International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Image Manipulation Detection Using Error Level Analysis and Deep Learning

Prajakta Kubal[1], Vanita Mane[2], Namita Pulgam[3]

Submitted: 08/05/2023 **Revised**: 16/07/2023 **Accepted**: 07/08/2023

Abstract*:* With the increasing prevalence of image forgery facilitated by digital editing software, the need for image verification has become paramount in maintaining image integrity and preventing misuse. In this paper we introduce our implemented system called EACN (Error Analysis and Convolutional Neural Network), which combines error level analysis and CNNs. By evaluating the error rate resulting from image quality reduction, we can determine the authenticity of an image. While metadata analysis has been used for image verification, it is susceptible to manipulation. Our implemented system, EACN (Error Analysis and Convolutional Neural Network), combines error level analysis and Convolutional Neural Networks (CNNs) to analyse error rates in genuine and manipulated images. With an impressive accuracy rate of 92.10%, our system leverages deep learning to provide a robust solution for detecting and identifying forged images, ensuring image integrity, preventing misuse, and safeguarding digital content authenticity.

Keywords: *Convolution neural network, Deep learning, Error Level Analysis, Image forgery.*

1. Introduction

The act of image forgery involves altering or manipulating original images. In the virtual communities of social networking sites, people can interact and communicate with each other. Identifying the legitimacy and source of multimedia content has become essential in today's world for building trust in pictures and videos shared on online platforms. Due to the ease of sharing content on social media, false images and videos can quickly become viral, and trusting discredited multimedia can lead to sensational news and gossip. Consequently, there is a critical need for a technology to distinguish between authentic and false photographs that are being shared online.

With the proliferation of digitally manipulated images in mainstream media and online, it has become increasingly difficult for people to discern whether an image has been tampered with. This poses a substantial danger to digital media's legitimacy and emphasizes the need for methods to validate the validity and integrity of digital images, particularly when they are used as evidence in legal processes or in financial and medical records. Image forensics, which aims to detect forgery, is crucial in addressing this issue. One technique used in image forensics is Error Level Analysis (ELA), which involves analyzing images at different levels of compression to identify any digital alterations. ELA is an effective tool in determining the veracity of image data.

There are two main ways for picture forgery: active and passive approaches. The active approach involves the use of pre-processing techniques and comprises two methods: digital signature and digital watermarking. On the other hand, passive approach involves copy and paste techniques and includes three methods: image splicing, image retouching, and image cloning. These methods are shown in figure 1.

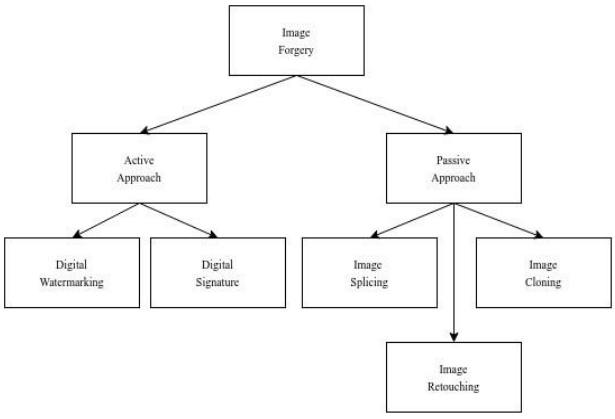

Fig 1: Methods in Image Forgery

1.1. Active Approach

The active approach is split into two ways, which are as follows:

1) Digital Watermarking: Digital watermarking refers to the process of embedding information or a mark into digital content.

*[1] *Student, Department of Computer Engineering, Ramrao Adik Institute of Technology, Dr.D.Y.Patil Deemed to be University, Nerul, Navi Mumbai, India*
[2,3] *Faculty, Department of Computer Engineering, Ramrao Adik Institute of Technology, Dr.D.Y.Patil Deemed to be University, Nerul, Navi Mumbai, India*

2) Digital Signature: A digital signature is a cryptographic method used to confirm the legitimacy and consistency of digital messages, documents, or transactions.

1.2. Passive Approach

Three different passive approaches can be used, and they are as follows:

1) Image Splicing: Image splicing refers to the act of combining parts or elements from different images to create a manipulated image.
2) Image Retouching: An image is the process of enhancing or making changes to it in order to make it look better or to fix any flaws.
3) Image Cloning: Image cloning refers to the act of duplicating or replicating specific regions or objects within an image.

2. Literature Survey

Currently, image forgery has become a criminal activity that requires control to prevent the dissemination of unauthorized and illegal content that can easily go viral. Several research papers have proposed various tools and methods aimed at detecting and preventing the use of forged images on social media platforms.

Jing Dong et al., have presented their motives, design criteria, frameworks, and self-evaluations, in addition to the CASIA Image Tempering Detection Evaluation Database. The CASIA V1.0 dataset consists of 800 real images and 921 altered images, while the CAISA V2.0 dataset has 7200 real images and 5123 altered images [1]. They made this database public so that researchers could compare and evaluate their proposed tamper detection techniques.

