Volume: 15 Issue: 03 Pages: 5946 - 5951 (2023) ISSN: 0975-0290

Detection of Forged Images and Accuracy Assessment Over Authenticated Images

Ganapathi Krishna. P. Hegde
Department of Information Science, SDM Institute of Technology, Ujire, India
Email: gphegde@sdmit.in
Dinesh G. Hegde
Department of Computer Science, SDM Institute of Technology, Ujire, India
Email: dineshhegdeofficial@gmail.com

----------**ABSTRACT**----------

Today manipulation of images drastically increasing in many fields of photography, this would cause the highly gradable threats. This makes misleading of authentication of communicational networks. The human eye cannot detect the manipulated image over original image. Similarly image to image feature transformation also cannot be achieved by human eye. This needs computer based learning techniques to identify image manipulation. Some of the state of art approaches was poor to classify and detect the manipulated images. This paper emphasizes the detection and assessment of forged content in manipulated images. This paper also implements the rate of false information added to original images and restore public confidence in the authenticity of images.

Keywords - Forged, Compression, Detection, Analysis.

Date of Submission: July 21, 2023 Date of Acceptance: September 25, 2023

I. INTRODUCTION

The image forging occurs when one image features are incorporated with some other images features either by hiding or exposing original image content. The authentic images are required for in large volume for social media networks. The outcome of the research experiments goes wrong due large usage of forged images with other images. Direct view of human cannot determine the fake content in the images, so it is essential to stop the fraud in image reformation. Image can be morphed or enhanced by using fraud tools to forge the images. The work carried out in this area illustrates and proposes a deep learning algorithm based image forging applications.

II. RELATED WORK

Sing et al. [1] used deep neural network for detecting forged content in image. They worked on (CNN) neural network and carried experiment on CASIA 2.0 database. Selvaraj et al.[2] worked on machine learning practices for the recognition of forged content in image. They combined machine learning through deep learning techniques. They limited their work for old images it cannot detect new images. Mena et al [3] carried out image forging method. They used tetrolet transform to extract feature vectors. Benhamza et a. l[4] proposed a framework on both image and document forgery detection. They verified image authentication by detecting forged content in images. The administrative documents forging detection has been carried by them. Huang et al. [5] worked on image forging technic based on scale invariants feature transform algorithm. The localized forging requires were found using single tempered region detection. Thepade et al. [6] proposed extraction of digital signatures and found difference between forged and authentication images. They implemented several machine learning techniques for image classification. Yeap et al. [7] addressed about copy move forging detection. They got 84.33% accuracy after evaluating image database hierarchical Agglomerative clustering as feature matching method.

III. PROPOSED FRAMEWORK

By combining different techniques, we can enhance the precision of image forensics. For instance, one strtaegy is to use error level analysis (ELA) to identify potential areas in images and compares the compression levels of different areas within the same image and highlights any discrepancies. Convolution Neural Network (CNN) approach can be trained by supervised learning technique to strengthen the reliability of the image data assessment. This approach involves feeding the CNN with a large dataset of authentic and tampered images to enable it to learn and recognize patterns associated with both categories. Once trained, the CNN can accurately classify whether an image is authentic or tampered. System design of our proposed system is described in the following steps.

3.1 Dataset used

We have used the CasiaV2 dataset to train the prototype model. The CasiaV2 dataset is a broadly used benchmark dataset for image forensics research. CasiaV2 contains over 12,532 authentic images and 7,408 Tampered images of all formats and sizes.

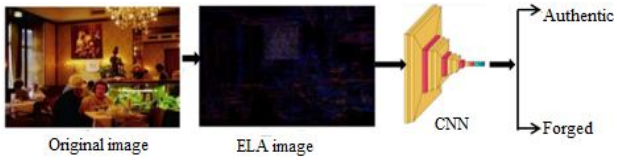

Figure 1. Architecture of proposed system

Volume: 15 Issue: 03 Pages: 5946 - 5951 (2023) ISSN: 0975-0290

3.2 Acquisition and Loading Data

The CasiaV2 dataset is a extensively used target database for image forensics study. It contains over 12,560 images, including both authentic and tampered images. The dataset was created by the Chinese Academy of Sciences and provides a diverse range of tampering techniques, such as copy-move, splicing, and removal, to name a few. The authentic images in the dataset were obtained from different sources, including professional photographers and public image-sharing websites. On the other hand, the tampered images were synthetically generated by applying various manipulation techniques to the authentic images. CasiaV2 contains over 7,437 authentic images and 5,123 Tampered images.

