International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 06 | June - 2023 SJIF Rating: 8.176 ISSN: 2582-3930

Image Forgery Detection using Deep Learning

Aishwarya Sedamkar[1], Sachin Deshpande[2]

[1] PG Student, Department of Computer Engineering, Vidyalankar Institute of Technology
[2]Professor, Department of Computer Engineering, Vidyalankar Institute of Technology

---

Abstract - Undoubtedly one of the most active study areas in the field of blind image forensics is copy-move forgery detection (CMFD). The majority of known algorithms rely on block and key-point approaches, alone or in combination. Deep convolutional neural network techniques have recently been used in picture classification, image forensics, image hashing retrieval, and other areas. These techniques have outperformed more conventional techniques in these areas. The work makes a novel convolutional neural network-based copy-move forgery detection algorithm suggestion. The suggested method makes minor adjustments to the net structure using small training samples after using an existing trained model from a sizable database like ImageNet. Results from the experiments demonstrate that the method we suggested produces a forgery image created automatically by computer with a simple copy-move operation in a satisfactory manner.

In order to automatically build hierarchical representations from the input RGB color photographs, this system proposes a new image fraud detection strategy based on deep learning that makes use of a convolutional neural network (ELA CNN) and transfer learning model. Image splicing and copy-move detection applications are the focus of the proposed ELA CNN and transfer learning methodology. The basic high-pass filter set used in the calculation of residual maps in the spatial rich model (SRM), which serves as a regularizer to effectively suppress the effect of image contents and capture the subtle artifacts introduced by the tampering operations, is initialized with the weights at the first layer of our network rather than using a random strategy. In order to extract dense features from the test images, a pre-trained model like Vgg, Densenet, or ELA CNN is used as a patch descriptor. A feature fusion strategy is then investigated in order to produce the final discriminative features for SVM classification.

Digital forensics research on forgery detection and localisation is important and has recently received more attention. Traditional approaches typically rely on manually created or shallowly learned features, but these have poor description capabilities and high computational costs. Deep neural networks have recently demonstrated their ability to efficiently learn the hierarchical representations of complicated statistical data from high-dimensional inputs. In this paper, we propose an improved mask regional convolutional neural network (Mask R-ELA CNN) that adds a Sobel filter to the mask branch in order to capture more distinguishing features between tempered and non-tempered areas. As a support job, the Sobel filter encourages predicted masks to have picture gradients that are close to those of the ground truth mask.The whole network is capable of spotting copy-move and splicing, two different types of image modification. The suggested model outperforms the current conventional methods for forgery detection, according to experimental results utilising two standard datasets (Casia) and ELA CNN.

***Key Words*:** forgery detection, forensic, image processing, ELA CNN, VGG, DenseNet

1. INTRODUCTION

With the rapid advancement of digital image processing technology and the widespread use of digital cameras, modifying or tampering with a digital image is now much simpler, even for a novice forger, thanks to applications like Adobe Photoshop. Splicing and copy-move are two of the most popular digital forgery tools that manipulate the images in a way that is difficult for the human perceptual system to detect. Over the past few decades, doctored photographs have become more common and sophisticated. Therefore, it is crucial for digital picture forensics to effectively detect these two types of forgeries.

The most frequent kind of tampering is copy-move forgery, which involves copying a portion of a picture and then pasting it into another portion of the same image. One of the most popular areas of research in blind image forensics is copy-move forgery detection (CMFD). The literature contains reports of several different CMFD techniques. They can be broadly categorized into two classes: block-based methods and key-point based approaches. The first category methods frequently use the techniques of scale-invariant feature transform (SIFT) and accelerated robust feature (SURF). From the entire image, essential point features are initially extracted. The next step is to compare each key point to each of these qualities in order to identify a similar point. If a clustering zone produced by matching pairings with the same affine transformation is sizable enough, a counterfeit region may be recognised. In addition to effectively locating

duplicated regions, key-point-based algorithms also perform well when dealing with geometric distortions like rotation, scaling, and translation. The disadvantage of keypoint-based approaches is that it can be challenging to find repeated regions with weak visual structures or key-points. The image is divided into overlapping blocks using block-based algorithms, which then extract some features from each block and search for matching block features. If there are enough matching pairings that share the same "shift vector" to reach a predetermined number, such matching pairs are taken into account to be a part of duplicated areas.

2. Proposed Technique

The CASIA v1.0 dataset includes 1,725 color images with a size of 384 x 256 pixels in JPEG format, 925 of which are forged images generated by pasting sections of cropped photos that have been rotated, resized, or otherwise altered. It is more difficult to implement post-processing on the boundary area of tampered regions in the CASIA v2.0 database. It includes 7,491 real and 5,123 fake color images in JPEG, BMP, and TIFF formats, with sizes ranging from 240 by 160 to 900 by 600 pixels. Splicing and copy-move forged pictures are present in both CASIA v1.0 and v2.0.

