INTERNATIONAL SCIENTIFIC JOURNAL OF ENGINEERING AND MANAGEMENT (ISJEM) ISSN: 2583-6129
CONFERENCE PROCEEDINGS: VOLUME: 05 ACME – 2026 DOI: 10.55041/ISJEM.ACME111
AN INTERNATIONAL SCHOLARLY || MULTIDISCIPLINARY || OPEN ACCESS || INDEXING IN ALL MAJOR DATABASE & METADATA

A Hybrid Deep Learning Framework for Digital Image Forgery Detection using Error Level Analysis and Grey Wolf Optimized Resnet50 Features

Dr. P. Harish M. Tech, ph. D
Department of Electronics and Communication Engineering
Annamacharya Institute of Technology & Sciences, Tirupathi, India
harishpasupulati.aits@gmail.com

Kaveti Sai Ram
Department of Electronics and Communication Engineering
Annamacharya Institute of Technology & Sciences, Tirupathi, India
Sram82445@gmail.com

M Radhika
Department of Electronics and Communication Engineering
Annamacharya Institute of Technology & Sciences, Tirupathi, India
radhikamudumuku1@gmail.com

Shaik Saad Ahamed
Department of Electronics and Communication Engineering
Annamacharya Institute of Technology & Sciences, Tirupathi
saadbaby960@gmail.com

M Muneeswar
Department of Electronics and Communication Engineering
Annamacharya Institute of Technology & Sciences,Tirupathi,
balu1muppala@gmail.com

Abstract— *Digital image manipulation has become increasingly common due to the availability of advanced editing tools, creating a need for reliable forgery detection techniques. This work proposes a hybrid framework for detecting tampered images by integrating image preprocessing, forensic analysis, deep feature extraction, and optimization techniques. Initially, the input image undergoes preprocessing using a median filter and anisotropic diffusion filter to reduce noise while preserving edge information. Error Level Analysis (ELA) is then applied to highlight compression inconsistencies that may indicate image manipulation. Deep features are extracted from the ELA-enhanced images using the Resnet50 model. To improve feature relevance and reduce redundancy, Grey Wolf Optimization (GWO) is employed to select the most informative features from the extracted deep feature set. The optimized feature vectors are then classified using a Softmax-based classifier to determine whether the image is authentic or tampered. The proposed hybrid approach combines image processing, deep learning, and optimization techniques to enhance the robustness and accuracy of image forgery detection. Experimental results demonstrate that the method effectively distinguishes between authentic and manipulated images, providing a reliable framework for digital image authentication. The proposed approach was evaluated using a dataset comprising 800 images from the Kaggle database. The dataset was split into 60% for training and 40% for testing purposes. The system is simple to implement in MATLAB R2025b and can assist in digital forensics and media authentication applications.*

Keywords— Digital Image Forgery Detection, Error Level Analysis (ELA), ResNet50, Grey Wolf Optimization (GWO), Deep Learning, Feature Extraction, Softmax Classifier.

I. INTRODUCTION

Digital images have become one of the most widely used forms of information in modern communication systems. With the rapid growth of smartphones, digital cameras, and social media platforms, images are continuously captured, stored, and shared across various digital platforms. With the advancement of

powerful image editing software, modifying digital images has become simple and accessible. Users can easily insert, remove, or alter objects in an image, creating manipulated images that often appear visually realistic. Such alterations can mislead viewers, spread false information, or produce fabricated evidence. Therefore, verifying the authenticity of digital images has become a critical task in the field of digital image forensics.

Conventional image forgery detection techniques mainly depend on handcrafted feature extraction and statistical analysis methods. Although these approaches can identify certain manipulation patterns, their performance is often limited when dealing with complex or sophisticated image editing operations. In recent years, deep learning methods have demonstrated strong capabilities in image analysis tasks because they can automatically learn meaningful and hierarchical features directly from image data.

