A NOVEL APPROACH FOR USIND MACHINE LEARNING FORENSIC SCANNER IDENTIFICATION

G.A K N Venkata Sainadh, B. Kavyasri, G.Tejaswini Niveditha, CH. Kowshik, Student,Department of CSE, NRI INSTITUTE OF TECHNOLOGY, Vijayawada, A.P., India.

Mr.P.Narendra Babu, Assistant Professor, Department of CSE, NRI INSTITUTE OF TECHNOLOGY, Vijayawada, A.P., India.

ABSTRACT:

In this paper, we review recent work in media forensics for digital images, video, audio, and documents. The proposed system uses deep-learning to automatically learn the intrinsic features from various scanned images. 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. This study is the first to extract brightness variations as a unique characteristic of each scanner model and recognize the potential of brightness variations in source identification and manipulation detection

INTRODUCTION

In many cases the ability to determine the source of a digital image is important. This paper presents methods for authenticating images that have been acquired using flatbed desktop scanners. These methods use scanner fingerprints based on statistics of imaging sensor pattern noise. To capture different types of sensor noise, a denoising filterbank consisting four different denoising filters is used for obtaining the noise patterns. To identify the source scanner, a support vector machine (SVM) classifier based on these fingerprints is used. These features are shown to achieve a high classification accuracy. 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 scanner independent 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

DOI : 10.36893.DRSR.2022.V12I11N01.182-186

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.

EXISTING APPROACH

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

LITERATURE SURVEY

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 de-noising 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.

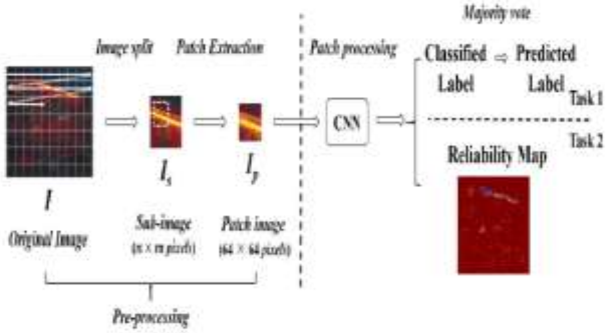
Source camera identification based on cfa interpolation

In this work, we focus our interest on blind source camera identification problem by extending our results in the direction of 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.

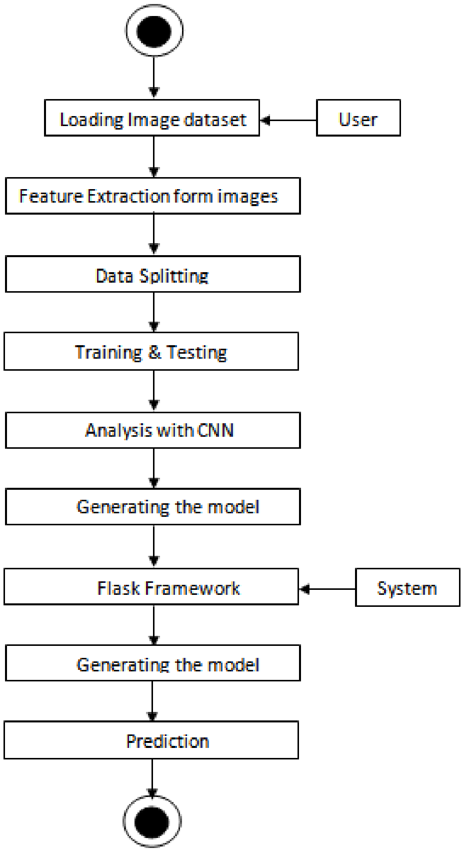
Camera model identification with the use of deep convolutional neural networks

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.

ARCHITECTURE



DOI : 10.36893.DRSR.2022.V12I11N01.182-186



SAMPLE RESULTS

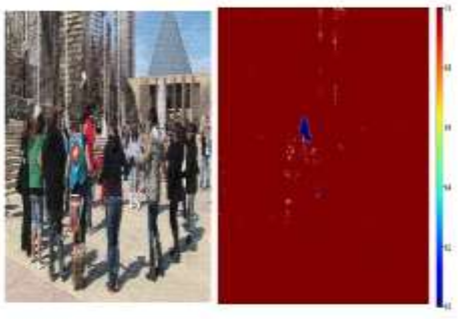


Figure 4: An original scanned image used for forged image creation

CONCLUSION

Proposed a classify an image based on scanner model rather than the exact instance of the image.

REFERENCES:

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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 2016, 06, pp. 365–372.

DOI : 10.36893.DRSR.2022.V12I11N01.182-186