Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 5, No.4, May : 2024

IMAGE FORGERY DETECTION BASED ON FUSION OF LIGHTWEIGHT DEEP LEARNING MODELS

Sireesha K (Faculty Guide), Depart. of Computer Science and Engineering, Andhra Loyola Institute of Engineering and Technology, Vijayawada, Andhra Pradesh, India sireeshakcs@aliet.ac.in
Sai Manoj Balasani, Depart. of Computer Science and Engineering, Andhra Loyola Institute of Engineering and Technology, Vijayawada, Andhra Pradesh, India saimanojbalasani4@gmail.com
Rahul Kommuri, Depart. of Computer Science and Engineering, Andhra Loyola Institute of Engineering and Technology,Vijayawada, Andhra Pradesh, India rahulkommuri7545@gmail.com
Anil Kumar Ontipuli, Depart. of Computer Science and Engineering, Andhra Loyola Institute of Engineering and Technology,Vijayawada, Andhra Pradesh, India anilkumarontipuli83@gmail.com

Abstract –
The ubiquity of cameras has fueled the popularity of photography, but it has also led to a surge in manipulated images, raising concerns about the prevalence and impact of photo forgeries. Convolutional neural networks (CNNs) have emerged as promising tools for detecting fake images, yet their performance has been inconsistent. To address this, we propose a method that evaluates original and compressed image versions, achieving a remarkable validation accuracy of 92.23%, surpassing industry standards. Our approach offers a swift and accurate solution to identify concealed forgeries, mitigating the spread of misinformation in photographs.

Keywords – Image forgery detection, Deep learning models, Lightweight models, Fusion techniques, Convolutional Neural Networks.

I. INTRODUCTION

Sales of digital cameras have increased dramatically as a result of the accessibility and affordability of electronic gadgets, which are fuelled by globalization and technical advancement. Because cameras are so widely available, a huge number of photos are taken every day, posted on social media, and utilized for online filings, which helps those who struggle with reading comprehend. Images are important on the internet because they help spread knowledge and document history. The widespread availability of photo editing software has made it possible for people to alter images, while some have taken advantage of this to disseminate false information, making it extremely difficult to undo the harm that has resulted.

The widespread use of Photoshopped images has damaged public confidence in visual media since distorted images spread misleading information. Photos that were formerly trusted sources are now regularly altered to trick. As a result, people are becoming more skeptical of photographic evidence because most people find it difficult to identify forgeries. It is critical to have techniques for identifying fake images in order to stop the spread of false information and restore confidence in visual media. Using different image processing techniques can reveal manipulation evidence, giving rise to a way to recognize bogus material and rebuild trust in photographic proof.

Scholars have put forth a number of methods for identifying manipulated photographs, including examining artifacts caused by changes in lighting and compression. Because Convolutional Neural Networks (CNNs) can recognize segments and objects, they are being employed more and more in computer vision applications. CNNs are able to identify image modifications by generalizing learned attributes through feature mapping, which makes use of shared weights and neighbourhood connections. In order to particularly learn artifacts in tampered images produced by disparities between original and altered areas, a lightweight CNN has been implemented.

II. LITERATURE REVIEW

Various techniques for detecting image manipulation are discussed, including Error Level Analysis (ELA), contourlet transform, and analysis of JPEG compression artifacts. CNNs, like the method proposed by Yang et al., employ two concatenated CNNs to extract discrepancies between original and spliced areas. Other approaches, such as ringed residual U-Net and reliability fusion maps, focus on detecting splicing and identifying fake images. Additionally, methods for detecting manipulated photos involve combining resampling characteristics with deep learning and clustering camera-based CNN features. Techniques like DOA-GAN and ManTra-Net further enhance detection capabilities by incorporating dual attention mechanisms. Moreover, researchers have explored the fusion of Zernike moments with SIFT characteristics for image recovery and detection.