Yuan Rao et al., the use of a convolutional neural network (CNN) to automatically generate hierarchical representations from input RGB color photographs is a new deep learning-based technique for detecting image tampering. For applications like image splicing and copy-move detection, authors developed a 10-layer CNN [2].

Myung-Joon Kwon et al., [3] in order to concurrently learn forensic features of compression artifacts on RGB and DCT domains, we present CAT-Net, an end-to-end fully convolutional neural network that integrates RGB and DCT streams. On a range of datasets, CAT-Net scored better than current networks at localizing spliced regions in JPEG or non-JPEG images.

Achilleas Vlogiaris et al., extracted features from two datasets of varying difficulty, CASIA v2.0 and NC16, using a CNN network [4]. The SVM that was trained and tested using the retrieved features had an accuracy of 96.82% on CASIA v2.0 and 84.89% on NC16.

N. Hema Rajini, [5] splicing and copy-move forgeries were both addressed by the method for identifying picture forgeries that were provided. The model will be trained on both real and fake photos after the filtered features have been included. In order to assess whether an image has been spliced or copied, CNN is then employed. The simulation values show how well the presented model performs.

Yue Wu et al., [6] ManTra-Net is a complete DNN solution for locating image tampering. It first collects image manipulation trace features from a test image, after which it determines the degree to which a local feature deviates from its reference features to spot anomalous areas. For learning robust picture manipulation traces from 385 different forms of image manipulation, they developed a straightforward yet effective self-supervised learning task.

Teddy Surya Gunawan et al., presented the creation of a forensic JPEG picture program. The JPEG photos were examined using error level analysis to look for any alterations. A digital camera and a smartphone were used to take a total of 20 photos. The first experiment examined the association between image quality as determined by SNR, MSE, and PSNR and JPEG quality levels of 75%, 85%, and 95% [7].

Vanita Mane et al., [8] offer a uniform technique for identifying copy-move fraud. The precision and robustness were increased by combining the MIFT and Zernike algorithms. As a result, flat sections that were copied and pasted into the overall image are identified.

Vanita Mane, [9] focuses on the detection of copy-move forgeries of digital images. By reducing FPR, the main objective is to increase detection accuracy. In order to remove false matches from the detected forged region in a picture, a new window-based feature-matching technique was proposed. The outcome is an increase in performance.

Wina Permana Sari et al., To increase the accuracy of results for digital image forgery detection, ELA can be applied to CNN. For ELA 90%, the training model's accuracy averaged 0.86. The use of ELA at 10% and 50% yielded an accuracy of 0.85 and 0.84, respectively [10]. Future research will aim to provide more accurate information on the modified pixel region in image forgery detection.

E Ramadhani, [11] The ELA approach and the Laplacian method are used in research of photo splicing detection. In a photo forensics inquiry, we cannot rely solely on the ELA approach to determine whether a photo is authentic; we must additionally employ a different way to verify the outcome.

V. Aravind et al., [12] This paper presents an overview of Deep Learning-Based Digital Image Tamper Detection. They created a hybrid system that integrates error analysis with advanced neural network machine learning. In comparison to the neural network conviction model, VGG-

16 has a high level of accuracy. Convolution neural network accuracy is 85.45%, while VGG-16 accuracy is over 86.24%.

Mohit Baviskar et al., provide a comparison of various methods. The pre-trained VGG-16 and VGG-19 models, which are regarded as the best models currently available for picture forgery detection, are compared to the CNN model built from images preprocessed with the ELA approach [13].

Hitesh C Patel et al., [14] Analyzing and testing the level of forgery knowledge in digital video publishing techniques for detecting video tampering are challenging. The current system uses the mean frame comparison methodology to identify fake video frames. This method compares the means and pixels of each frame in a video data frame using an unidentified data source.

Vijayalakshmi V S et al., focuses on utilizing several classifiers to identify image splicing. The first step in finding splicing is edge detection. The subsequent stage is featuring extraction using the GLCM technique [15].

Abhishek Gupta et al., Every image in CASIA's training data is subjected to the Error Level Analysis technique in order to identify between genuine and photographs that have been altered with editing software. [16] Then, the two different classes are divided into them using a straightforward convolutional neural network.

Aditya Pandey et al., demonstrates the effectiveness of using Deep Learning/Machine Learning models in conjunction with image transformations in detecting image forgery. [17] As demonstrated by the results, the Digital Cosine Transformation is an extremely powerful tool for identifying images with a frequency anomaly.

Nor Bakiah Abd Warif et al., [18] Several methods of picture modification, including JPEG compression, image splicing, copy-move, and image retouching, were used to test the Error Level Analysis (ELA) technique. The test showed that the ELA held up well against JPEG compression, image splicing, and image fraud.

