IMAGE FORGERY DETECTION BASED ON FUSION OF LIGHTWEIGHT DEEP LEARNING MODELS

DR . K.SUDHAKAR[1], LAHARI MURIKI[2], MAROJU SANJANA[3],PABBOJU SHIVANI[4]

[1]Professor and Department of ECE, Malla Reddy Engineering College for Women (UGC-Autonomous) Maisammaguda,Hyderabad, TS, India.

[2,3,4] UG students Department of ECE, Malla Reddy Engineering College for Women (UGC-Autonomous) Maisammaguda,Hyderabad, TS, India.

ABSTRACT:

Capturing images has been increasingly popular in recent years, owing to the widespread availability of cameras. Images are essential in our daily lives because they contain a wealth of information, and it is often required to enhance images to obtain additional information. A variety of tools are available to improve image quality; nevertheless, they are also frequently used to falsify images, resulting in the spread of misinformation. This increases the severity and frequency of image forgeries, which is now a major source of concern. Numerous traditional techniques have been developed over time to detect image forgeries. In recent years, convolutional neural networks (CNNs) have received much attention, and CNN has also influenced the field of image forgery detection. However, most image forgery techniques based on CNN that exist in the literature are limited to detecting a specific type of forgery (either image splicing or copy-move). As a result, a technique capable of efficiently and accurately detecting the presence of unseen forgeries in an image is required. In this paper, we introduce a robust deep learning based system for identifying image forgeries in the context of double image compression. The difference between an image's original and recompressed versions is used to train our model. The proposed model is lightweight, and its performance demonstrates that it is faster than state-of-the-art approaches. The experiment results are encouraging, with an overall validation accuracy of 92.23%.

Keyword: CNN, image forgery, high efficiency.

INTRODUCTION

Due to technological advancements and globalization, electronic equipment is now widely and inexpensively available. As a result, digital cameras have grown in popularity. There are many camera sensors all around us, and we use them to collect a lot of images. Images are required in the form of a soft copy for various documents that must be filed online, and a large number of images are

shared on social media every day. The amazing thing about images is that even illiterate people can look at them and extract information from them. As a result, images are an integral component of the digital world, and they play an essential role in storing and distributing data. There are numerous tools accessible for quickly editing the images [1,2]. These tools were created with the intention of enhancing and improving the images. However, rather than enhancing the image, some people exploit their capabilities to falsify images and propagate falsehoods [3,4]. This is a significant threat, as the damage caused by faked images is not only severe, but also frequently irreversible.

There are two basic types of image forgery: image splicing and copy-move, which are discussed below:

• Image Splicing: A portion of a donor image is copied into a source image. A sequence of donor images can likewise be used to build the final forged image.

• Copy-Move: This scenario contains a single image. Within the image, a portion of the image is copied and pasted. This is frequently used to conceal other objects. The final forged image contains no components from other images.

The primary purpose in both cases of image forgery is to spread misinformation by changing the original content in an image with something else [5,6]. Earlier images were an extremely credible source for the information exchange, however, due to image forgery, they are used to spread misinformation. This is affecting the trust of the public in images, as the forging of images may or may not be visible or recognizable to the naked eye. As a result, it is essential to detect image forgeries to prevent the spread of misinformation as well as to restore public trust in images. This can be done by exploring the various artifacts left behind when an image forgery is performed, and they can be identified using various image processing techniques.

Researchers have proposed a variety of methods for detecting the presence of image forgeries [7–9]. Conventional image forgery detection techniques detect forgeries by concentrating on the multiple artifacts present in a forged image, such as changes in illumination, contrast, compression, sensor noise, and shadow. CNN's have gained popularity in recent years for various computer vision tasks, including image object recognition, semantic segmentation, and image classification. Two major features contribute to CNN's success in computer vision. Firstly, CNN takes advantage of the significant correlation between adjacent pixels. As a result, CNN prefers locally grouped connections over one-to-one

connections between all pixel. Second, each output feature map is produced through a convolution operation by sharing weights. Moreover, compared to the traditional method that depends on engineered features to detect specific forgery, CNN uses learned features from training images, and it can generalize itself to detect unseen forgery. These advantages of CNN make it a promising tool for detecting the presence of forgery in an image. It is possible to train a CNN-based model to learn the many artifacts found in a forged image [10–13]. Thus, we propose a very light CNN-based network, with the primary goal of learning the artifacts that occur in a tampered image as a result of differences in the features of the original image and the tampered region.