Steps -

1. Data Collection from kaggle
2. Importing required libraries .
3. Dataset loading .
4. Data Cleaning
5. Data Preprocessing:- Applying ELA, Labeling data , and label encoding etc.
6. Data Visualization
7. Splitting data into train, test with different ratio
8. Training model
9. Model evaluation

List of Models -

1. ELA CNN (Error Level Analysis CNN)
2. VGG
3. DENSENET

Model Evaluation Techniques -

1. Confusion matrix
2. Classification report

3. Design Methodology

The training data set is provided to the classifier as input. This classified data is also used for the purpose of testing. We used the ELA CNN algorithm.
The system will operate mainly in two stages:

1. Training phase
2. Testing phase

Training Phase - Classification assumes labeled data: we know how many classes there are, and for each class we have examples (labeled data).
Testing Phase - Testing phase involves the prediction of unknown data samples.

4. Performance Evaluation Metrics

Based on values from the confusion matrix and the classification report, assessment metrics are used to gauge how well machine learning can classify images. This is a two-dimensional matrix that details the real and anticipated category.

1. Confusion matrix
2. Classification Report

False alarm rate: It's also known as the false positive, and it's characterized as the ratio of incorrectly predicted Attack samples to all Normal samples.
True negative rate: It's the number of correctly labeled Normal samples divided by the total number of samples that are Normal.
Precision: It's the ratio of correctly expected Attacks to all Attacks samples.
Recall: It's the proportion of all Attacks samples correctly listed to all Attacks samples that are actually Attacks. It's also known as a Detection Rate.
F-Measure: Precision and Recall are combined to form the harmonic mean. To put it another way, it's a mathematical method for evaluating a system's accuracy by taking into account both precision and recall .

5. Results & Discussion

Following is a summary of the main contributions made as part of the discussion based on the findings: (1) Using labeled patches (p*p) from the training images, we first trained a supervised ELA CNN to learn the hierarchical aspects of tampering operations (splicing and copy-move). The ELA CNN's initial convolutional layer functions as a pre-processing module to effectively muffle the impact of the image contents. In order to boost generalization ability and hasten network convergence, the first layer's kernel weights are initialized using the 30 fundamental high-pass filters used in the computation of residual maps in the spatial rich model (SRM). (2) After scanning the entire image with a patch-sized sliding window, we could then extract the features for an image using the ELA CNN based on the p*p patch. The final discriminative feature is then obtained by condensing the produced image representation using a straightforward

feature fusion approach called regional pooling. (3) After that, an SVM classifier is trained for binary classification (authentic/forged) using the output feature representation.

The representation for Loss and Accuracy is shown in Fig 5.1 and 5.3 for DenseNet and VGG respectively. According to Fig 5.5, loss is minimum and accuracy is maximum in the ELA CNN algorithm. Further, the confusion matrix in Fig 5.6 shows the better true negative values over DenseNet and VGG Algorithm which is shown in Fig 5.2 and 5.4.

