IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Automated Forensic Analysis Of Scanned Images Via Ela And Cnns

[1]Boddeti Nagendra Kumar, Student in Dept. Of Master of Computer Applications, at Miracle Educational Society Group of Institutions

[2]Mr. N Mahendra, Associate Professor at Miracle Educational Society Group of Institutions

[3]Maradana Siva, Assistant Professor at Miracle Educational Society Group of Institutions

ABSTRACT

The focus of this work relates to the identification and tampering detection of forensic scanners through deep neural production techniques. Tools built on convolution neural networks (CNNs) and the CASIA dataset are employed to determine which type of scanner was used to create an image and locate portions that were edited. Among others, processes involve transforming the photographs into error level analysis (ELA) images in order to accentuate the inconsistencies and training a CNN in a procedure where the CNN architecture is optimized. The system achieves promising levels of performance and is thus appropriate for distinguishing between images that are or are not altered. As demonstrated by the series of experiments, the model was able to withstand different circumstances and enabled accuracy of over 82% during validation. This work has a considerable contribution to automated media forensics since it solves the problem of scanner identification and digital manipulation detection in an effective and scalable manner.

Keywords: CNN, ELA, SCANNER

INTRODUCTION:

The image has become an edited artifact and as such necessitates the need for qualifiers such as deep fake forensics in order to determine how real or fake an image is. It is worth noting that the digitization of images coupled with edited has changes the dynamics of user engagements and interactions. The challenges posed by copy move and splicing attacks are being worked on as has been in numerous studies aimed at addressing the issues of digital image editing and manipulation. It has also meant that different types of devices for example cameras, phones and scanners, are found to have their own unique traits and characteristics. Different spatial image characteristics will be presented depending on the cylinder rotation of the camera or the tip of the line sensors rotating on the flatbed scanner. Older algorithms would be very effective at Oil Painting Effective Foreground Segmentation while clearly lacking in depth learning aspects of the analysis. Newer algorithms based on Artificial Neural Networks are superior in terms of control mechanisms especially when dealing with 3D volumetric imaged data by truely understanding the source geometry during the scanning process with thorough image reconstruction during the processing phase.

GAP IDENTIFIED BASED ON LITERATURE SURVEY:

In the world of papers, it is easy to spot forgeries; however, within the domain of images, it is easier to spot them by the use of different types of scanners. Scanner forensic still needs to be explored. Most of the past research make use of old features and algorithms, this implies that machine intelligence is not effectively used for the sophisticated non printer scanner artifacts and artifacts on images.

Key Gaps:

1. Dataset Size Recursiveness: Those datasets are small or particular, it is clear that there will be limitations when scaling it to other scanner models or other scanner resolutions in the future due to lack of variation.
2. Boundary conditions on feature extraction: Normalized noise on the scanner lacks a bypass feature that may be useful because each feature will be compromised.
3. Minimal use of deep learning: Only a few studies focused on what was required for the purpose and potential of using CNN's for code detection.
4. Code Detection restrictions: Present codes do not allow locating offensive areas, instead only classification is available.
5. Cost returns Management: Considerable time is expended in the application of the deep model code.
6. Security Requirements: On compression and resizing of present images, A model recognizing those images will fail as for which it was trained.

Gaps are filled by relying on classification for recognition and tamper identification through CNN integrating ELA based on large variety of datasets such as CASIA.

PROBLEM STATEMENT:

With the rise of digital manipulation, there is a pressing need for systems that quickly point out tampered images and their sources. Scanner forensics, which is a less tapped area, needs sophisticated techniques to reasonably classify the scanner models and also check for any modifications.

Key Challenges:

1. High level of Complexity in Artifacts: The distinguishing of editing artifacts from the scanner specific features distinctively requires a scratch analysis. 2. Dataset Influence: Cross matching of model depicted and the various samples taken from diverse scanners and resolutions is a crucial part. 3. Timeliness Efficiency: Efficient timing practically applies when there is proper speed as well as accuracy.

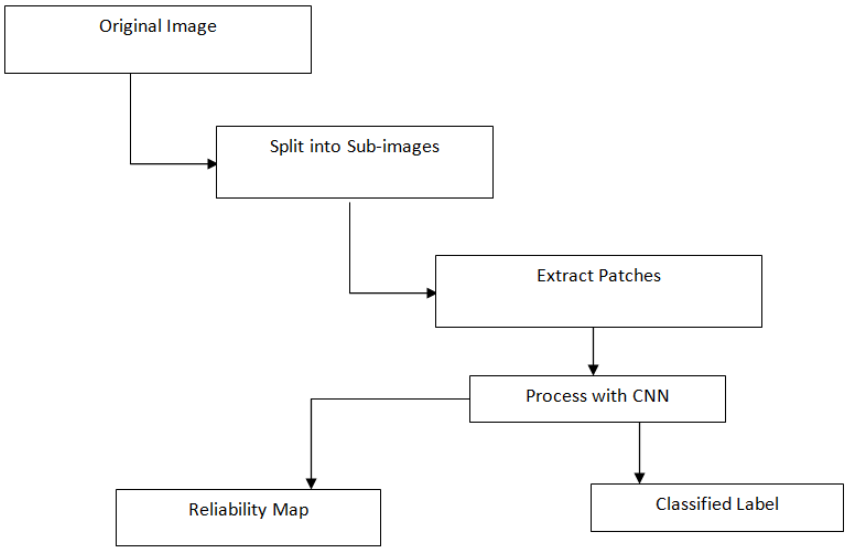
2. Forgery Localization: There remains the issue of precisely identifying the altered parts in a scanned image.