The major contribution of the proposed technique are as follows:

• A lightweight CNN-based architecture is designed to detect image forgery efficiently. The proposed technique explores numerous artifacts left behind in the image tampering process, and it takes advantage of differences in image sources through image recompression.

• While most existing algorithms are designed to detect only one type of forgery, our technique can detect both image splicing and copy-move forgeries and has achieved high accuracy in image forgery detection. • Compared to existing techniques, the proposed technique is fast and can detect the presence of image forgery in significantly less time. Its accuracy and speed make it suitable for real-world application, as it can function well even on slower devices.

LITERATURE SURVEY

Various approaches have been proposed in the literature to deal with image forgery. The majority of traditional techniques are based on particular artifacts left by image forgery, whereas recently techniques based on CNNs and deep learning were introduced, which are mentioned below. First, we will mention the various traditional techniques and then move on to deep learning based techniques.

In [14], the authors' proposed error level analysis (ELA) for the detection of forgery in an image. In [15], based on the lighting conditions of objects, forgery in an image is detected. It tries to find the forgery based on the difference in the lighting direction of the forged part and the genuine part of an image. In [16], various traditional image forgery detection techniques have been evaluated. In [17], Habibi et al., use the contourlet transform to retrieve the edge pixels for forgery detection. In [18], Dua et al., presented a JPEG compression-based method. The discrete DCT coefficients are assessed independently for each block of an image partitioned into non-overlapping blocks of size 8 × 8 pixels. The statistical features of AC components of block DCT coefficients alter when a JPEG compressed image tampers. The SVM is used to classify authentic and forged images using the retrieved feature vector. Ehret et al. in [19] introduced a technique that relies on SIFT, which

provides sparse keypoints with scale, rotation, and illumination invariant descriptors for forgery detection. A method for fingerprint faking detection utilizing deep Boltzmann machines (DBM) for image analysis of high-level characteristics is proposed in [20]. Balsa et al. in [21] compared the DCT, Walsh–Hadamard transform (WHT), Haar wavelet transform (DWT), and discrete Fourier transform (DFT) for analog image transmission, changing compression and comparing quality. These can be used for image forgery detection by exploring the image from different domains. Thanh et al. proposed a hybrid approach for image splicing in [22], in which they try to retrieve the original images that were utilized to construct the spliced image if a given image is proven to be the spliced image. They present a hybrid image retrieval approach that uses Zernike moment and SIFT features

Bunk et al. established a method for detecting image forgeries based on resampling features and deep learning in [23]. Bondi et al. in [24] suggested a method for detecting image tampering by the clustering of camera-based CNN features. Myung-Joon in [2] introduced CAT-Net, to acquire forensic aspects of compression artifact on DCT and RGB domains simultaneously. Their primary network is HR-Net (high resolution). They used the technique proposed in [25], which tells us that how we can use the DCT coefficient to train a CNN, as directly giving DCT coefficients to CNN will not train it efficiently. Ashraful et al. in [26] proposed DOA-GAN, to detect and localize copy-move forgeries in an image, authors used a GAN with dual attention. The first-order attention in the generator is designed to collect copy-move location information, while the second-order attention for patch co-occurrence exploits more discriminative properties. The affinity matrix is utilized to extract both attention maps, which are then used to combine location-aware and co-occurrence features for the network's ultimate detection and localization branches.

Yue et al. in [27] proposed BusterNet for copy-move image forgery detection. It has a two-branch architecture with a fusion module in the middle. Both branches use visual artifacts to locate potential manipulation locations and visual similarities to locate copymove regions. Yue et al. in [28] employed a CNN to extract block-like characteristics from an image, compute self-correlations between various blocks, locate matching points using a point-wise feature extractor, and reconstruct a forgery mask using a deconvolutional network. Yue et al. in [3] designed ManTra-Net that is s a fully convolutional network that can handle any size image and a variety of forgery types, including copy-move, enhancement, splicing, removal, and even unknown forgery forms. Liu et al. in [29] proposed PSCC-Net, which analyses the image in a two-path methodology: a top-down route that retrieves global and local features and a bottom-up route that senses if the image is tampered and predicts its masks at four levels, each mask being constrained on the preceding one.