3.3 Data Preprocessing and ELA

We have loaded the images of all formats from the CasiaV2 dataset which contains 2 folders, tampered and Authentic. It consists of 7,437 authentic and 5,123 tampered images of various sizes from 240x160 to 900x600 with JPEG, BMP, and TIFF formats. In resizing the images process, we have reshaped the images into 128x128 pixels. Resizing an image to 128 by 128 pixels is preferred in CNNs because it reduces the computational density of the network. This means that the network can process the image faster and with fewer resources. Additionally, resizing the image to a standard size ensures that all images fed into the network have the same dimensions, which is necessary for the network to work properly.

One of the techniques used to detect image manipulation is Error Level Analysis (ELA). This technique involves saving a picture at a certain quality level and then calculating the comparison between its levels. ELA is typically performed on images in JPEG format. In JPEG images, compression is independently applied to each 8x8 pixel in the image. If an image is not manipulated, each 8x8 pixel in the image should have the same error level. However, saving a JPEG image causes the colors to change slightly, and the ELA results highlight the areas in the image that are most susceptible to color degradation during a resave. Any edits made to the image will stand out as a region with a higher degradation potential compared to the remaining images. ELA saves the image at a specified JPEG quality level, which introduces a known amount of error across the entire image.

The resaved image is then compared to the original image. If the image is unmodified, then all 8x8 squares should have similar error potentials, and if the image is unmodified and resaved, then every square should degrade at approximately the same rate. However, if the image is modified, then every 8x8 square that was affected by the modification should have a higher error potential than the remaining image, and modified areas will appear with a higher potential error level.

After applying Error Level Analysis on each image in the dataset, it is appended to the X variable and parallelly append 0 to the Y variable to indicate the Tampered image and 1 to indicate the authentic image. Architecture of proposed system is shown in Figure 1.

3.4 Splitting Data

Data in machine learning, splitting the dataset into training, validation, and testing sets is crucial to confirm that the model is able to generalize well on new, unseen data. In our system, a split of 76% training, 19% validation, and 5% testing is reasonable for many applications. The training set is used to train the model, while the validation set is used to evaluate the performance of the model during training and to fine-tune hyper parameters. The testing set, which is separate from the training and validation sets, is used to evaluate the final performance of the model on unseen data. A 76% training set provides sufficient data for the model to learn from, while a 19% validation set allows for adequate monitoring of the model's performance during training without over fitting. Finally, a 5% testing set is enough to obtain a reliable estimate of the model's generalization performance. However, the specific split ratio may vary depending on the size and complexity of the dataset, the nature of the problem, and the available computational resources. It is also important to ensure that the data is split randomly to avoid bias in the model's performance. So, a random state of 0.5 is applied.

3.5 Training and Testing

Convolutional Neural Network (CNN) is a type of deep learning algorithm that is commonly used for image and video recognition tasks. CNNs are particularly useful in these fields because they are designed to effectively handle the large quantity of data and complex structures that are often present in images and videos. One key advantage of CNNs is their ability to automatically learn features from raw pixel data, without the need for manual feature extraction. This is achieved through the use of convolutional layers, which apply a set of learned filters to input data, allowing the network to identify important features at multiple scales and levels of abstraction. Performance metrics used for evaluation include accuracy and F1 score values [14].

