International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

Forensic Scanner Identification Using Machine Learning

Rangumudri Harsha Vardhan Sai[1], Vitla Durga Prasad[2] ,Kalluri Sri Harsha[3], Attluri Uday kiran[4]

[1,2,3]B.Tech Student, Department of Computer Science and Engineering, CMR Technical Campus, Medchal, Hyderabad, Telangana, India.

[1]197r1a05g2@gmail.com, [2]197r1a05h8@gmail.com, [3]197r1a05e4@cmrtc.ac.in

[4]Assistant Professor, Department of Computer Science and Engineering, CMR Technical Campus, Medchal, Hyderabad Telangana, India,

[4]udaykiran.cse@cmrtc.ac.in

Abstract—Due to the increasing availability and functionality of image editing tools, Several forensic techniques, including digital image authentication and source identification, tamper detection are important for forensic image analysis. In this paper, we describe a system based on machine learning is proposed to tackle the forensic analysis of scanner devices. The system employs deep learning techniques to automatically acquire the intrinsic features from various scanned images The results of our experiments indicate that the system is capable of achieving high levels of accuracy when identifying the source scanner.. The proposed system can also generate a The proposed system can generate a reliability map, which highlights the regions in a scanned image suspected to be manipulated.

Keywords-scanner classification; machine learning; media forensics; convolutional neural network;

I. INTRODUCTION

With powerful image editing tools such as Photoshop and GIMP being easily accessible, image manipulation has become very easy. Therefore, the development of forensic tools to ascertain 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. New tools have been created for forensic purposes, specifically to identify instances of copy-move attacks [1], [2] and splicing attacks [3]. Methods are also able to identify the manipulated region the manipulation types [4], [5]. Additional tools can recognize the digital image capture device utilized to acquire the image. device used to acquire the image [6], [7], [8], which can be a first step in many types of image forensics analysis.There are two main methods for obtaining "real" digital images, excluding computer-generated ones, which are digital cameras and scanners.. In this study, our focus is on the forensic analysis of images that have been captured using scanners, which differs from the analysis of other types of digital images camera images, scanned images

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

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. 1D "line" sensors are commonly used in scanners, whereas cameras typically use 2D "area" sensors. Previous work in scanner classification and scanned image forensics mainly focuses on handcrafted feature extraction [9], [10], [11They capture features that are not related to the image content, such as the sensor pattern noise [9], dust, and scratches [10]. In [12], Gou et al. extract statistical features Images are analysed using principle component analysis (PCA) and support vector machine (SVM) to extract features and classify them.do scanner model identification. The goal is to classify an image based on the model focuses on the image's general characteristics rather than its specific instance. In [9], linear discriminant analysis (LDA) PCA and SVM are employed with noise pattern features to analyse scanned images. identify the scanner model. The proposed method demonstrates high accuracy in classification and shows robustness .Under different types of post-processing, such as contrast stretching and sharpening. In [10], Dirik et al. propose to use the impurities (i.e. The proposed method demonstrates high accuracy in classification and shows robustness.. Convolutional neural networks (CNNs) such as VGG [13], Res Net [14], Google Net [15], and Xception [16] have produced state-of-art results in object classification on ImageNet CNN's 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 introduce a system that utilizes CNNs to identify the model of a scanner. Model identification. We will investigate the reduction of the network depth and the 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 Res Net [14] and Google Net [15]. The system that we propose is capable of achieving high performance or accuracy. Accurately classifying and producing a map that indicates the level of reliability, also known as a reliability map. We incorporate a heat map into the system to demonstrate or indicate the suspected manipulated region).