In [30] Yang et al., proposed a technique based on two concatenated CNNs: the coarse CNN and the refined CNN, which extracts the differences between the image itself and splicing regions from patch descriptors of different scales. They enhanced their work in [1] and proposed a patch-based coarse-to-refined network (C2RNet). The coarse network is based on VVG16, and the refined network is based on VVG19. In [31] Xiuli et al., proposed a ringed residual U-Net to detect the splicing type image forgery in the images. Younis et al. in [32] utilized the reliability fusion map for the detection of the forgery. By utilizing the CNNs, Younis et al. in [33] classify an image as the original one, or it contains copy-move image forgery. In [34] Vladimir et al., train four models at the same time: a generative annotation model GA, a generative retouching model GR, and two discriminators DA and DR that checks the output of GA and GR. Mayer et al. in [35] introduced a system that maps sets of image regions to a value that indicates if they include the same or different forensic traces

PROPOSED SYSTEM

CNNs, which are inspired by the human visual system, are designed to be non-linear interconnected neurons. They have already demonstrated extraordinary potential in a variety of computer vision applications, including image segmentation and object detection. They may be beneficial for a variety of additional purposes, including image forensics. With the various tools available today, image forgery is fairly simple to do, and because it is extremely dangerous, detecting it is crucial. When a fragment of an image is moved from one to another, a variety of artifacts occur due to the images' disparate origins. While these artifacts may be undetectable to the naked eye, CNNs may detect their presence in faked images. Due to the fact that the source of the forged region and the background images are distinct, when we recompress such images, the forged is enhanced differently due to the compression difference. We use this concept in the proposed approach by training a CNN-based model to determine if an image is genuine or a fake.

A region spliced onto another image will most likely have a statistically different distribution of DCT coefficients than the original region. The authentic region is compressed twice: first in the camera, and then again in the fake, resulting in periodic patterns in the histogram [2]. The spliced section behaves similarly to a singly compressed region when the secondary quantization table is used.

As previously stated, when an image is recompressed, if it contains a forgery, the forged portion of the image compresses differently from the remainder of the image due to the difference between the source of the original image and the source of the forged portion. When the difference between the

original image and its recompressed version is analyzed, this considerably emphasizes the forgery component. As a result, we use it to train our CNN-based model for detecting image forgery.

Algorithm 1 shows the working of the proposed technique, which has been explained here. We take the forged image A (images shown in Figure 1b tamper images), and then recompress it; let us call the recompressed image as Arecompressed (images shown in Figure 1c are recompressed forged images). Now we take the difference of the original image and the recompressed image, let us call it Adi f f (images shown in Figure 1e are the difference of Figure 1b,c, respectively). Now due to the difference in the source of the forged part and the original part of the image, the forged part gets highlighted in Adi f f (as we can observe in Figure 1d,e, respectively). We train a CNN-based network to categorize an image as a forged image or a genuine one using Adi f f as our input features (we label it as a featured image). Figure 2 gives the pictorial view of the overall working of the proposed method.

To generate Arecompressed from A, we use JPEG compression. Image A undergoes JPEG compression and produces Arecompressed as described in Figure 3. When there is a single compression, then the histogram of the dequantized coefficients exhibits the pattern as shown in Figure 4, this type of pattern is shown by the forged part of the image. Moreover, when there is a sort of double compression then, as described in Figure 5, there is a gaping between the dequantized coefficients as shown in Figure 6, this type of pattern is shown by the genuine part of the image.

We constructed a very light CNN model with minimal parameters in our proposed model (line number 5 to 13 of Algorithm 1). We constructed a model consisting of 3 convolutional layers after which there is a dense fully connected layer, as described below:

• The first convolutional layer consists of 32 filters of size 3-by-3, stride size one, and “relu” activation function.

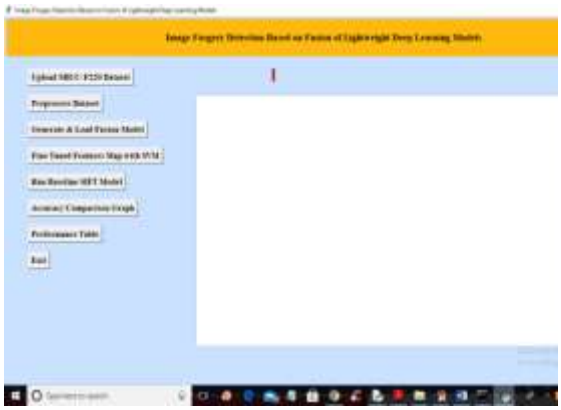
• The second convolutional layer consists of 32 filters of size 3-by-3, stride size one, and “relu” activation function.

• The third convolutional layer consists of 32 filters of size 7-by-7, stride size one, and “relu” activation function, followed by max-pooling of size 2-by-2.

