Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 7, July : 2023

USING MACHINE LEARNING FOR PARTICLE IDENTIFICATION IN FORENSIC SCANNER

SHAIK USMAN, MCA, DCA, DVR & Dr.Hima Shekar MIC College of Technology, A.P., India.
S.MOUNIKA, M.Tech, Associate Professor, Dept.of AI & IT, DVR & Dr.Hima Shekar MIC college of Technology, A.P., India.

***Abstract*—** image manipulation has become very easy. Hence, developing forensic tools to determine the origin or verify the authenticity of a digital image is important. Due to the increasing availability and functionality of image editing tools, many forensic techniques such as digital image authentication, source identification and tamper detection are important for forensic image analysis. In this paper, we describe a machine learning based system to address the forensic analysis of scanner devices. Our experimental results show that high accuracy can be achieved for source scanner identification. The proposed system can also generate a reliability map that indicates the manipulated regions in an scanned image.

INTRODUCTION

Hence, developing forensic tools to determine the origin or verify the authenticity of a digital image is important. These tools provide an indication as to whether an image is modified and the region where the modification has occurred. A number of methods have been developed for digital image forensics. For example, forensic tools have been developed to detect copy-move attacks [1], [2] and splicing attacks [3]. Methods are also able to identify the manipulated region regardless of the manipulation types [4], [5]. Other tools are able to identify the digital image capture device used to acquire the image [6], [7], [8], which can be a first step in many types of image forensics analysis. The capture of "real" digital images (not computer-generated images) can be roughly divided into two categories: digital cameras and scanners.

In this paper, we are interested in forensics analysis of images captured by scanners. Unlike camera images, scanned images usually contain additional features produced in the pre-scanning stage, such as noise patterns or artifacts generated by the devices producing the "hard-copy" image or document. These scannerindependent features increase the difficulty in scanner model identification. Many scanners also use 1D "line" sensors, which are different than the 2D "area" sensors used in cameras. Previous work in scanner classification

and scanned image forensics mainly focus on handcrafted feature extraction [9], [10], [11]. They extract features unrelated to image content, such as sensor pattern noise [9], dust and scratches [10]. In [12], Gou et al. extract statistical features from images and use principle component analysis (PCA) and support vector machine (SVM) to do scanner model identification. The goal is to classify an image based on scanner model rather than the exact instance of the image. In [9], linear discriminant analysis (LDA) and SVM are used with the features which describe the noise pattern of a scanned image to identify the scanner model. This method achieves high classification accuracy and is robust under various post-processing (e.g. , contrast stretching and sharpening). In [10], Dirik et al. propose to use the impurities (i.e. , dirt) on the scanner pane to identify the scanning device.

Convolutional neural networks (CNNs) such as VGG [13], ResNet [14], GoogleNet [15], and Xception [16] have produced state-of-art results in object classification on ImageNet [17]. CNNs have large learning capacities to "describe" imaging sensor characteristics by capturing low/median/high-level features of images [8]. For this reason, they have been used for camera model identification [8], [18] and have achieved state-of-art results.

In this paper, we propose a CNN-based system for scanner model identification. We will investigate the reduction of the network depth and number of parameters to account for small image patches (i.e. , 64 × 64 pixels) while keeping the time for training in a reasonable range. Inspired by [16], we propose a network that is light-weight and also combines the advantages of ResNet [14] and GoogleNet [15]. The proposed system can achieve a good classification accuracy and generate a reliability map (i.e. , a heat map, to indicate the suspected manipulated region).

LITERATURE REVIEW

M. Kharrazi et al. (2004). The interpolation in the color surface of an image due to the use of a color filter array (CFA) forms the basis of the paper. We propose to identify the source camera of an image based on traces of the proprietary interpolation algorithm deployed by a digital camera. For this purpose, a set of image characteristics are defined and then used in conjunction with a support vector machine based multi-class classifier to determine the originating digital camera. We also provide initial results on identifying source among two and three digital cameras.

Camera model identification with the use of deep convolutional neural networks

In this paper, we propose a camera model identification method based on deep convolutional neural networks (CNNs). Unlike traditional methods, CNNs can automatically and simultaneously extract features and learn to classify during the learning process. A layer of preprocessing is added to the CNN model, and consists of a high pass filter which is applied to the input image. Before feeding the CNN, we examined the CNN model with two types of residuals. The convolution and classification are then processed inside the network. The CNN outputs an identification score for each camera model. Experimental comparison with a classical two steps machine learning approach shows that the proposed method can achieve significant detection performance. The well known object recognition CNN models, AlexNet and GoogleNet, are also examined.

Digital camera identification from sensor pattern noise

In this paper, we propose a new method for the problem of digital camera identification from its images based on the sensor's pattern noise. For each camera under investigation, we first determine its reference pattern noise, which serves as a unique identification fingerprint. This is achieved by averaging the noise obtained from multiple images using a denoising filter. To identify the camera from a given image, we consider the reference pattern noise as a spread-spectrum watermark, whose presence in the image is established by using a correlation detector. Experiments on approximately 320 images taken with nine consumer digital cameras are used to estimate false alarm rates and false rejection rates. Additionally, we study how the error rates change with common image processing, such as JPEG compression or gamma correction.

RELATED WORK

TRAINING

A test image will first be split into sub-images, and then subsequently extracted into patches of size 64×64 pixels. The extracted patches will be used as inputs for the proposed neural network.

PRE-PROCESSING

This pre-processing enables the proposed system to work with small-size images and use smaller network architecture to save training time and memory usage. Designing suitable network architecture is an important part in the scanner model identification system.