3. Automation: Decreasing the use of manual feature engineering but not affecting the output quality.

PROPOSED METHOD:

This study presents a tampering detection and scanner identification CNN-based system. It uses ELA for image preprocessing aimed at removing artifacts caused by compression or distortion. After that, resized copies of the images are passed through a CNN built with convolutional, dropout and dense layers to improve feature extraction. The CASIA database are partitioned into the training and validation subsets for performance evaluation. The model demonstrates useful accuracy in classifying an image either as original or altered. Further evaluations are carried such as confusion matrix and precision-recall scores, to evaluate the model's effectiveness. It puts forward a cost effective system for scanner and forgery detection.

ARCHITECTURE:



The process initiates with a singular original picture which is then divided into smaller images comprising n x m pixel dimensions. These minor images are then split further into patches of 64 by 64 pixels. The Convolutional Neural Network (CNN) model takes this sub images as inputs and sorts them into their respective labels. The classified labels then go through a series of majority votes to derive a conclusive label (Task 1). Furthermore, essential task two, which requires the development of a reability map, is accomplished by specifying the degree of confidence for classification purposes. This is of great importance especially when one is dealing with complexities involving images as classification accurate is of great importance.

CASIA DATASET:

The dataset has two subsets which are purchased together with the final output which is the casia1 and the casia 2. This dataset which is also used in this research contains images which are labelled original or tampered with the alterations being for example copy paste and also object erasures. The dataset contains several types of images with varying sizes and formats in order to facilitate multiple training. Each of the images is subject to preprocessing which is done by Elstic Laer Abssorptiom (ELA) techniques in order to aid in the areas of interest. In particular, CASIA2 is the most the most increased with more than 3000 images which were marked for binary classification. The much appealing feature of the dataset is its variability to models which enhances both training and validation to achieve good accuracy in the identification of the scanner and detection of forgery tasks.

METHODOLOGY:

Dataset Preparation:

Utilising images from the tampered casia1 and casia2 dataset for images which are original.

Split the dataset into test and training set which consist of 80-20% ratio respectively.

Image Preprocessing:

First, apply ELA format to the images to detect any evidence of compression or editing.

Then, resize all images to a resolution of 60×6060 \times 60 60×60 to standardize the input dimensions.

Model Design:

Use the following components to construct the layers of the model:

First add two convolutional layers (filter size: 5×55 \times 55×5) for feature extraction followed by Max-pooling layers to down-sample the input feature maps, and then add the Dropout layers (25% and 50%) for regularization. Add Dense layers for the decision making with ReLU and softmax functions.

Training and Validation:

Train the model by using the adamhr m optimizer with categorical cross entropy loss (CELoss) through SGD.

Assess the performance in terms of accuracy and loss rates on validation data after 5 epochs.

Model Evaluation:

Use confusion matrices and precision, recall, F1 score, and other metrics to appraise the model.

Test the tampering robustness of images having manipulations like copy paste and image paste.

Forgery Localization:

Utilize ELA preprocessing to help establish which regions have been tampered with on the images.

Use model's outputs to validate that tampering has occurred and what it is.

Implementation and Automation:

Utilize Python, Keras, PIL and Matplotlib libraries to do the preprocessing, training and evaluation without manual interaction.

Keep the trained models for further use in real world applications.

EVALUATION:

Precision:

$$\text{Formula: Precision} = \frac{\text{True Positives}}{\text{True Positives} + \text{False Positives}}$$

Recall (Sensitivity):

$$\text{Formula: Recall} = \frac{\text{True Positives}}{\text{True Positives+False Negatives}}$$

F1 Score:

$$\text{Formula: } F1 = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision+Recall}}$$

Accuracy:

$$\text{Formula: Accuracy} = \frac{\text{Correct Predictions}}{\text{Total Predictions}}$$

RESULTS:

Prediction with the Model for the input Image

Predicting the class of uploaded image

Model	Accuracy (Per Image)	Accuracy (Per Patch)	Precision	Recall	F1 Score
Proposed CNN	82.97%	84.49%	83.17%	82.97%	83.03%

Accuracy Comparison

CONCLUSION

This is a powerful CNN architecture for forensic scanner recognition and even forgery detection. By embedding ELA preprocessing, the system detects alterations and specific classes of scanners as well. Evaluations on the CASIA dataset show that it is robust and achieves a validation accuracy of more than 82%. It shows quite good results and addresses some of the main problems faced in the area of scanner forensics. Modeling a deep learning approach combined with some practical pre-processing techniques seems to solve important issues encoder. Future modeling will aim at enhancing model extensibility, expanding the scope of applications to multiclass classifications, and advanced forgery detection methods. This form of research paves the way for autonomous and effective scanning forensics in a world that is fully submerged with altered materials.

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 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.

[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 Vegas, NV.