In this study, a hybrid framework for digital image forgery detection is proposed by integrating image preprocessing, Error Level Analysis (ELA), deep feature extraction using the ResNet50 model, and feature optimization through Grey Wolf Optimization (GWO). Initially, preprocessing techniques are applied to improve image quality and enhance overall visual clarity for analysis. ELA is then used to reveal compression inconsistencies that may indicate image tampering. The ResNet50 network extracts deep features from the processed images, and GWO selects the most relevant features from the extracted feature set. Finally, a Softmax classifier determines whether the input image is authentic or manipulated. Experimental evaluation demonstrates that the proposed method provides effective and reliable detection of digital image manipulation.

II. LITERATURE SURVEY

2.1 Related Works

Digital image forgery detection has become an important research topic in the field of digital image processing and multimedia forensics. With the increasing availability of image editing software, it has become easy to manipulate digital images in a realistic way. As a result, several techniques have been developed to detect image manipulation and verify the authenticity of digital images. These techniques generally rely on analyzing inconsistencies in image properties such as texture, compression artifacts, lighting conditions, and statistical features.

Ramesh Gorle and Anitha Guttavelli (2025) proposed an image tampering detection method that combines Error Level Analysis (ELA) with Convolutional Neural Networks (CNN). In their approach, ELA is used to highlight compression artifacts in images, and the processed images are fed into a CNN model for classification. The model was evaluated using the CASIA v2.0 dataset and achieved an accuracy of approximately 96.21%, demonstrating the effectiveness of combining ELA with deep learning techniques.

A. M. Nagm, M. Moussa, and R. Shoitan (2024) introduced a deep learning framework for detecting manipulated images using ELA and CNN models. Their system first generates ELA images to reveal compression differences and then uses a CNN architecture to extract spatial and texture features. The experimental results showed a testing accuracy of about 94.14%, indicating that deep learning-based feature extraction can improve image manipulation detection.

Nazrin et al. (2023) developed an image forgery detection system by combining Error Level Analysis with deep CNN architectures such as VGG16 and MesoNet. The ELA images are used as inputs to the deep learning models, which automatically extract manipulation-related features. The proposed approach achieved an accuracy of approximately 92.7%, highlighting the capability of deep CNN models in detecting forged images.

Nalluri Brahma Naidu, Thokala Kavyasree, and Ravi Teja (2024) proposed a forgery detection framework based on the ResNet50 deep learning architecture. Their method uses ELA preprocessing followed by deep feature extraction using ResNet50 to classify images as authentic or manipulated. The study demonstrated that residual networks can effectively capture hierarchical features that help identify image manipulation.

In the paper titled “Copy-Move and Image Splicing Forgery Detection using Convolutional Neural Networks”, authored Li Lin, Jian Zhao, and Xiaofei Wang in year 2022.This research focuses on detecting two common types of image forgery: copy-move and image splicing. The methodology uses a CNN-based deep learning model combined with image preprocessing techniques. First, images are processed to identify manipulation artifacts and inconsistencies.

The processed images are then used to train the CNN model. The CNN automatically extracts features such as edges, textures, and color patterns from the images. The dataset used includes CASIA and Columbia image splicing datasets. The CNN model achieved high accuracy in detecting manipulated images. The output of the system includes classification results and identification of suspicious regions. The authors concluded that deep learning models outperform traditional feature-based methods for image forgery detection.

Although these existing approaches have achieved promising results, many of them still face challenges such as redundant feature extraction and higher computational complexity. Therefore, integrating deep feature extraction with feature optimization techniques can further improve detection performance. In this work, a hybrid framework combining Error Level Analysis, ResNet50 feature extraction, and Grey Wolf Optimization is proposed to enhance the accuracy and efficiency of digital image forgery detection.