Amit Doegar et al., [19] The Random Forest machine learning technique was used to identify whether the image was fake or not, and the Google Net deep learning model was utilized to extract image attributes. Utilizing k-fold cross-validation to split the benchmark dataset MICC-F220 into training and testing datasets, the suggested strategy is applied, and it is also contrasted with state-of-the-art methodologies.

Xiuli Bi et al., [20] They suggest the ringed residual U-Net (RRUNet), an end-to-end picture essence property segmentation network that can detect forgeries without any preprocessing or postprocessing, to detect image splicing frauds.

The literature review comprises various research papers discussing topics such as error level analysis, convolutional neural network, recurrent neural network, and JPEG compression. After a thorough examination of these papers, the literature review also includes the discussion of various methods used for image forgery and their identification techniques. In the CNN method, feature extraction step is commonly used which takes time to train the model because it has to remove the redundant information of the images. With the help of ELA output, we can differentiate the original and forged images.

3. Proposed Technique

3.1. Problem Statement

Accompanying images often accompany fake news, and humans rely on them to recreate reality, as they are frequently used as evidence in news articles, books, and other documents. It can be difficult to differentiate between fake and genuine photos with the naked eye, and the audience is more inclined to accept and trust fake news that is accompanied by images. To address this issue, we aim to create a technique that can determine the authenticity of an image, whether it is real or manipulated. This approach will aid ordinary people in determining the credibility of an image.

3.2. Image Dataset

Two publicly accessible benchmark datasets for forgery detection, CASIA v1.0 and CASIA v2.0, are used in our experiment. 1,721 color images in the JPEG format with a resolution of 384 by 256 pixels can be found in the CASIA v1.0 dataset. It separated these pictures into two groups: the original set and the altered set. The bogus set has 921 photos, while the actual set includes 800. The majority of the photographs on the retail set were taken using Corel's cameras, but some images were taken using external sources [1].

Although the CASIA ITDE database V2.0 is an expanded version of database V1.0, both databases share a similar structure. 7,200 genuine photographs are included in the original set, while 5,123 altered images are included in the tampered set. However, database V2.0 is more intricate and complete than database V1.0. implemented blurring and splicing while editing the altered image set in database V2.0. Unlike V1.0, images in V2.0 are available in JPEG, BMP, and TIFF formats in a range of sizes, from 320x240 to 800x600 pixels [2].

3.3. EACN Proposed System

Error Level Analysis and Convolution Neural Network is known as EACN. The proposed EACN system is shown in Figure 2, where data input can be in either.jpg or.png format. Sections 3.4, 3.5, and 3.6, respectively, discuss the phases

of data preparation, data pre-processing, and model development.

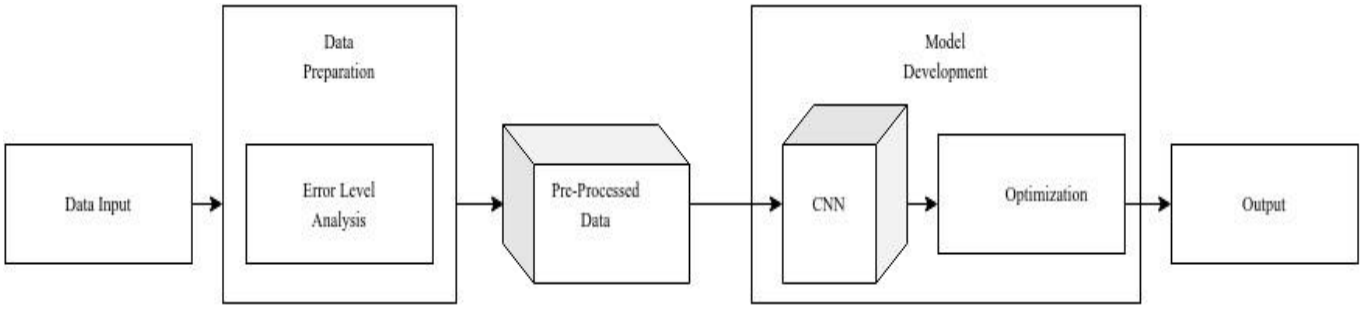

Fig 2: EACN Proposed System

3.4. Error Level Analysis (ELA)

By saving the image at a specific quality level and comparing the compression levels, the Error Level Analysis (ELA) approach is used to detect image manipulation. If the image is unaltered, the probability of errors in the 8x8 square should remain constant. However, if the image is resized, the newly added region should be more susceptible to errors than the original. ELA functions by deliberately saving images with a specific error percentage, and then measuring the differences between the saved images. [2].

In this context, the 8x8 grid generated using JPEG technology represents the compression level. The spatial and frequency domains of an image are combined via the lossy compression method known as JPEG. JPEG compression reduces the amount of data handled and undergoes sampling and RGB conversion by breaking the raw image data into 8x8 blocks. Next, a discrete cosine transform (DCT) is used to convert the image into the frequency domain. A quantization table is then used to zigzag and quantize the DCT coefficients. To make a compressed JPEG file, the quantization coefficients are compressed using entropy lossless coding.

