise (SPN). These pattern noises have a distinctive quality that makes them specific to that camera imaging sensor. Consequently, it serves as a "fingerprint" of that specific digital camera. The major component of SPN is the Photo Response Non-Uniformity (PRNU) noise. Therefore, analyzing the PRNU noise which is considered a unique camera fingerprint is one of the reliable methods for source camera identification using SPN.

In a study that has been considered as a benchmark source camera identification using SPN, Lukas et al [6], proposed an algorithm that used discrete wavelet transform for the decomposition of the original images into four subbands. They then applied a wiener denoising filter on the three resulting high-frequency subbands to denoise the high-frequency subbands, reconstructed the image and subtract the resulting denoised image from the original image to obtain the reference pattern noise of a particular image. The camera fingerprint is obtained by averaging the reference pattern noise of several images from the same camera under various conditions. Then, to determine if the image is from the reference camera, they used the normalized cross correlation as the measure.

Soobhany *et al* in [7] proposed another technique like [6] where they used discrete wavelet transform to decompose the input image into four wavelet sub-bands using non-decimated wavelet transform. To extract the SPN from the image, the coefficients inside the generated wavelet high-frequency sub-bands are denoised. The image SPN signature was compared to the camera reference SPN signature to determine the image's source camera.

Subsequently, Al-Athamneh et al [8] proposed the use of only the green component of the Red, Green, and Blue (RGB) of the color image for PRNU extraction while using a similar technique introduced in [6]. Akshatha et al [9] proposed a technique in which PRNU noise is removed from images using a wavelet-based denoising methodology and is represented by higher-order wavelet statistics (HOWS). Georgievska et al [10] proposed a camera identification method where images are clustered based on Peak to Correlation Energy (PCE) similarity scores of their PRNU patterns. Balamurugan et al in [11] proposed a technique that uses an improved Locally Adaptive Discrete Cosine Transform (LADCT) Filter followed by a weighted averaging method to exploit the content of images carrying PRNU efficiently. LADCT is believed to perform well on images with high image-dependent noise like multiplicative noise of which PRNU is one of such. Chen & Thing [12] adopted what they called Block Matching & 3D Filtering (BM3D) which is known as a collaborative filtering process. This grouped similar blocks extracted from images where each group is stacked together to form 3D cylinder-like shapes

2.2 Intrinsic Lens Radial Distortion

In a camera, a lens is a device that directs light toward a fixed focal point. The symmetric distortion caused by imperfection in the lens's curvature during the grinding process is known as radial lens distortion. Most image-capturing digital devices, as opined by Choi et al [13], include lenses with spherical surfaces; these lenses' intrinsic radial distortions act as a distinctive fingerprint for identifying source cameras. In this field, [13] made a ground-breaking proposal by proposing two kinds of features based on pixel intensities and distortion measurements, considering the peculiarities of the radial distortion that causes straight lines to become curved. Bernacki [5] proposed a technique for tracing digital cameras based on the study of vignetting and distortion faults, with a real-time picture processing algorithm. Their algorithm does not necessitate the use of a wavelet-based denoising filter or the calculation of camera fingerprints, both of which have a substantial impact on image processing speed. Rather, the technique extracts the red colour band from the input image and filters it using the median filter.

2.3 Colour Filter Array Interpolation

A demosaicing approach used in digital image processing called Colour Filter Array (CFA) interpolation, also known as colour reconstruction, reconstructs a full-colour image from the incomplete colour samples produced by an image sensor overlaid with a colour filter array. Using a predetermined CFA pattern this demosaicing information can be extracted and used as a camera fingerprint.

To identify the correlation structure that exists in each colour band and can be used for image classification, Bayram et al in [14] investigate the CFA interpolation procedure. The primary premise is that each manufacturer's interpolation algorithm and CFA filter pattern design are relatively unique from one another, and as a result, distinct correlation structures will be visible in the collected images. Two sets of characteristics are obtained for classification using the iterative Expectation Maximization (EM) algorithm. Lia & Lin [15] proposed a technique that uses an interpolation of images to figure out image characteristic values with a support vector machine to reduce computational time and achieve a high true positive. Chen & Stamm [16] proposed a technique that first re-samples the image colour components according to a predetermined CFA pattern, applies M different baseline demosaicing algorithms to re-demosaic missing colour components, and subtracts each re-demosaiced version from the original image to obtain M different sets of demosaiced residuals. Extract demosaicing information as co-occurrence matrices for each set of demosaicing residuals using K different geometric patterns. Then, perform multi-class ensemble classification on the feature space for camera source identification.