III. METHODOLOGY

The proposed system introduces a hybrid deep learning framework for detecting digital image forgery by integrating image preprocessing, forensic analysis, deep feature extraction, and feature optimization techniques. The overall workflow of the proposed method consists of several stages, including image preprocessing, Error Level Analysis (ELA), deep feature extraction using the ResNet50 model, feature optimization using Grey Wolf Optimization (GWO), and classification using a Softmax classifier.

3.1 Image Preprocessing

Image preprocessing is the first stage of the proposed system. The main purpose of preprocessing is to improve the quality of the input image and remove unwanted noise that may affect the performance of the detection model. Noise present in the image can distort important features and reduce the effectiveness of feature extraction algorithms. Therefore, preprocessing is performed using two filtering techniques:

3.1.1 Median Filter

Median filtering is a nonlinear filtering technique used to remove impulse noise (salt-and-pepper noise) from digital images. Instead of averaging pixel values like a mean filter, the median filter replaces the central pixel value with the median value of neighboring pixels. This approach effectively removes noise while preserving important edges in the image.

$$I'(x,y) = median\{I(i,j)\}$$

Where:

- $I(X,Y)$Yrepresents the original image pixel
- $I'(x,y)$represents the filtered image pixel
- I(i,j)represents neighboring pixel values

3.1.2 Anisotropic Filter

Anisotropic diffusion filtering is applied after median filtering to further smooth the image while preserving structural details. Unlike traditional smoothing filters, anisotropic diffusion reduces noise without blurring important edges. This technique works by performing diffusion in homogeneous regions while limiting diffusion near edges.

$$\frac{\partial I}{\partial t} = div(c(x,y,t)\nabla I)$$

Where:

- Irepresents the image intensity
- $t$represents the diffusion time
- c(x,y,t)represents the diffusion coefficient

Fig 3.1 (a) Original images, (c) Median Anisotropic Hybrid filter images

3.2 Error Level Analysis (ELA)

Error Level Analysis is a digital image forensic technique used to identify potential tampered regions in JPEG images. JPEG compression introduces uniform compression artifacts across the image. However, when an image is edited and saved again, the manipulated areas may exhibit different compression levels. ELA detects these inconsistencies

by recompressing the image and analyzing the difference between the original and recompressed images.

3.2.1 Image Recompression

The input image is recompressed at a predefined JPEG quality level. This step helps identify variations in compression artifacts that may occur due to image manipulation. The image is saved again at a fixed compression level. Compression artifacts are introduced uniformly.

3.2.2 Difference Calculation

The difference between the original image and the recompressed image is calculated to highlight potential manipulation areas. Regions with higher differences appear brighter in the ELA image, indicating possible inconsistencies. These highlighted areas help in identifying suspicious regions that may have been tampered or edited.

$$ELA = | I_{original} - I_{recompressed} |$$

Where:

- $I_{original}$ represents the original image
- $I_{recompressed}$ represents the recompressed image

Fig 3.2 ELA Map Generated images

3.3 Deep Feature Extraction using ResNet50

Once the ELA map is generated, deep feature extraction is performed using the ResNet50 deep convolutional neural network. ResNet50 is a residual network consisting of 50 layers that utilizes skip connections to overcome the vanishing gradient problem and improve feature learning. The ELA images are used as input to the ResNet50 model, which automatically extracts hierarchical features such as edges, textures, and structural patterns. The output of the global average pooling layer produces a 2048-dimensional feature vector representing the image characteristics.