Once a JPEG image is saved for the first time, it is subjected to its initial compression. The majority of image-editing programs, including Adobe Photoshop and other applications, support JPEG compression. As a result, if an image is opened in one of these tools, edited, and then saved again as a JPEG, it will undergo compression once again. This means that the "original" portions of the photograph have been compressed twice, once by the camera and again by Photoshop. However, it should be noted that Photoshop only applies compression once to the "altered" area of the photograph. It is difficult for humans to distinguish between these two types of compression just by looking at the image [2]. Error Level Analysis (ELA) entails recompressing an image with a preset error rate after it has already been compressed using a lossy technique. The absolute difference between the analysed image and the recompressed image is then calculated by ELA. To put it more formally, ELA can be explained as follows.

Error levels, denoted as ELA (n1, n2), using row (n1) and column (n2) indices, can be represented by,

$$\boldsymbol{ELA}(\mathbf{n1},\mathbf{n2}) = |\boldsymbol{X}(\mathbf{n1},\mathbf{n2}) - \boldsymbol{X_{rc}}(\mathbf{n1},\mathbf{n2})| \quad \text{.....} \quad (1)$$

for each color channel, where X is the image suspected of forgery and Xrc is the recompressed image. Total error levels are error levels averaged across all color channels, as in,

$$\boldsymbol{ELA}(\mathbf{n1},\mathbf{n2}) = \tfrac{\mathbf{1}}{\mathbf{3}}\textstyle\sum_{\boldsymbol{i-1}}^{\mathbf{3}} |\boldsymbol{X}(\mathbf{n1},\mathbf{n2}) - \boldsymbol{X_{rc}}(\mathbf{n1},\mathbf{n2})| \quad \text{.....} \quad (2)$$

where i = 1,2,3, for a RGB image.

3.5. Data Preprocessing

- Instead of using raw image with pixel block as input for the CNN model I decided to use Output of Error Level Analysis as an input for the CNN model.
- ELA focuses more on manipulated area of the image and it helps CNN model while extracting features for Predicting the image class.
- In this step I applied ELA method on whole CASIA v2 dataset and converted ELA result into an array, this array will act as an input into the proposed CNN model.
- The model is trained using 80% of the pre-processed data, and the model is evaluated using 20% of the pre-processed data.

3.6. Convolutional Neural Network (CNN)

In figure 4 we used pre-processed data from the previous step to build CNN (Convolutional Neural Network) model. CNNs have great power in classifying large images. Designed for image classification tasks is a convolutional neural network (CNN). Here's a breakdown of the layers and operations in the model:

Using the ReLU activation function, the first layer is a Conv2D layer with 32 filters, each with a kernel size of 4x4. The input shape of the images is (128, 128, 3), which means the images have a height and width of 128 pixels and 3 color channels (RGB). This layer applies convolution to the input image to extract features.

The next is maxpooling with a pool size of 2x2. This layer downsamples the output of the convolutional layer by taking the maximum value of each 2x2 window, lowering the output's spatial dimensions.

Then another Conv2D layer with 64 filters and a kernel size of 4x4, using the ReLU activation function. This layer continues to extract higher-level features from the downsampled output of the previous layer. Next is another maxpooling with a pool size of 2x2, further lowering the output's spatial dimensions.

The last Conv2D layer with 128 filters and a kernel size of 4x4, using the ReLU activation function. This layer continues to extract even higher-level features from the down sampled output of the previous layer. Once more, max pooling with a 2x2 pool size reduces the output's spatial dimensions.

Next layer is a GlobalAveragePooling2D layer, which averages each feature map in the output of the previous layer into a single value. As a result, the model's parameter count is decreased, and the output is ready for the final classification layers. The Dense layer, which has 64 units, is followed by the ReLU activation function. This layer applies a fully connected neural network to the output of the previous layer, allowing the model to learn non-linear relationships between the extracted features.

Another dense layer with two units and the softmax activation function makes up the final layer. This layer applies another fully connected neural network to the output of the previous layer and produces a probability distribution over the two possible classes.

Because the results of the conversion procedure into ELA images can highlight crucial elements to evaluate whether an image is original or has been carefully edited therefore, only three convolutional layers are required in the architecture utilized.