III. EXITING SYSTEM

We assessed the efficacy of our suggested approach with the popular CASIA 2.0 image forgeries database [22, 49]. 12,614 BMP, JPG, and TIF photos total—7,491 real and 5,123 fake—are included in this database. Images of landscapes, textures, and interiors are all included in CASIA 2.0, offering a wide range of data for analysis. The resolutions of the photographs in the database differ widely, from 800x600 to as low as 384x256. Table 1 contains information regarding CASIA 2.0. A PC with an Intel(R) Core(TM) i5-2400 CPU running at 3.1 GHz and 16 GB of RAM was used for testing.

The baseline parameters for evaluation are as follows:

- Total Images: Represents the total number of test pictures.
- TP (True Positive): Denotes the correct identification of altered photographs.
- TN (True Negative): Refers to the accurate identification of genuine/original photographs.
- FN (False Negative): Indicates modified photographs incorrectly classified as unaltered.
- FP (False Positive): Occurs when genuine images are mistakenly labelled as fakes.

To assess the effectiveness of the proposed technique, accuracy, precision, recall, and F-measure are calculated and compared against alternative methods. These metrics are determined using the following equations:

$$Accuracy = \frac{T_P + T_N}{T_{Total\_Images}} \times 100$$

$$Recall = \frac{T_P}{T_P + F_N}$$

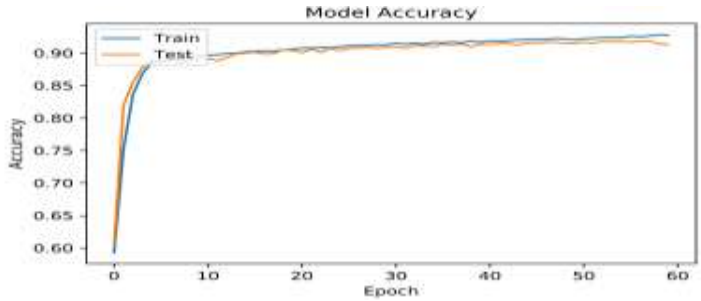
$$Precision = \frac{T_P}{T_P + F_P}$$

$$F_{measure} = \frac{2 \times Recall \times Precision}{Recall + Precision} \times 100$$

These metrics provide a comprehensive evaluation of the proposed technique's performance, facilitating comparisons with other methods.

Model Training and Testing:

We did a randomized distribution of original photos (80%) and changed images (4,099 out of 10,092 total images) in order to assess the effectiveness of the suggested strategy. We trained the model using the CASIA 2.0 database using Adam's optimizer with an initial learning rate of 1 x 10^5 and a batch size of 64. There were 2,522 photos in the collection; 1,498 of them were classified as legitimate ("real"), and 1,024 of them had been digitally altered to produce "fake" outcomes. The suggested model's training phase made use of these specifications.



Comparison with Other Techniques:

We evaluated the performance of our suggested method using a subset of the CASIA 2.0 database consisting of 20% of modified images and 80% of real photos. Of the 10,092 photos in total, 4,099 were changed photographs. Training was done using Adam's optimizer with a batch size of 64 and an initial learning rate of 1 x 10^5.

2,522 photos in the collection were examined; 1,498 of them were determined to be authentic ("real"), and 1,024 had been digitally altered to yield "fake" findings. Table 2 presents a comparison of our approach with existing methods for detecting phony photos using the CASIA 2.0 database.

The proposed method demonstrates superior speed and accuracy in predicting potential photo manipulation compared to current leading techniques

IV. PROPOSED WORK

The design of an advanced image analysis algorithm involves a multifaceted approach to detect signs of manipulation. It scrutinizes pixel values for inconsistencies, examines metadata alterations, and conducts content analysis to identify discrepancies within the image. By integrating these techniques, the algorithm aims to ensure the integrity and authenticity of digital imagery by identifying even subtle alterations.