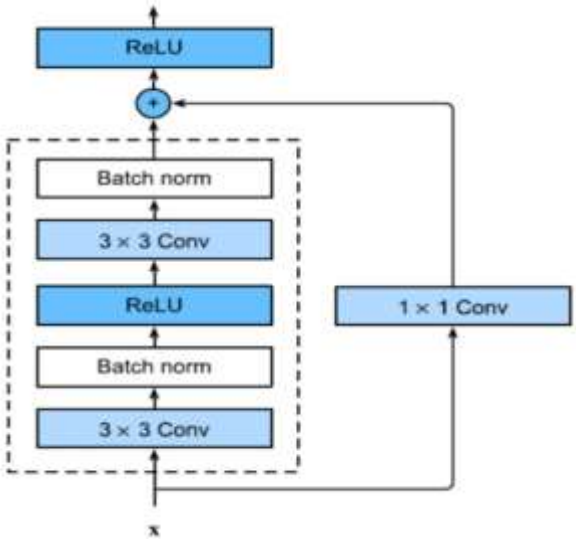


Fig 3.3 Architecture of ResNet50

3.4 Feature Optimization using Grey Wolf Optimization

Although the extracted deep features contain important information, some of them may be redundant or irrelevant for classification. To address this issue, Grey Wolf Optimization (GWO) is used for feature selection. GWO is a nature-inspired optimization algorithm that simulates the hunting behavior and leadership hierarchy of grey wolves. The algorithm identifies the most informative features by iteratively updating candidate solutions and selecting the optimal subset of features. In the proposed system, the feature vector is reduced from 2048 features to 100 optimized features.

3.5 Classification using Softmax Classifier

Finally, the optimized feature set is provided to a Softmax classifier for final decision making. The Softmax classifier converts the input feature values into probability scores for each class and assigns the class label with the highest probability. In this framework, the classifier determines whether the input image belongs to one of two categories: authentic image or tampered image. The integration of deep feature extraction and optimization techniques improves the accuracy and reliability of digital image forgery detection.

Softmax Probability Function

$$p(y = i|x) = \frac{e^{z_i}}{\sum_i^k e^{z_j}}$$

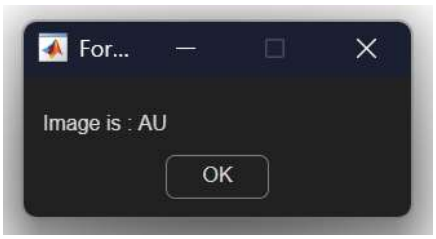
Where:

- z_i represents the input score for class i
- k represents the total number of classes

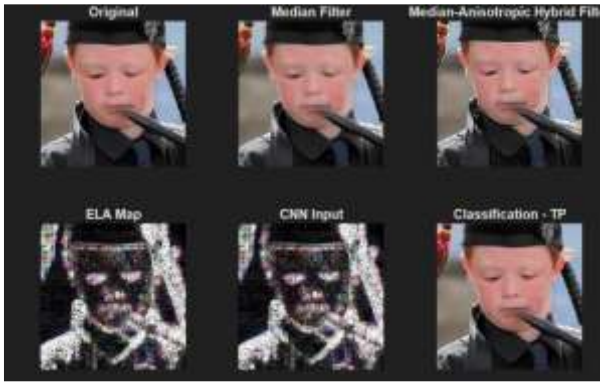
Classification Output

The classifier assigns the image to one of the following classes:

- Real Image
- Fake Image



(a)



(b)

Fig 3.5 (a),(b) are the outputs of Proposed Methodology

IV. RESULT AND DISCUSSION

4.1 Result

- The proposed hybrid deep learning framework was evaluated using 800 images from the Kaggle dataset, with 60% used for training and 40% for testing.
- The confusion matrix shows the performance of the classification model by comparing the actual class labels with the predicted class labels.
- In this matrix, 154 authentic images and 156 tampered images are correctly classified, while 6 authentic images and 4 tampered images are incorrectly classified.