TESTING

The same pre-processing procedure as described in the training section will be used in the testing stage. Our proposed system will evaluate two tasks on

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 7, July : 2023

scanned images: scanner model classification and reliability map generation. In Task 1 (scanner model classification), we assign the predicted scanner labels to both patches Ip and original images I. The predicted scanner label for the sub-image is the same as the predicted label of its corresponding patch. The classification decision for the original image I is obtained by majority voting over the decisions corresponding to its individual sub-images. In Task 2, a reliability map [19] is generated based on the majority vote result from Task 1. The pixel values in the reliability map indicate the probability of the corresponding pixel in the original image being correctly classified.

PROPOSED WORK

With powerful image editing tools such as Photoshop and GIMP being easily accessible, image manipulation has become very easy. Hence, developing forensic tools to determine the origin or verify the authenticity of a digital image is important. These tools provide an indication as to whether an image is modified and the region where the modification has occurred. A number of methods have been developed for digital image forensics. For example, forensic tools have been developed to detect copy-move attacks and splicing attacks.

DISADVANTAGES

- Less accuracy .

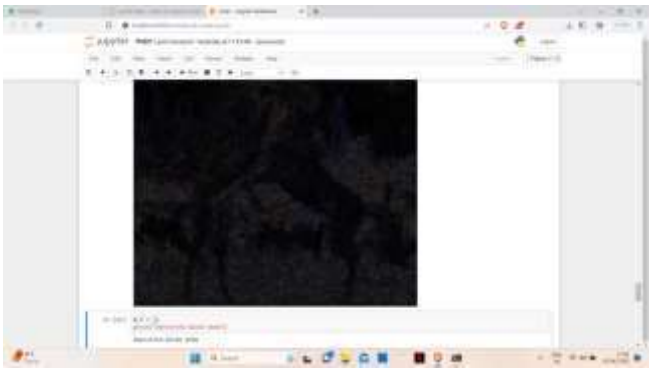
PROPOSED SYSTEM

The proposed system An input image is first split into smaller sub-images Is of size n ×m pixels. This is done for four reasons: a) to deal with large scanned images at native resolution, b) to take location independence into account, c) to enlarge the dataset, and d) to provide low pre-processing time

ADVANTAGES

More accurate

SAMPLE SCREENSHOTS



CONCLUSION

In this paper, we propose a new method for the problem of digital camera identification from its images based on the sensor's pattern noise. For each camera under investigation, we first determine its reference pattern noise, which serves as a unique identification fingerprint. This is achieved by averaging the noise obtained from multiple images using a denoising filter. To identify the camera from a given image, we consider the reference pattern noise as a spread-spectrum watermark, whose presence in the image is established by using a correlation detector.

REFERENCES

[1] A. J. Fridrich, B. D. Soukal, and A. J. Luka´s, "Detection of ˇ copy-move forgery in digital images," Proceedings of the Digital Forensic Research Workshop, August 2003, Cleveland, OH.

[2] Sevinc Bayram, Husrev Taha Sencar, and Nasir Memon, "An efficient and robust method for detecting copy-move forgery," Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing, pp. 1053–1056, April 2009, Taipei, Taiwan.

[3] Y. Q. Shi, C. Chen, and W. Chen, "A natural image model approach to splicing detection," Proceedings of the 9th workshop on Multimedia & Security, pp. 51–62, September 2007, Dallas, TX.

[4] A. C. Popescuand H. Farid, "Exposing digital forgeries in color filter array interpolated images," IEEE Transactions on Signal Processing, vol. 53, no. 10, pp. 3948–3959, October 2005.

[5] B. Bayar and M. C. Stamm, "A deep learning approach to universal image manipulation detection using a new convolutional layer," Proceedings of the 4th ACM Workshop on Information Hiding and Multimedia Security, pp. 5–10, June 2016, Vigo, Galicia, Spain.

[6] 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.

[7] S. Bayram, H. Sencar, N. Memon, and I. Avcibas, "Source camera identification based on cfa interpolation," Proceedings of the IEEE International Conference on Image Processing, pp. 69–72, September 2005, Genova, Italy.

[8] A. Tuama, F. Comb, and M. Chaumont, "Camera model identification with the use of deep convolutional neural networks," Proceedings of the IEEE International Workshop on Information Forensics and Security (WIFS), pp. 1–6, December 2016, Abu Dhabi, United Arab Emirates.

[9] N. Khanna, A. K. Mikkilineni, and E. J. Delp, "Scanner identification using feature-based processing and analysis," IEEE Transactions on Information Forensics and Security, vol. 4, no. 1, pp. 123–139, March 2009.

[10] A. E. Dirik, H. T. Sencar, and N. Memon, "Flatbed scanner identification based on dust and scratches over scanner platen," Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing, pp. 1385–1388, April 2009, Taipei, Taiwan.

[11] T. Gloe, E. Franz, and A. Winkler, "Forensics for flatbed scanners," Proceedings of the SPIE International Conference on Security, Steganography, and Watermarking of Multimedia Contents IX, p. 65051I, February 2007, San Jose, CA.

[12] H. Gou, A. Swaminathan, and M. Wu, "Robust scanner identification based on noise features scholar," Proceedings of the SPIE International Conference on Security, Steganography, and Watermarking of Multimedia Contents IX, p. 65050S, February 2007, San Jose, CA.

[13] K. Simonyan and A. Zisserman, "Very deep convolutional networks for large-scale image recognition," Proceedings of the International Conference on Learning Representations, May 2015, San Diego, CA.

[14] K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 770–778, June 2019.