V. RESULTS & ANALYSIS

In above screen we can see dataset contains 220 images and all images are processed and now click on 'Generate & Load Fusion Model' button to train all algorithms and then extract features from them and then calculate their accuracy

In above screen with existing SIFT SVM features we got 68% accuracy and in confusion matrix graph we can see existing SIFT predicted 6 and 8 instances incorrectly. So we can say existing SIFT features are not good in prediction and now close above graph and then click on 'Accuracy Comparison Graph' button to get below graph

VI. FURURE SCOPE

Moving forward, there are promising avenues for enhancing the method of identifying fake photos using CNNs. By integrating it with other advanced techniques, we can improve its accuracy and

effectiveness in detecting various forms of image manipulation. Adapting the technology to handle lower-quality photographs would make it more versatile and applicable to a wider range of scenarios. Moreover, the creation of a comprehensive database of image forgeries will strengthen the training process for deep learning networks, ultimately leading to more robust detection capabilities. These developments offer hope for combating the proliferation of false information and preserving trust in visual communication channels.

VII. CONCLUSION

The popularity of photos has increased due to the broad availability of inexpensive cameras, making visual communication essential. But this accessibility also makes photo-editing and the dissemination of false information easier. To overcome this, a novel method for identifying fake photos using CNNs is put forth. This method compares original and compressed images for training, combining image-reduction algorithms within the CNN framework. Finding fraudulent methods such as copy-move and splicing, it achieves 92.23% validation accuracy, which is promising. The objective is to reduce the complexity of image localization time and enhance accuracy by refining this technology through integration with other methods. The technique will also be modified for use with lower-quality photographs, and a thorough database of image forgeries will be created in order to train deep learning networks.

REFERENCES

[1] Amerini I, Uricchio T, Ballan L, Caldelli R. Localization of JPEG double compression through multi-domain convolutional neural networks. In: IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW); Honolulu, HI, USA; 2017. pp. 1865-1871. doi: 10.1109/CVPRW.2017.233

[2] Xiao B, Wei Y, Bi X, Li W, Ma J. Image splicing forgery detection combining coarse to refined convolutional neural network and adaptive clustering. Information Sciences 2020; 511: 172-191. doi: 10.1016/j.ins.2019.09.038

[3] K. D. Kadam, S. Ahirrao, and K. Kotecha, ‘‘Multiple image splicing dataset (MISD): A dataset for multiple splicing,’’ Data, vol. 6, no. 10, p. 102, Sep. 2021.

[4] R. Agarwal, O. P. Verma, A. Saini, A. Shaw, and A. R. Patel, ‘‘The advent of deep learning-based,’’ in Innovative Data Communication Technologies and Application. Singapore: Springer, 2021.

[5] M. A. Elaskily, M. H. Alkinani, A. Sedik, and M. M. Dessouky, ‘‘Deep learning based algorithm (ConvLSTM) for copy move forgery detection,’’ J. Intell. Fuzzy Syst., vol. 40, no. 3, pp. 4385–4405, Mar. 2021.

[4] A. Mohassin and K. Farida, ‘‘Digital image forgery detection approaches: A review,’’ in Applications of Artificial Intelligence in Engineering. Singapore: Springer, 2021.

[5]Sutthiwan P, Shi YQ, Zhao H, Ng TT, Su W. Markovian rake transform for digital image tampering detection. In: Shi YQ, Emmanuel S, Kankanhalli MS, Chang S-F, Radhakrishnan R (editors). Transactions on Data Hiding and Multimedia Security VI. Lecture Notes in Computer Science, Vol. 6730. Berlin, Germany: Springer; 2011, pp. 1-17

[6] He Z, Lu W, Sun W, Huang J. Digital image splicing detection based on Markov features in DCT and DWT domain. Pattern Recognition 2012; 45 (12): 4292-4299.

[7] Chang IC, Yu JC, Chang CC. A forgery detection algorithm for exemplar-based inpainting images using multi-region relation. Image and Vision Computing 2013; 31 (1): 57-71. [

8] Rhee KH. Median filtering detection based on variations and residuals in image forensics. Turkish Journal of Electrical Engineering & Computer Science 2017; 25 (5): 3811-3826.

[9] Lamba AK, Jindal N, Sharma S. Digital image copy-move forgery detection based on discrete fractional wavelet transform. Turkish Journal of Electrical Engineering & Computer Science 2018; 26 (3): 1261-1277. Lin Z, He J, Tang X, Tang CK. Fast, automatic, and fine-grained tampered JPEG image detection via DCT coefficient analysis. Pattern Recognition 2009; 42 (11): 2492-2501