II. PROPOSED SYSTEM

The proposed system is shown in Figure 1. An input image I 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,

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

c) to enlarge the dataset, and

d) to provide low pre-processing time and memory usage

A. Training As indicated in Figure 1, input image I is split into sub-images Is (n × m pixels) in zig-zag form. The values of n and m should be no smaller than 64. From each Is, a patch
of size 64 × 64 is extracted from a random location. We denote this extracted patch as Ip. The extracted patches, denoted as Ip, and their corresponding labels, denoted as S, serve as inputs to the network.. This pre-processing enables the proposed system to work with small-size images and use a smaller network architecture to save training time and memory usage. Designing

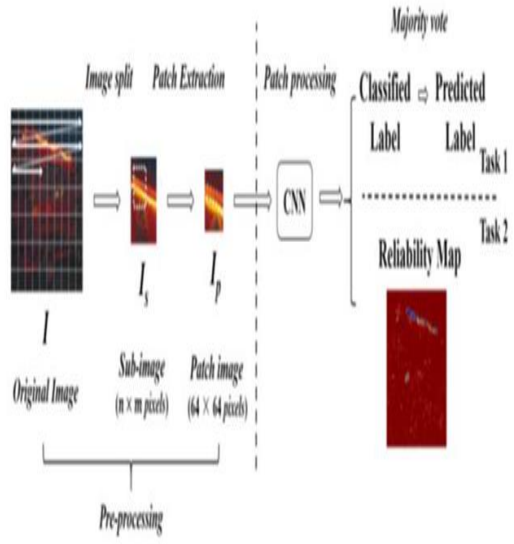

Figure 1

a suitable network architecture is an important part in the scanner model identification system. There are several factors that need to be considered to build the network: a) the kernel size,
the utilization of pooling layers, c) the depth of the network, and d) the implementation of the network modules. Our proposed network is shown in Figure 2. B. Testing The same pre-processing procedure as described in the training section will be used in the testing stage Initially, a test image will be divided into smaller sub-images, which will then be further divided into patches measuring 64x64 pixels each.. The extracted patches will be used as inputs for the proposed neural network. Figure 1 illustrates that the two tasks to be carried out on scanned images by our proposed system are the classification of scanner models and the generation of a reliability map.
For Task 1, which involves scanner model classification, the predicted scanner labels are assigned to both the patches, Ip, and the original images, I . In other words, the predicted label of a patch Ip is equivalent to the sub-image it represents.
b) The classification decision for the original image I is obtained by majority voting over the decisions corresponding to its individual sub-images Is. In Task 2, a reliability map [19] is generated based on the majority vote result from Task 1. The probability of a pixel being accurately classified in the original image is indicated by its corresponding value in the reliability map. To determine the probability of pixel x belonging to scanner s, the average value of probabilities for

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

the sub-images that contain the pixel is calculated.

x: Ps(x) = 1 n Xni=1 Ps(Subi) (1)

The equation represents that for a given pixel x, Subi denotes the sub-image that contains it, n is the total count of such sub-images, and Ps(·) represents the probability of an object belonging to scanner s.

III. THE EXPERIMENTS

In this section, we provide details of the dataset used in our experiments and the experiments conducted using the proposed system shown in Figure 1. We utilize the Dartmouth Scanner Dataset, which comprises 3,874 scanned images from 169 different scanner models in JPEG format. The original scanned images have varying sizes, ranging from 500 × 500 pixels to 5, 000 × 5, 000 pixels, and various scan resolutions (dpi - dots per inch). We partition the images into training, validation, and testing subsets for each scanner model. We create a sub-dataset with 10 randomly selected scanners, called the "10-scanner dataset," to evaluate the proposed system's performance. Additionally, we construct several forged images using copy-move attacks to evaluate the reliability maps.