We have used CNN Sequential model to perform the classification of Authentic and Tampered images. The Convolutional Layers are shown in Figure 2. The model starts with two convolutional layers (Conv2D) that have 32 filters each. These layers apply a set of filters to the input image, capturing different features at different scales. The kernel size is set to (5, 5), which means each filter operates on a 5x5 window of the input. The activation function used in these layers is ReLU, which introduces nonlinearity and helps the model learn complex patterns. Following the convolutional layers, a max pooling layer (MaxPool2D) with a pool size of (2, 2) is added. This layer reduces the spatial dimensions of the feature maps while retaining the most important information. Max pooling helps make the model more robust to spatial variations and reduces the number of parameters, making the model more efficient. To prevent

Volume: 15 Issue: 03 Pages: 5946 - 5951 (2023) ISSN: 0975-0290

over fitting, a dropout layer (Dropout) is included after the max pooling layer. It randomly sets 25% of the input units to 0 during training, which reduces the reliance of the model on specific features and encourages it to learn more generalizable representations. The output of the dropout layer is then flattened into a 1D vector using the Flatten layer. This flattening operation prepares the data to be fed into the subsequent fully connected layers. The model continues with a dense layer (Dense) consisting of 256 units. This layer is fully connected to the flattened input and learns high-level representations by combining the features learned by the previous convolutional layers. The activation function used is ReLU, introducing non-linearity to the model. To further prevent over fitting, another dropout layer is added after the dense layer. This time, 50% of the units are randomly set to 0 during training. This dropout layer encourages the model to learn more robust and generalizable representations. Finally, the model ends with a dense layer with a single unit. This layer uses a sigmoid activation function to produce the result of the model. The sigmoid function squashes the output between 0 and 1, representing the predicted probability of the input image belonging to the positive class. This output is utilized to predict whether the image is Authentic or Tampered.

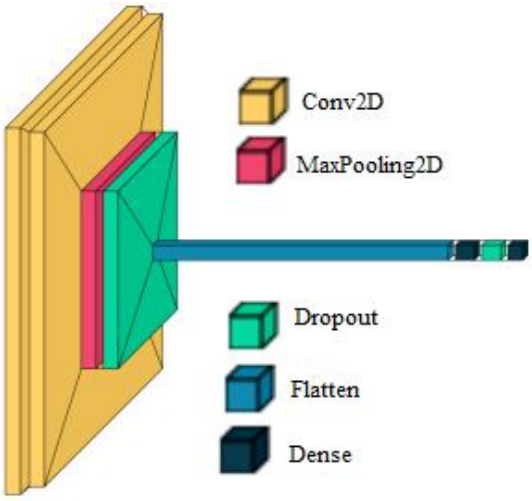

Figure 2. Convolutional layers

Two important components of the model training process are implemented, the optimizer and early stopping. The optimizer determines how the model's weights are updated during the training process to minimize the loss function. In this case, the Adam optimizer is used, which a popular optimization algorithm is known for its efficiency and good performance on various deep-learning tasks. The learning rate is set to 1e-4, which controls the step size taken during weight updates. Additionally, the decay parameter is set to init_lr/epochs, which reduces the learning rate over time as the training progresses, allowing the model to fine-tune its performance. After defining the optimizer, the model is compiled using the compile function. The chosen loss function is 'binary_crossentropy which is commonly used for binary classification tasks. The metrics parameter is set to ['accuracy'], which means the model's performance will be evaluated based on its accuracy during training.

Over fitting is a common problem in machine learning models, where the model performs well on the training data but fails to generalize to unseen data. Early stopping is a technique used to prevent over fitting by monitoring a specific metric during training and stopping the training process if the metric stops improving. The min_delta parameter is set to 0, indicating that any improvement in the monitored metric is considered significant. The patience parameter is set to 10, meaning that if the monitored metric does not improve for 10 consecutive epochs, the training process will be stopped. By using early stopping, we can prevent the model from over fitting and save time by avoiding unnecessary training epochs. Figure 3 depicts the proposed frame work.