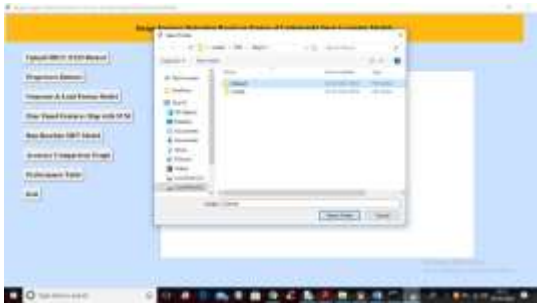
• Then we have the dense layer that has 256 neurons with “relu” activation function, finally which is connected to two neurons (output neurons) with “sigmoid” activation.

IMPLEMENTATION :

To run project double click on ‘run.bat’ file to get below output



In above screen click on 'Upload MICC-F220 Dataset' button to upload dataset and get below output

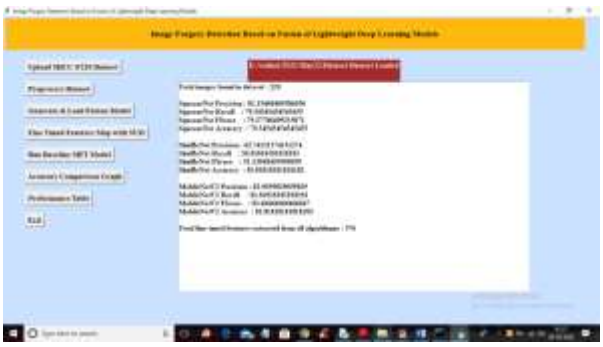


In above screen selecting and uploading 'Dataset' folder and then click on 'Select Folder' button to load dataset and get below output

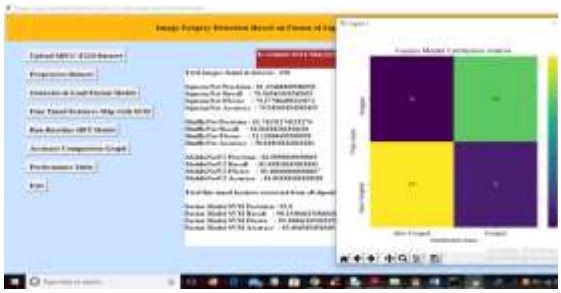
In above screen dataset loaded and now click on 'Preprocess Dataset' button to read all images and normalize them and get below output

In above screen all images are processed and to check images loaded properly I am displaying one sample image and now close above image to get below output

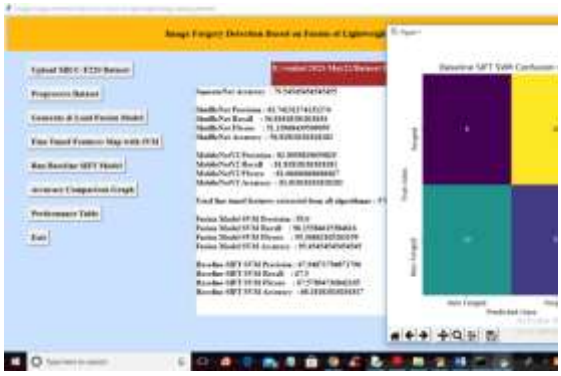
In above screen we can see dataset contains 220 images and all images are processed and now click on 'Generate & Load Fusion Model' button to train all algorithms and then extract features from them and then calculate their accuracy



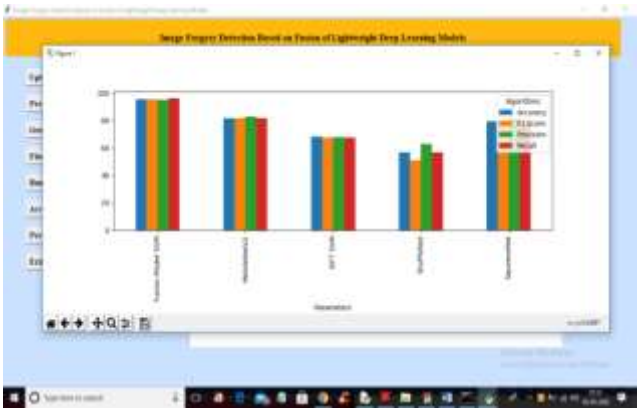
In above screen we can see accuracy of all 3 algorithms and then in last line we can see from all 3 algorithms application extracted 576 features and now click on 'Fine Tuned Features Map with SVM' to train SVM with extracted features and get its accuracy as fusion model