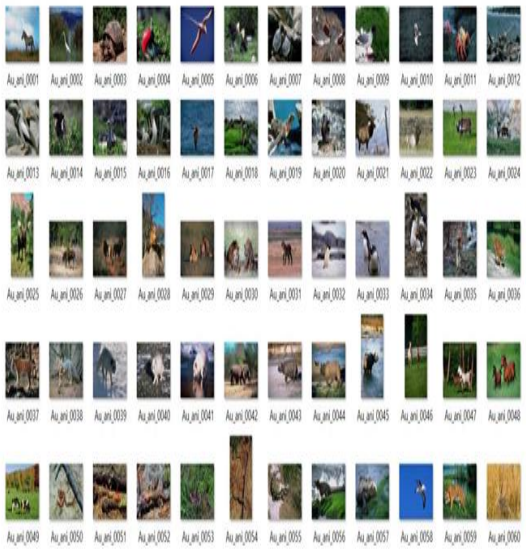

Figure 2 : dataset

B. Experimental Results

For Task 1, we implement a neural network in Pytorch using SGD with learning rate 0.01, momentum 0.5, and weight decay 0.0001 for scanner model classification. We compare our method with other CNN architectures such as InceptionV3, Resnet34, and Xception. The results of the experiments are reported in Table I and Figure 3, showing that our proposed method achieves high accuracy on patch-level and image-level classification tasks, with fewer parameters and a shallower model compared to other CNN architectures.

For Task 2, we investigate the generation of reliability maps that can indicate suspicious forged areas in the images. The reliability map is generated based on the predicted label obtained by majority vote, as explained in equation 1. We demonstrate the effectiveness of our reliability maps in identifying manipulated regions in the images, irrespective of the image content, using

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

copy-move attacks. The results are presented in Figure 4 and 5, indicating that our reliability maps can effectively detect suspicious forgery.

IV. CONCLUSION

This paper explores the potential of deep-learning methods for scanner modelclassification
and localization, highlighting several advantages over classical methods, such as automatic learning of intrinsic scanner features, no restrictions on data collection, high accuracy in associating small image patches (64x64 pixels) with scanner models, and the ability to detect image forgery and localization on small image sizes. Our experimental results, as presented in Table I, demonstrate the effectiveness of our proposed system in differentiating scanner models and its robustness to JPEG compression. Additionally, our results in Figure 5 demonstrate the system's ability to detect suspected forged regions in scanned images through the use of our reliability map. Future work will focus on improving the neural network architecture, detecting other types of forgeries, and evaluating the system's performance on scanned documents.

Figure 3 : Result

V. ACKNOWLEDGMENTS

We thank CMR Technical Campus for supporting this paper titled " Forensic Scanner Identification Using Machine Learning", which provided good facilities and support to accomplish our work. Sincerely thank our Chairman, Director, Deans, Head Of the Department, Department Of Computer Science and Engineering, Guide and Teaching and Non- Teaching faculty members for giving valuable suggestions and guidance in every aspect of our work

VI. 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.

[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 2016, Las Vegas, NV.

[15] C. Szegedy, W. Liu, Y. Jia, P. Sermanet, S. Reed, D. Anguelov, D. Erhan, V. Vanhoucke, and A. Rabinovich, "Going deeper with convolutions," Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 1–9, June 2015, Boston, MA. [16] F. Chollet, "Xception: Deep learning with depthwise separable convolutions," Proceedings of the IEEE Conference on Computer Vision and

Pattern Recognition, pp. 1800–1807, July 2017, Honolulu, HI.

[17] J. Deng, W. Dong, R. Socher, L.-J. Li, K. Li, and L. FeiFei, "Imagenet: A large-scale hierarchical image database," Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 248–255, JUne 2009, Miami Beach, FL.

[18] L. Bondi, L. Baroffio, D. Guera, P. Bestagini, E. J. Delp, and ¨ S. Tubaro, "First steps toward camera model identification with convolutional neural networks," IEEE Signal Processing Letters, vol. 24, no. 3, pp. 259–263, March 2017.

Vegas, N

[19] B. Zhou, A. Khosla, Lapedriza. A., A. Oliva, and A. Torralba, "Learning deep features for discriminative localization," Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 2921–2929, June, Las Vegas, NV.

[20] C. Szegedy, V. Vanhoucke, S. Ioffe, J. Shlens, and Z. Wojna, "Rethinking the inception architecture for computer vision," Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 2818–2826, June 2016, Las