2.4 Learning-Based Techniques

Deep learning technology has been steadily incorporated into the field of image forensics with the advancement of artificial intelligence and the growth of available image datasets. Additionally, deep learning technology can extract the best features from a variety of training datasets, eliminating the drawbacks of features that were created artificially.

Ahmed et al [17] proposed a deep convolutional neural network for source camera identification method that uses a max pooling layer, three convolutional layers with batch normalization, rectified linear unit as an activation function, one fully connected layer, drop out layer, and classification layer as its first few layers. A small number of training images are used to train the network to identify the source of an image, and the noise pattern of the images is extracted using the same technique as described in [6]. Kirchner and Johnson in [18] proposed a technique that uses a Convolutional Neural Network (CNN) to train and estimate the camera signature and then extract the noise residual from the test images and use the Maximum Likelihood fingerprint Estimator (MLE) to estimate the fingerprint of the test images. Ding et al [19] proposed a technique which involves one pre-processing module, one feature extractor, and one hierarchical multi-task learning algorithm. The pre-processing module introduces domain information for the deep learning method of camera identification. Liu et al [20] proposed an efficient convolutional neural network-based source camera identification approach, consisting of three fundamental blocks: multiple-criteria-based patch selection, fine-grained multiscale residual prediction, and modified Visual Geometry Group (VGG) identification, arguing that traditional SCI performance is susceptible to image content and far from satisfactory for small image patches in real-world demanding applications.

3 Conclusion and Future Studies

This study investigated the performance of various well-known techniques for source camera identification for both intrinsic hardware artefacts-based techniques like sensor pattern noise (SPN), lens optical distortion and software artefacts-based techniques like CFA, with various authors using different or similar techniques. Findings show that while some techniques' performances are comparable other performances are wide apart. Sensor pattern noise generates the best performance result at camera level identification but with high computational cost. Lens optical distortion and deep learning techniques were all able to achieve camera-level identification, but SPN achieved higher accuracy. Colour filter array (CFA) equally does well but is able to achieve identification at the camera model level, which could not do well when you have sets of images from the same camera model. VISION image dataset and Dresden image datasets were widely used by the researchers using various assessment criteria like FAR/FRR Error Rate, ROC, TPR/FPR, FPR/FNR, Confusion Matrix, and RER.

For improvement in the accuracy of prediction of source camera identification at reduced computational time, this study recommends the exploration of the application of other transforms for image source camera identification.

Reference

[1] Y. Su, J. Zhang, and Z. Ji, "A Source Video Identification Algorithm Based on Features in Video Stream," *Int. Work. Educ. Technol. Train. 2008 Int. Work. Geosci. Remote Sens.*, pp. 719–723, 2009, doi: 10.1109/ETTandGRS.2008.325.

[2] S. Chen, A. Pande, K. Zeng, and P. Mohapatra, "Video Source identification in lossy wireless networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 1, pp. 28–39, 2015, doi: 10.1109/TIFS.2014.2362848.

[3] T. H. Thai, F. Retraint, and R. Cogranne, "Camera model identification based on the generalized noise model in natural images," *Digit. Signal Process. A Rev. J.*, vol. 48, pp. 285–297, 2016, doi: 10.1016/j.dsp.2015.10.002.

[4] K. S. Choi, E. Y. Lam, and K. K. Y. Wong, "Source camera identification using footprints from lens aberration," *Digit. Photogr. II*, vol. 6069, no. February, p. 60690J, 2006, doi: 10.1117/12.649775.

[5] J. Bernacki, "Digital camera identification based on analysis of optical defects," *Multimed. Tools Appl.*, pp. 2945–2963, 2019, doi: 10.1007/s11042-019-08182-z.