Training using DenseNet

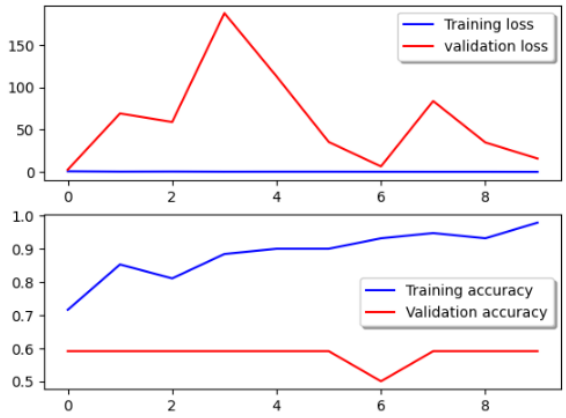

Fig 5.1 Loss and Accuracy Graph for DenseNet

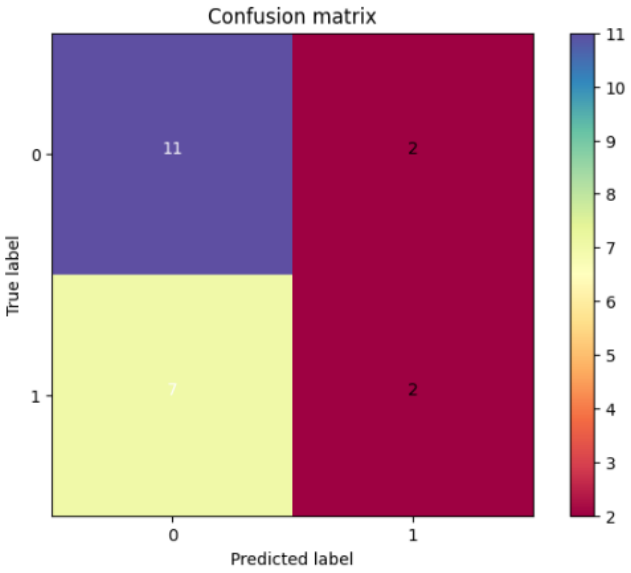

Fig 5.2 Confusion Matrix for DenseNet

Training using VGG

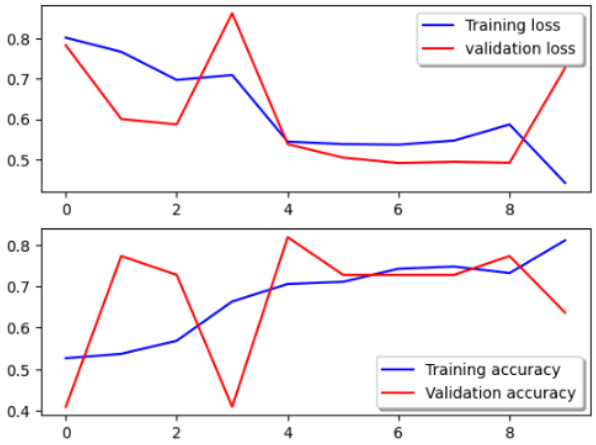

Fig 5.3 Loss and Accuracy Graph for VGG

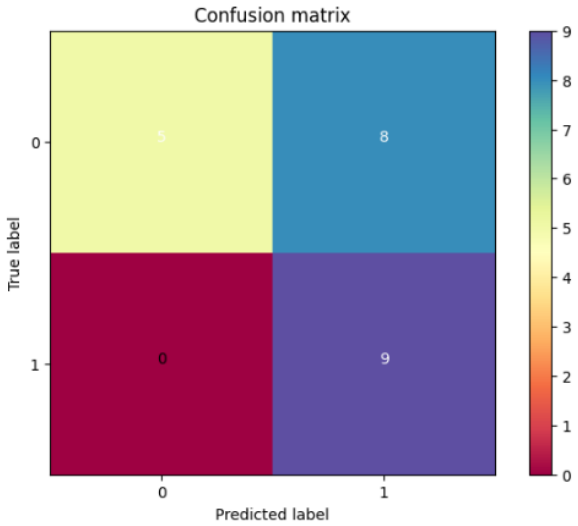

Fig 5.4 Confusion Matrix for VGG

Training using ELA CNN

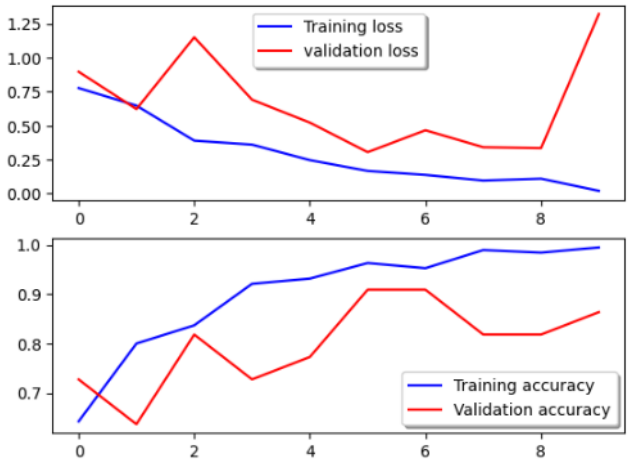

Fig 5.5 Loss and Accuracy Graph for ELA CNN

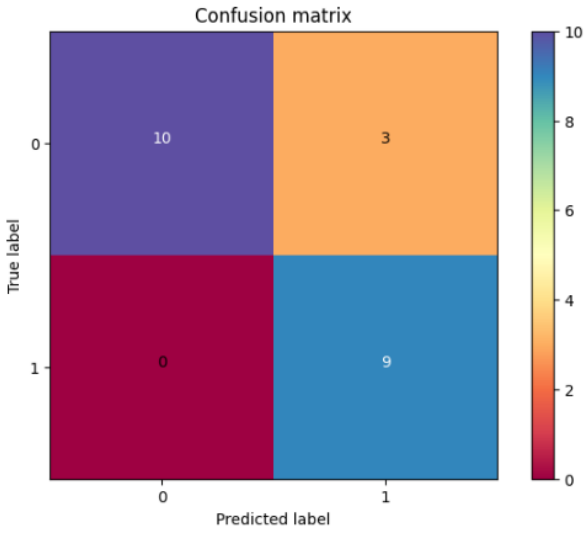

Fig 5.6 Confusion Matrix for ELA CNN

Therefore, based on the results that are graphically represented above, it is very evident that the ELA CNN algorithm shows better performance on some specific performance parameters.