In above screen with Fine tune SVM fusion model we got 95% accuracy and in confusion matrix graph x-axis represents PREDICTED LABELS and y-axis represent TRUE labels and we can see both X and Y boxes contains more number of correctly prediction classes. In all algorithms we can see fine tune features with SVM has got high accuracy and now close confusion matrix graph and then click on 'Run Baseline SIFT Model' button to train SVM with SIFT existing features and get its 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



In above graph x-axis represents algorithm names and y-axis represents accuracy and other metrics where each different colour bar represents different metrics like precision, recall etc. Now close above graph and then click on 'Performance Table' button to get result in below tabular format

In above screen we can see propose fusion model SVM with fine tune features has got 95% accuracy which is better than all other algorithms

CONCLUSION

The increased availability of cameras has made photography popular in recent years. Images play a crucial role in our lives and have evolved into an essential means of conveying information since the general public quickly understands them. There are various tools accessible to edit images; these tools are primarily intended to enhance images; however, these technologies are frequently exploited to forge the images to spread misinformation. As a

result, image forgery has become a significant problem and a matter of concern. In this paper, we provide a unique image forgery detection system based on neural networks and deep learning, emphasizing the CNN architecture approach. To achieve satisfactory results, the suggested method uses a CNN architecture that incorporates variations in image compression. We use the difference between the original and recompressed images to train the model. The proposed technique can efficiently detect image splicing and copy-move types of image forgeries. The experiments results are highly encouraging, and they show that the overall validation accuracy is 92.23%, with a defined iteration limit.

We plan to extend our technique for image forgery localization in the future. We will also combine the suggested technique with other known image localization techniques to improve their performance in terms of accuracy and reduce their time complexity. We will enhance the proposed technique to handle spoofing [50] as well. The present technique requires image resolution to be a minimum of 128 × 128, so we will enhance the proposed technique to work well for tiny images. We will also be developing a challenging extensive image forgery database to train deep learning networks for image forgery detection.

REFERENCES

1.Xiao, B.; Wei, Y.; Bi, X.; Li, W.; Ma, J. Image splicing forgery detection combining coarse to refined convolutional neural network and adaptive clustering. Inf. Sci. 2020, 511, 172–191. [CrossRef]

2. Kwon, M.J.; Yu, I.J.; Nam, S.H.; Lee, H.K. CAT-Net: Compression Artifact Tracing Network for Detection and Localization of Image Splicing. In Proceedings of the 2021 IEEE Winter Conference on Applications of Computer Vision (WACV), Waikoloa, HI, USA, 5–9 January 2021; pp. 375–384.

3. Wu, Y.; Abd Almageed, W.; Natarajan, P. ManTra-Net: Manipulation Tracing Network for Detection and Localization of Image Forgeries With Anomalous Features. In Proceedings of the 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), Long Beach, CA, USA, 15–20 June 2019; pp. 9535–9544.

4. Ali, S.S.; Baghel, V.S.; Ganapathi, I.I.; Prakash, S. Robust biometric authentication system with a secure user template. Image Vis. Comput. 2020, 104, 104004. [CrossRef]

5. Castillo Camacho, I.; Wang, K. A Comprehensive Review of Deep-Learning-Based Methods for Image Forensics. J. Imaging 2021, 7, 69. [CrossRef] [PubMed]

6. Zheng, L.; Zhang, Y.; Thing, V.L. A survey on image tampering and its detection in real-world photos. J. Vis. Commun. Image Represent. 2019, 58, 380–399. [CrossRef]

7. Jing, L.; Tian, Y. Self-supervised Visual Feature Learning with Deep Neural Networks: A Survey. IEEE Trans. Pattern Anal. Mach. Intell. 2020, 43, 1. [CrossRef]

8. Meena, K.B.; Tyagi, V. Image Forgery Detection: Survey and Future Directions. In Data, Engineering and Applications: Volume 2; Shukla, R.K., Agrawal, J., Sharma, S., Singh Tomer, G., Eds.; Springer: Singapore, 2019; pp. 163–194.

9. Mirsky, Y.; Lee, W. The Creation and Detection of Deepfakes: A Survey. ACM Comput. Surv. 2021, 54, 1–41. [CrossRef]

10. Rony, J.; Belharbi, S.; Dolz, J.; Ayed, I.B.; McCaffrey, L.; Granger, E. Deep weakly-supervised learning methods for classification and localization in histology images: A survey. arXiv 2019, arXiv:abs/1909.03354.