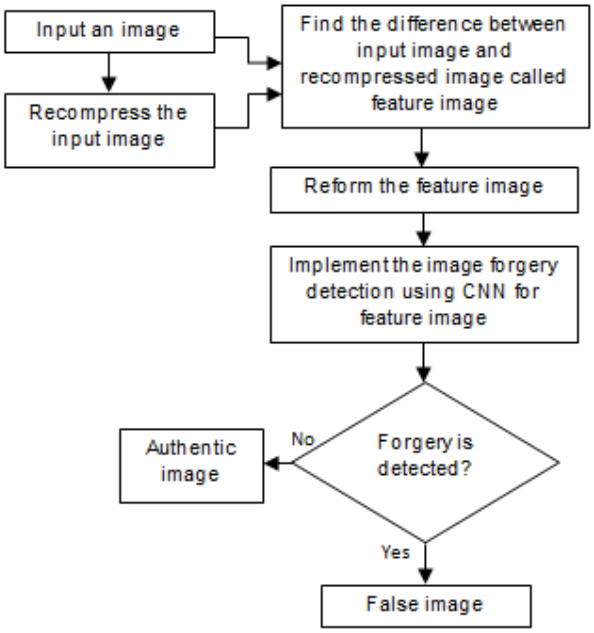

Figure 3. Proposed framework

Within Deep Learning, a Convolutional Neural Network or CNN is a type of artificial neural network, which is widely used for image or object recognition and classification. Deep Learning thus recognizes objects in an image by using a CNN. The major role of CNNs is found in diverse tasks or functions like image processing problems, computer vision tasks like localization and segmentation, video analysis, recognizing obstacles in self-driving cars, as well as speech recognition in natural language processing.

To classify an image as tampered and authentic images, we used a deep learning model to extract features of images automatically. More specifically, we have used Error Level Analysis (ELA) to detect areas of an image that may have been tampered. Error Level Analysis takes the image and recompresses it and then takes the difference between the input image and recompressed

Volume: 15 Issue: 03 Pages: 5946 - 5951 (2023) ISSN: 0975-0290

image. Then Convolution Neural Network (CNN) is used to train a supervised model for classifying whether an image is an authentic or tampered image.

Any edits made to the image will stand out as a region with a higher degradation potential compared to the rest of the image. ELA saves the image at a specified JPEG quality level which introduces a known amount of error across the entire image. The resaved image is then compared to the original image. If the image is unmodified, then all 8x8 squares should have similar error potentials, and if the image is unmodified and resaved, then every square should degrade at approximately the same rate. However, if the image is modified, then every 8x8 square that was affected by the modification should have a higher error potential than the remaining images, and modified areas will appear with a higher potential error level. After applying Error Level Analysis on each image in the dataset, it is appended to the X variable and parallelly append 0 to the Y variable to indicate the Tampered image and 1 to indicate the authentic image.

Author	Method/Technique used	Percentage of accuracy
Y Zhu et al. [8]	end-to-end neural network MICC-F220 data set	95%
A. Islam[9]	Dual-order attentive generative adversarial network	90%
Y. Wu [10]	BusterNet	85%
J.-L. Zhong[11]	Dense-InceptionNet and DN Network	75%
Amerini[12]	invariant features transform (SIFT)	90.6
Elaskily[13]	copy-move forgery detection	96.00

Table 1 shows state of art approaches.