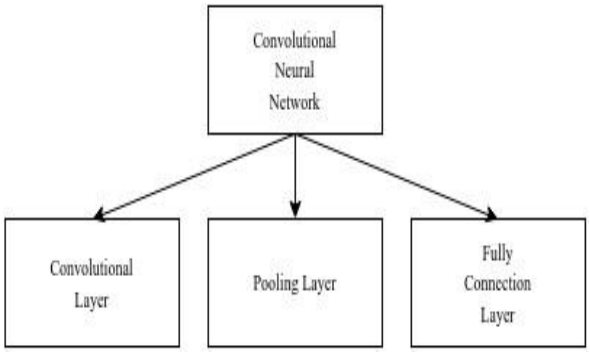

Fig 3: Layers in CNN

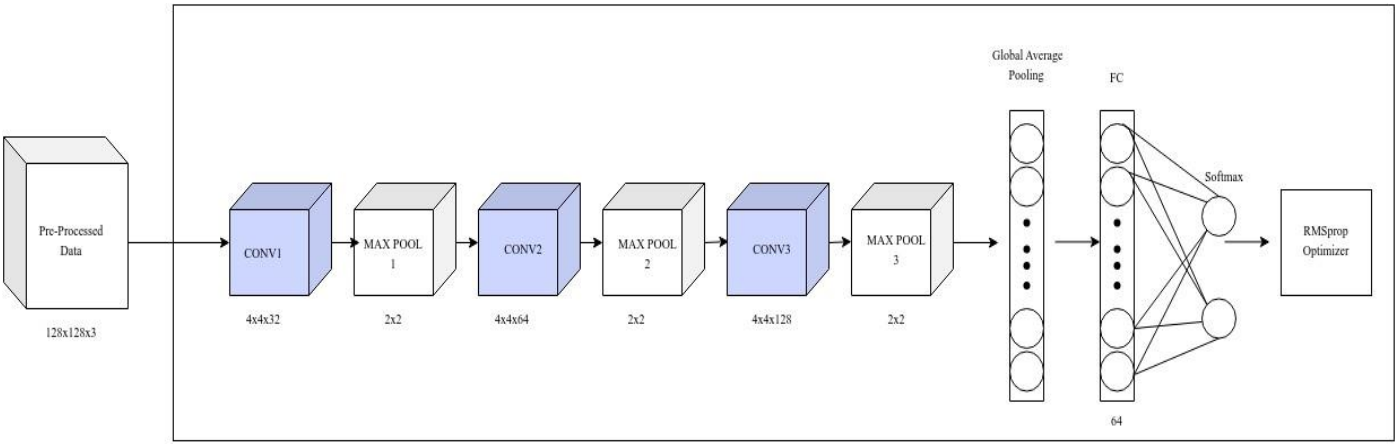

Fig 4: Architecture of CNN Model Development

3.7. Model Optimization

The optimizer is an algorithm that determines how the model weights are updated during training in order to minimize the loss function. In this example, the optimizer being used is RMSprop.

RMSprop is a popular optimization algorithm for deep learning models. It uses a moving average of squared gradients to scale the learning rate for each weight in the model, which can help to prevent the learning rate from becoming too large or too small. The learning rate parameter sets the initial learning rate for the optimizer, and rho controls the smoothing factor for the moving average. The epsilon parameter is used to prevent division by zero, and decay controls the learning rate decay over time.

3.8. Evaluation Metrics

The primary goal of image splicing forgery detection is to precisely find the altered pixels. The number of successfully detected tampered pixels (TP), wrongly detected tampered

pixels (FP), and incorrectly detected un-tampered pixels (FN) is used to assess the efficacy of this detection. It is usual practice to assess the effectiveness of splicing forgery detection systems at the pixel level using precision, recall, and F-measure. Recall evaluates the likelihood that the tampered regions in the ground-truth image will be accurately detected, whereas Precision measures the likelihood that the discovered regions are indeed tampered regions. F-measure is a combination of Precision and Recall that provides an overall evaluation of the detection method's performance. The mean values of the testing set in the experiments are used to determine the Precision, Recall, and F-measure values. This assessment aids in determining the precision and potency of the splicing forgery detection techniques.

$$\boldsymbol{Accuracy} = \frac{\boldsymbol{TP+TN}}{\boldsymbol{T_{Total\_Images}}} \times \mathbf{100} \quad \ldots\ldots (3)$$

$$\boldsymbol{Precision} = \frac{\boldsymbol{TP}}{\boldsymbol{TP+FP}} \quad \ldots\ldots (4)$$

$$\boldsymbol{Recall} = \frac{\boldsymbol{TP}}{\boldsymbol{TP+FN}} \quad \ldots\ldots (5)$$

$$\boldsymbol{F-Measure} = \frac{\boldsymbol{2 \times Precision \times Recall}}{\boldsymbol{Precision+Recall}} \ldots\ldots (6)$$

4. Results And Discussion

Table 1 displays the image forgery detection accuracies attained by various techniques, including our proposed method, on the CASIA 2.0 database. The outcomes show that the proposed technique performs better in terms of accuracy than the other techniques. The main goal of the suggested method is to determine whether an image is real or altered. The utilization of the feature image, which is created by figuring out the difference between the original image and its recompressed counterpart, is what gives our proposed technique its improved performance. This approach is more effective in detecting image forgery as the forged parts are more pronounced in the feature image. Consequently, the proposed technique achieves a higher accuracy rate of 92.10%, highlighting its effectiveness in accurately detecting image forgery.

Table 1. Accuracy comparison of the proposed technique with other techniques on CASIA.