6. CONCLUSIONS

In this system, we suggest a brand-new method for detecting picture forgeries that is based on transfer learning and deep convolutional neural networks (ELA CNN). The planned ELA CNN features several tailored designs for applications that detect picture manipulation. In order to effectively suppress the effect of complex image contents and hasten network convergence, the weights at the first layer of our network are initialized with the 30 fundamental high-pass filters used in the spatial rich model (SRM) for image steganalysis. In our approach, a local patch descriptor is created using an ELA CNN model that has been pre-trained using labeled patch samples that have been painstakingly drawn along fabricated boundaries in altered images. The test images are then processed by the ELA CNN to extract dense features, and a feature fusion approach is added to provide the final discriminative features for classification. The suggested ELA CNN-based technique performs better than existing conventional image forgery detection algorithms, as shown by extensive trials on a number of public datasets.

ACKNOWLEDGEMENT

I wholeheartedly thank my guide Prof. Dr. Sachin Deshpande and the HOD Prof. Dr. Sachin Bojewar for constant encouragement and support for completing my work. I thank the Department of Computer Engineering at Vidyalankar Institute of Technology, Mumbai for the research facilities and learning environment provided which lead to this development of study.

REFERENCES

[1] X. Pan and S. Lyu, "Region duplication detection using image feature matching," IEEE Transactions on Information Forensics and Security, vol. 5, no.4, pp. 857-867, 2010.

[2] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo and G. Serra, "A sift-based forensic method for copy–move attack detection and transformation recovery," IEEE Transactions on Information Forensics and Security, vol. 6, no. 3, pp. 1099- 1110, 2011.

[3] S.-J. Ryu, M.-J. Lee and H.-K. Lee, "Detection of copy rotate- move forgery using Zernike moments," in Proc. Information Hiding Conference, 2010.

[4] H.-J. Lin, C.-W. Wang and Y.-T. Kao,"Fast copy-move forgery detection," WSEAS Transactions on Signal Processing, vol. 5, no. 5, pp. 188-1975, 2009.

[5] V. Christlein, C. Riess, J. Jordan and E. Angelopoulou, "An evaluation of popular copy-move forgery detection approaches", IEEE Transactions on Information Forensics and Security, vol. 7, no. 6, pp. 1841-1854, 2012.

[6] J. L. Ouyang, J. Wu, G. Coatrieux , Z. Shao, , H.Z. Shu. "A robust copy-scale-move forgery detection method based on pyramid model", Journal of southeast university (Natural science edition), vol. 45, no. 06, pp.1116-1120, 2014.

[7] C.-S. Park, C. Kim, J. Lee, and G.-R. Kwon, “Rotation and scale invariant upsampled log-polar fourier descriptor for copy-move forgery detection,” Multimedia Tools and Applications, pp. 1-19, 2016.

[8] J. Zheng, Y. Liu, J. Ren, T. Zhu, Y. Yan, and H. Yang, “Fusion of block and keypoints based approaches for effective copy-move image forgery detection,” Multidimensional Systems and Signal Processing, pp. 1-17, 2016.

[9] X. Bi, C.-M. Pun, and X.-C. Yuan, “Multi-Level Dense Descriptor and Hierarchical Feature Matching for Copy–Move Forgery Detection,” Information Sciences, vol. 345, pp. 226- 242, 2016.

[10] X. Wang, G. He, C. Tang, Y. Han, and S. Wang, “Keypoints-Based Image Passive Forensics Method for Copy- Move Attacks,” International Journal of Pattern Recognition and Artificial Intelligence, vol. 30, no. 03, pp. 1655008, 2016.

[11] J. Li, X. Li, B. Yang, and X. Sun, "Segmentation-based image copy-move forgery detection scheme," IEEE Transactions on Information Forensics and Security, vol. 10, no. 3, pp. 507-518, 2015.

[12] M. Zandi, A. Mahmoudi-Aznaveh, and A. Talebpour, "Iterative copy-move forgery detection based on a new interest point detector," IEEE Transactions on Information Forensics and Security, vol. 11, no. 11, pp. 2499-2512, 2016.

[13] C.-M. Pun, X.-C. Yuan, and X.-L. Bi, "Image forgery detection using adaptive over segmentation and feature point matching," IEEE Transactions on Information Forensics and Security, vol. 10, no. 8, pp. 1705-1716, 2015.