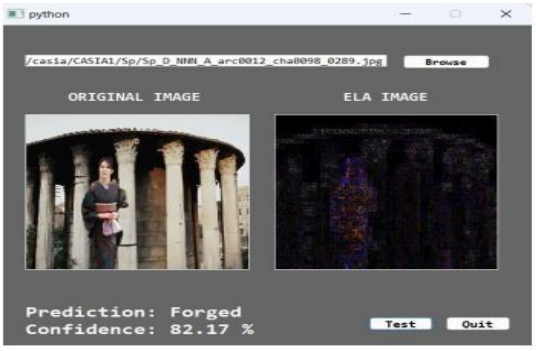

Figure 4. Front end design

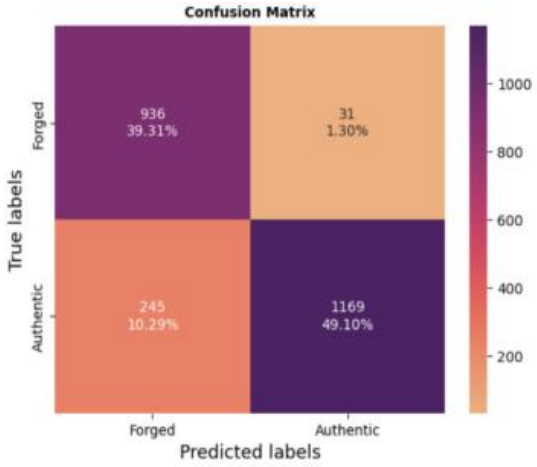

Figure 5. Confusion matrix

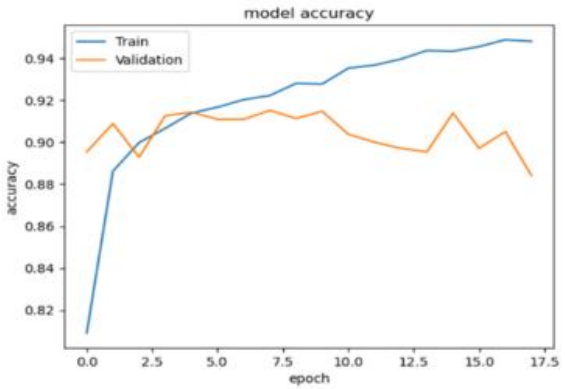

Figure 6. Model accuracy curve

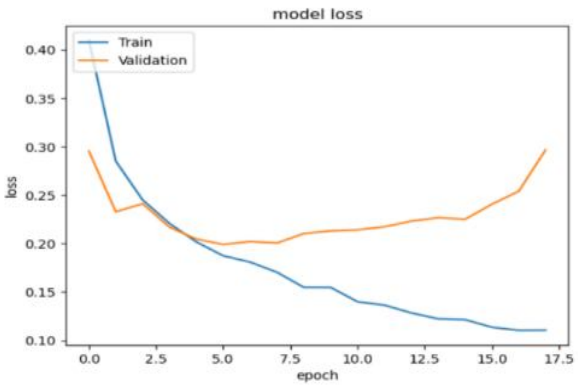

Figure 7. Model loss curve

Volume: 15 Issue: 03 Pages: 5946 - 5951 (2023) ISSN: 0975-0290

IV. RESULTS AND DISCUSSIONS

In this section all the results and the discussions should be made. The task of detecting image forgery poses significant challenges in today's technologically advanced era. It is crucial to differentiate between authentic and manipulated images accurately. In this research, we propose a deep-learning approach for identifying image forgery. In this work model developed utilizes Convolutional Neural Network (CNN) architecture, incorporating Error Level Analysis. By employing this architecture, we aim to enhance the detection rate of tampered images, contributing to more effective image forgery detection method. Figure 4 shows front end design. Figure 5 shows confusion matrix. Model accuracy Curve shown in Figure 6 produced by CNN model, while training the model using the training dataset. Our model has epoch loss of 1.1%. Figure 7 shows the model loss of our CNN model. Our model has achieved an accuracy of 95.3% and an F1 score of 96.9%.

V. CONCLUSION

To obtain larger number of contents from the images and to enhance the quality of images it is essential to enhance the images. Hence image forging helps in reduce the false information in images. The identification of fake images can be achieved through conventional techniques. Recently manipulation of image content and its detection was carried out through convolutional neural networks. Our work proposes a framework for identification of image false information using a 13 combination of Convolutional Neural Network (CNN)[15] and Error Level Analysis (ELA). We recognized the increasing prevalence of manipulated images in the digital landscape, which has become a significant source of fake news and misinformation. To report this issue, we developed a prototype that leverages the power of deep learning and ELA to accurately identify altered regions within images. We used Casia V2 dataset for accuracy assessment of both manipulated images and authenticated images. Proposed CNN model designed in this work produced 95.5% accuracy and F1 score of 96.6%.

REFERENCES

[1] A. Singh and J. Singh, "Image forgery detection using Deep Neural Network," 2021 8th International Conference on Signal Processing and Integrated Networks (SPIN), 2021, pp. 504-509, doi: 10.1109/SPIN52536.2021.9565953.

[2] Selvaraj, Shanthraj and I M, Ramya, Image Forgery Detection Using Machine Learning (October 27, 2021). //dx.doi.org/10.2139/ssrn.3950994.

[3] Kunj Bihari Meena, Vipin Tyagi, A copy-move image forgery detection technique based transform, Journal of Information Security and Applications, Volume 52, 2020, 102481, ISSN 2214-2126,

[4] Benhamza, H., Djeffal, A., Cheddad, A. (2021) Image forgery detection review In: Proceedings - 2021 International Conference on Information Systems and Advanced Technologies, ICISAT 2021 Institute of Electrical and Electronics Engineers Inc.