Technique	Accuracy	Precision	Recall	F-measure
RRUNet [20]	76	0.84	0.83	0.84
Mantra-Net [6]	56.14	0.48	0.79	0.59
CAT-Net [3]	87.29	0.62	0.87	0.72
EACN Proposed System	**92.10**	**0.84**	**0.99**	**0.91**

The graph's numbers represent each technique's performance in terms of accuracy, precision, recall, and F-measure. When the methods are compared, it is clear that our suggested approach, EACN, gets the best accuracy of 92.10%. It also demonstrates high precision (0.84), recall (0.99), and F-measure (0.91), indicating its effectiveness in detecting and identifying forged images while minimizing false positives and false negatives.

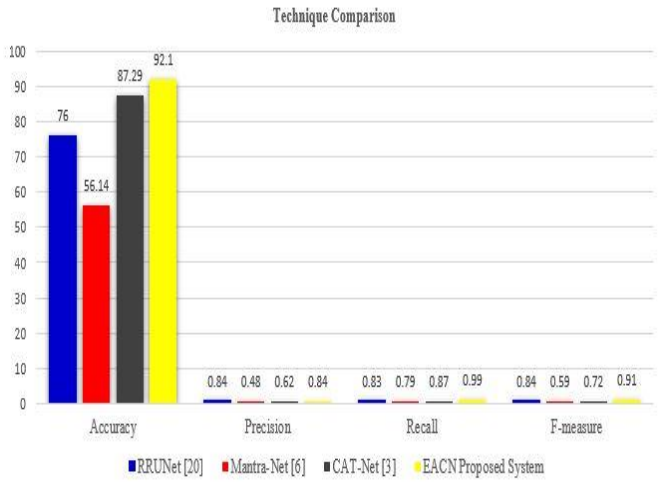

Fig 5: Technique Comparison of All Model

Table 2. Comparison of the time taken to process single image by the proposed technique with other techniques on CASIA 2.0 database (displayed values are in milliseconds).

Technique	Time Taken
Mantra-Net [6]	10927
CAT-Net [3]	2506
EACN Proposed System	**39**

To assess the effectiveness of the proposed technique, I conducted an evaluation using the popular CASIA2.0 image forgery database. The database contains 12,617 photos in the BMP, JPG, and TIF formats, 7,493 of which are real and 5,124 of which have been altered. The resolution of the photo's ranges from 800 × 600 to 384 * 256 pixels. A computer with an Intel(R) Core (TM) i5-8250U CPU running at 1.6 GHz and 8 GB of RAM was used to carry out the experiment. The evaluation's goal was to ascertain how effective the strategy was.

We randomly divided the CASIA 2.0 database into two sets: 80% for training and 20% for testing in order to evaluate our model. For training, we used 80% of the photos and an RMSprop optimizer with a batch size of 40 and an initial learning rate of 0.0005. The remaining 20% of the photographs were used to test the suggested method and

evaluate it against other frameworks already in use. Several figures were used to analyze the results. Figures 6 and 7 demonstrate the train and test loss and the model's accuracy during training and testing, respectively. The maximum accuracy, greater than 92%, was achieved at the 10th epoch due to a smaller number of parameters and convolutional layers, allowing for convergence in less than 10 epochs. Finally, Figure 9 shows the ROC AUC score with an area under the curve of 93.10%, Figure 8 is the confusion matrix.

In Figure 6 the graph of training loss and validation loss shows both curves decreasing during training, indicating effective learning. Additionally, the model is not overfitting as the training loss and validation loss decreases significantly. Monitoring these curves helps optimize the model and achieve a balance between training and generalization performance.

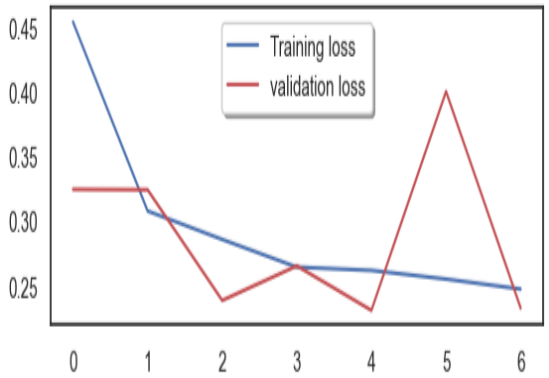

Fig 6: Training Loss and Validation Loss

The Figure 7 shows graph of training accuracy and validation accuracy reveals that both curves increase during training, indicating effective learning. Furthermore, the model is not overfitting as the training accuracy consistently improves, while the validation accuracy remains comparable or slightly lower. Monitoring these curves aids in optimizing the model and ensuring a balance between accuracy and generalization.

Fig 7: Training Accuracy and Validation Summary

The confusion matrix Figure 8 provides valuable insights into the model's performance. With 1276 true positives, it correctly identifies genuine images. However, there are 214 false positives, indicating instances where manipulated images are incorrectly classified as genuine. The model exhibits excellent performance in detecting manipulated images with only 8 false negatives, while correctly identifying 1014 true negatives as forged images.