[6] J. Lukáˇ, J. Fridrich, and M. Goljan, "Digital Image Identification from Sensor Pattern Noise," *IEEE Trans. Inf. Forensics Secur. Forensics Secur.*, vol. 1, no. 2, pp. 205–214, 2006.

[7] A. R. Soobhany, A. S. Akbari, and Z. C. Schreuders, "Source Camera Identification using Non-decimated Wavelet Transform," *https://eprints.leedsbeckett.ac.uk/id/eprint/3155/*, pp. 125–133, 2017.

[8] M. Al-Athamneh, F. Kurugollu, D. Crookes, and M. Farid, "Digital Video Source Identification Based on Green-Channel Photo Response Non- Uniformity (G-PRNU)," *IEEE*, pp. 47–57, 2016.

[9] K. R. Akshatha, A. K. Karunakar, H. Anitha, U. Raghavendra, and D. Shetty, "Digital camera identification using PRNU: A feature-based approach," *Digit. Investig.*, vol. 19, pp. 69–77, 2016, doi: 10.1016/j.diin.2016.10.002.

[10] S. Georgievska, R. Bakhshi, A. Gavai, A. Sclocco, and B. Van Werkhoven, "Clustering Image Noise Patterns by Embedding and Visualization for Common Source Camera Detection," *Digit. Investig.*, 2017.

[11] B. Balamurugan, S. Maghilnan, and M. R. Kumar, "Source camera identification using SPN with PRNU estimation and enhancement," *Proc. 2017 Int. Conf. Intell. Comput. Control. I2C2 2017*, vol. 2018-Janua, pp. 1–6, 2018, doi: 10.1109/I2C2.2017.8321801.

[12] Y. Chen and V. L. L. Thing, "A Study on the Photo Response Non-Uniformity Noise Pattern based Image Forensics in Real-World Applications," *World Congr. Comput. Sci. Comput. Eng. Appl. Comput.*, 2012.

[13] K. S. Choi, E. Y. Lam, and K. K. Y. Wong, "Automatic source camera identification using the intrinsic lens radial distortion," *Opt. Express*, vol. 14, no.

24, p. 11551, 2006, doi: 10.1364/oe.14.011551.

[14] S. Bayram, H. T. Sencar, N. Memon, and I. Avcibas, “Source camera identification based on CFA interpolation,” in *IEEE International Conference on Image Processing 2005*, 2005, no. May 2014. doi: 10.1109/ICIP.2005.1530330.

[15] C. Lai and C. Lin, “Source Camera of Digital Image Identification base on Interpolation Algorithm,” *Dep. Appl. Informatics, Fo Guang Univ.*, vol. 55, no. 160, pp. 1886–1889, 2014, doi: 10.1049/cp.2012.1360.

[16] C. Chen and M. C. Stamm, “Robust camera model identification using demosaicing residual features,” *Multimed. Tools Appl.*, vol. 80, no. 8, pp. 11365–11393, 2021, doi: 10.1007/s11042-020-09011-4.

[17] F. Ahmed, F. Khelifi, A. Lawgalv, and A. Bouridane, “Comparative Analysis of a Deep Convolutional Neural Network for Source Camera Identification,” *Proc. 12th Int. Conf. Glob. Secur. Saf. Sustain. ICGS3 2019*, 2019, doi: 10.1109/ICGS3.2019.8688260.

[18] M. Kirchner and C. Johnson, “SPN-CNN: Boosting Sensor-Based Source Camera Attribution with Deep Learning,” 2019.

[19] X. Ding, Y. Chen, Z. Tang, and Y. Huang, “Camera Identification Based on Domain Knowledge-Driven Deep Multi-Task Learning,” *IEEE Access*, vol. 7, no. c, pp. 25878–25890, 2019, doi: 10.1109/ACCESS.2019.2897360.

[20] Y. Liu, Z. Zou, Y. Yang, N. F. B. Law, and A. A. Bharath, “Efficient source camera identification with diversity-enhanced patch selection and deep residual prediction,” *Sensors*, vol. 21, no. 14, pp. 1–22, 2021, doi: 10.3390/s21144701.

.