[5] Huang, HY., Ciou, AJ. Copy-move forgery detection for image forensics using the superpixel segmentation and the Helmert transformation. J Image Video Proc. 2019, 68 (2019).,https://doi.org/10.1186/s13640-019-0469-9.

[6] S. D. Thepade, S. Bhandari, C. Bagde, R. Chaware and K. Lodha, "Image Forgery Detection using Machine Learning with Fusion of Global and Local Thepade's SBTC Features," 2021 International Conference on Disruptive Technologies for Multi-Disciplinary Research and Applications (CENTCON), Bengaluru, India, 2021, pp. 234-238, doi: 10.1109/CENTCON52345.2021.9688094.

[7] Y. Y. Yeap, U. U. Sheikh and A. A. -H. Ab Rahman, "Image forensic for digital image copy move forgery detection," 2018 IEEE 14th International Colloquium on Signal Processing & Its Applications (CSPA), Penang, Malaysia, 2018, pp. 239-244, doi: 10.1109/CSPA.2018.8368719.

[8] Y. Zhu, Ch. Chen, G. Yan, Y. Guo, and Y. Dong, ‘‘AR-Net: Adaptive attention and residual refinement network for copy-move forgery detection,’’ IEEE Trans. Ind. Info

[9] A. Islam, C. Long, A. Basharat, and A. Hoogs, ‘‘DOA-GAN: Dual-order attentive generative adversarial network for image copy-move forgery detection and localization,’’ in Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit., Jun. 2020, pp. 4676–4685.

[10] Y. Wu, W. Abd-Almageed, and P. Natarajan, ‘‘BusterNet: Detecting copy-move image forgery with source/target localization,’’ in Proc. Conf. Comput. Vis. Pattern Recognit., 2018, pp. 168–184. [Online]. Available: https://link.springer.com/conference/eccv

[11] J.-L. Zhong and C.-M. Pun, ‘‘An end-to-end dense-inceptionNet for image copy-move forgery detection,’’ IEEE Transaction. Information. Forensics Security, vol. 15, pp. 2134–2146, 2020, doi: 10.1109/TIFS.2019.2957693.

[12] I. Amerini, L. Ballan, R. Cardelli, A. Del Bimbo, and G. Serra, ‘‘A siftbased forensic method for copy–move attack detection and transformation recovery,’’ IEEE Trans. Inf. Forensics Security, vol. 6, no. 3, pp. 1099–1110, Mar. 2011.

[13]M. Elaskily, H. Elnemr, M. Dessouky, and O. Faragallah, ‘‘Two stages object recognition based copy-move forgery detection algorithm,’’ Multimedia Tools Appl., vol. 78, no. 11, pp. 15353–15373, 2019.

Volume: 15 Issue: 03 Pages: 5946 - 5951 (2023) ISSN: 0975-0290

[14] Zanardelli, M., Guerrini, F., Leonardi, R. et al. Image forgery detection: a survey of recent deep-learning approaches. Multimed Tools Appl **82**, 17521–17566 (2023). https://doi.org/10.1007/s11042-022-13797-w

[15] Adel Hassan, Muath Sabha, "Feature Extraction for Image Analysis and Detection using Machine Learning Techniques", Int. J. Advanced Networking and Applications Volume: 14 Issue: 04 Pages: 5499-5508(2023) ISSN: 0975-0290 5499

[16] Manjeshbn, Madhu BN, "Enhancing Image Copy-Move Forgery Detection using Particle Swarm Optimization Techniques", International Journal of Advanced Networking & Applications (IJANA) ISSN: 0975-0282

Authors Biography

First Author is presently working as Associate Professor in SDM Institute of Technology, Ujire. India. He has completed PhD degree in Computer Science Engineering from VT University, Belagavi during 2018. He has 27 years of experience. He has completed MTech in Computer Science Engineering from VTU. He has completed BE in 1994 from Karnataka University Dharwad. And he has published more than 30 research articles in various reputed International Journals. He is the member of various review committees of International Journals.

Second author is a student of SDM Institute of Technology, Ujire, studying in final year BE computer science engineering. He is interested in machine learning, data science, image processing and computer networks.