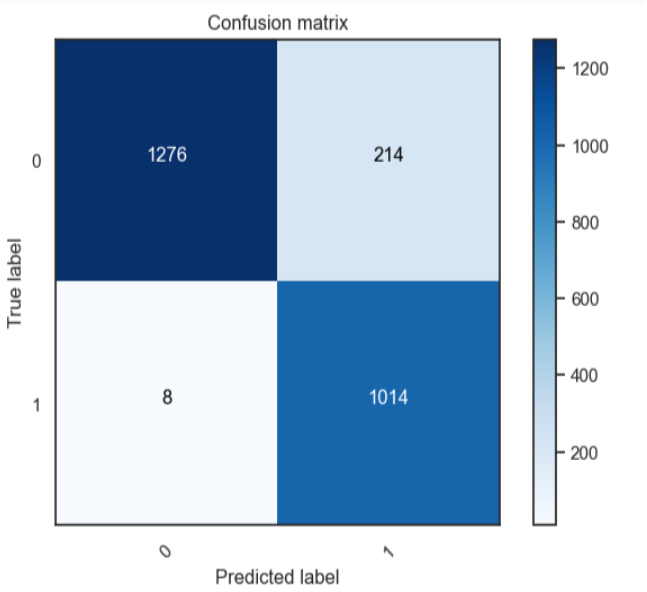

Fig 8: Confusion Matrix

A metric used to assess the effectiveness of a classification model is the ROC AUC Figure 9 score. Having an AUC (area under the curve) of 93.10%), it indicates a strong ability of the model to distinguish between positive and negative classes. A higher AUC suggests better discrimination power and predictive accuracy.

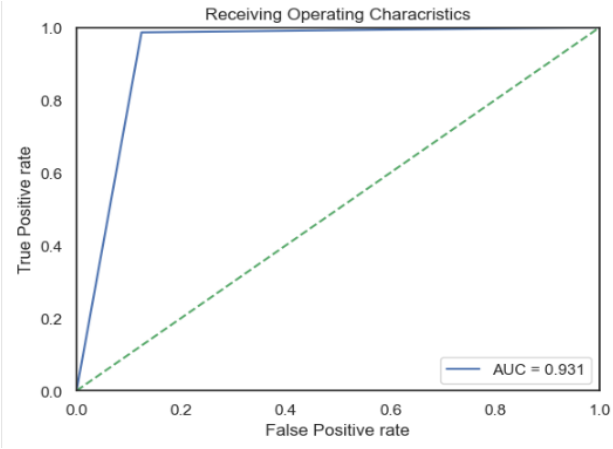

Fig 9: ROC AUC CURVE

5. Conclusion

The challenge of detecting electronic forgery in digital forensics highlights the need for suitable techniques to

identify fake images. To address this challenge, proposed a method that utilizes Error Level Analysis (ELA) and deep learning to determine the authenticity of digital images. This method seeks to increase the precision of identifying false images by adding ELA into the convolutional neural network. The experimental results showed a validation accuracy of 92.10% with a 98% compression rate in ELA. Moreover, the processing time for a single image was approximately 50ms on standard hardware. This proposed method can be a valuable tool in various fields, including social media and digital forensics, for identifying and preventing image forgery.

Additionally, picture forgery localization can be added to the suggested technique in the future. This method can be used in conjunction with other established image localization techniques to improve accuracy while lowering time complexity. The current approach requires a minimum image resolution of 128*128, but it can be further improved to work on even smaller images.

6. References and Footnotes

Acknowledgements

I would like to thank our guide and mentor Dr. Vanita Mane and co-guide Mrs. Namita Pulgam for the topic "Image Manipulation Detection Using Error Level Analysis and Deep Learning " who mentored us throughout and cleared the concepts and helped us understand all the topics. I would also like to thank the Head of the Department Dr. A. V. Vidhate for giving us an opportunity to understand and implement this project. I want to express my gratitude to the principle, Prof. Dr. Mukesh Patil, for providing us with all the resources and tools needed for this project.

Author contributions

Prajakta Kubal: Developed, designed, and executed the algorithm and experiments, including significant adjustments to the parameters utilized in the study. **Dr. Vanita Mane:** Designed CNN model with the smaller number of convolutional layers as compared to the existing approaches by other authors. **Prof. Namita Pulgam:** proposed model has less trainable parameters as compared to other models, with the help of this we can reduce the computational cost and my proposed model can work on commodity hardware. Experimented proposed model on CASIA V2 data set.

Conflicts of interest

The authors declare no conflicts of interest.

References

[1] Jing Dong, Wei Wang and Tieniu Tan, "Casia Image Tampering Detection Evaluation Database", 978-1-4799-1043-4/13/2013 IEEE.

[2] Yuan Rao, Jiangqun Ni, "A Deep Learning Approach to Detection of Splicing and Copy-Move Forgeries in Images", 978-1-5090-1138-4/16/2016 IEEE.

[3] Myung-Joon Kwon, In-Jae Yu, Seung-Hun Nam, and Heung-Kyu Lee, "CAT-Net: Compression Artifact Tracing Network for Detection and Localization of Image Splicing",78-1-6654-0477-8/20/2021IEEE/DOI:10.1109/WACV48630.2021.00042.

[4] Achilleas Vlogiaris, Arkajit Bhattacharya, Kyriakos Psarakis, Panagiotis Soilis, Rafail Skoulos, "Image Forgery Detection CS4180 Deep Learning - Group 10".

[5] N. Hema Rajini, "Image Forgery Identification using Convolution Neural Network", ISSN: 2277-3878, Volume-8, Issue-1S4, June 2019.

[6] Yue Wu, Wael Abd Almageed, and Premkumar Natarajan, "ManTra-Net: Manipulation Tracing Network for Detection and Localization of Image Forgeries with Anomalous Features", DOI 10.1109/CVPR.2019.00977.

[7] Teddy Surya Gunawan, Siti Amalina Mohammad Hanafiah, Mira Kartiwi, Nanang Ismail, Nor Farahidah Za'bah, Anis Nurashikin Nordin, "Development of Photo Forensics Algorithm by Detecting Photoshop Manipulation Using Error Level Analysis", Vol. 7, No. 1, July 2017, DOI: 10.11591/ijeecs. v7. i1. pp131-137.

[8] Vanita Mane and Subhash Shinde, "An Integrated Copy-Move Forensic Method for Tamper Detection and Localization of Duplicated Regions", DOI: 10.5769/J201801003.

[9] Vanita Mane, "Copy-Move Forgery Detection of Digital Images using Window Based Feature Matching Approach".

[10] Wina Permana Sari, Hisyam Fahmi, "The effect of error level analysis on the image forgery detection using deep learning", Vol. 6, No. 3, August 2021, Pp. 187-194, https://doi.org/10.22219/kinetik.v6i3.1272.

[11] E Ramadhani, "Photo splicing detection using error level analysis and laplacian-edge detection plugin on GIMP", doi:10.1088/1742-6596/1193/1/012013.

[12] V.Aravinda, V. Durga Prasada, S. Swathia, Y.V.S Kalyana, U. Sandhyaa, R. Cristin, "Survey on Digital Image Tamper Detection Using Deep Learning Algorithms", Vol 3, no 4, pp 24-29, May 2022.

[13] Mohit Baviskar, Sheetal Rathod, Jay Lohokare, "A Comparative Analysis of Image Forgery Detection Techniques", DOI: 10.1109/IC3SIS54991.2022.9885600.

[14] Hitesh C Patel, Mohit M Patel, "An Improvement of Forgery Video Detection Technique using Error Level Analysis", Volume 111 – No 15, February 2015.

[15] Vijayalakshmi V S, Shwetha B, Dr. S V Sathyanarayana, "Image Classifier based Digital Image Forensic Detection-A Review and Simulations", Computer Science and Technology – 2015.

[16] Abhishek Gupta, Raunak Joshi, Ronald Laban, "Detection of Tool Based Edited Images from Error Level Analysis and Convolutional Neural Network".

[17] Aditya Pandey, Anshuman Mitra, "Detecting and Localizing Copy-Move and Image-Splicing Forgery".

[18] Nor Bakiah Abd Warif, Mohd. Yamani Idna Idris, Ainuddin Wahid Abdul Wahab, Rosli Salleh, "An Evaluation of Error Level Analysis in Image Forensic", 978-1-4673-6713-4/15/2015 IEEE.

[19] Amit Doegar, Maitreyee Dutta, Gaurav Kumar, "Image Forgery Detection Using Google Net and Random Forest Machine Learning Algorithm", D.O.I - 10.51201/12508.

[20] Xiuli Bi, Yang Wei, Bin Xiao, Weisheng Li, "RRU-Net: The Ringed Residual U-Net for Image Splicing Forgery Detection".

[21] C. S., S., Kunju, N. ., & Shahul Hameed, T. A. . (2023). Design and Simulation of Two Stage Wideband CMOS Amplifier in 90 NM Technology. International Journal on Recent and Innovation Trends in Computing and Communication, 11(2s), 249–258. https://doi.org/10.17762/ijritcc.v11i2s.6144

[22] Thompson, A., Walker, A., Fernández, C., González, J., & Perez, A. Enhancing Engineering Decision Making with Machine Learning Algorithms. Kuwait Journal of Machine Learning, 1(2). Retrieved from http://kuwaitjournals.com/index.php/kjml/article/view/127

[23] Suspicious activity detection and classification in IoT environment using machine learning approach. Paper presented at the PDGC 2022 - 2022 7th International Conference on Parallel, Distributed and Grid Computing, 531-535. doi:10.1109/PDGC56933.2022.10053312 Retrieved from www.scopus.com