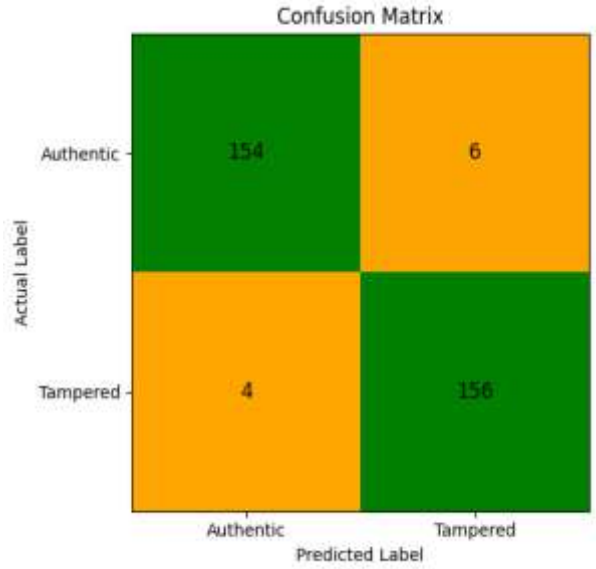


Fig 4.1 Confusion Matrix For a Hybrid Deep Learning Framework For Digital Image Forgery Detection

4.2 Performance Calculations

From the confusion matrix, various parameters are calculated to analyse the efficiency of the presented method. Figure 4.1 Shows the parameter variations in the proposed method.The proposed algorithm model is evaluated against other algorithms, demonstrating superior performance compared to the alternatives. Table 4.1 shows the parameters and their values. Fig

4.2 shows the bar graph for performance indicators for proposed algorithm. Table 4.2 Indicates the relativity of the proposed method with other methods. Fig.4.3 shows the correlation of the proposed method with other methods.

Table 4.1 Performance Metrics

Parameter	Value(%)
Sensitivity	97.50
Specificity	96.25
Accuracy	96.88
Precision	96.29
Fl score	96.89
NPV	97.47
FDR	3.70
FPR	2.5

Formulae:

Sensitivity: TPR = TP/(TP+FN)
Specificity: SPC = TN/(FP+TN)
Accuracy: ACC = (TP+TN)/(P+N)
Precision: PPV = TP/(TP + FP)
Fl Score: F1 = 2TP/(2TP+FP+FN)
False Discovery Rate: FDR = FP/(FP+TP)
False Positive Rate: FPR = FP/(FP+TN)
Negative Predictive Value: NPV = TN/(TN+FN)
False Negative Rate: FNR = FN/(FN+TP)

Fig 4.2 Performance Indicators for Proposed Algorithm

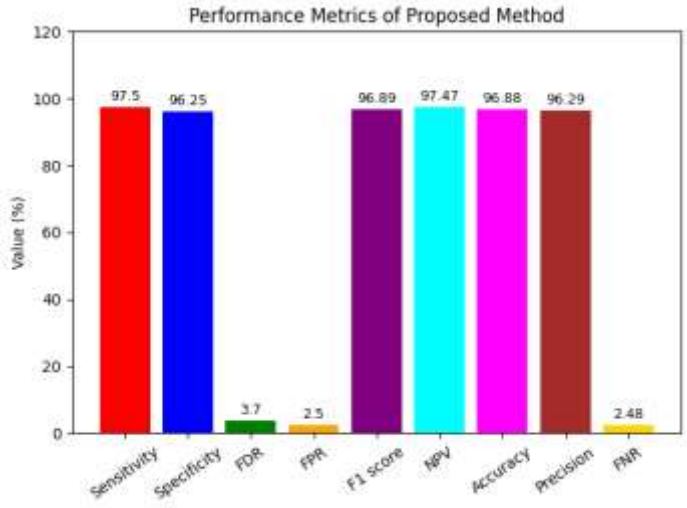


Table: 4.2 Relativity of the proposed method

Author	Year	Methods Used	Accuracy (%)
Ramesh Gorle and Anitha Guttavelli	2025	ELA + CNN	95.21
A. M. Nagm, M. Moussa, and R. Shoitan	2024	ELA + Deep CNN	94.14
Nazrin et al.	2023	ELA+ VGG16 and MesoNet CNN Models	92.7
Proposed Method		ELA + ResNet50 Feature Extraction + GWO	96.88

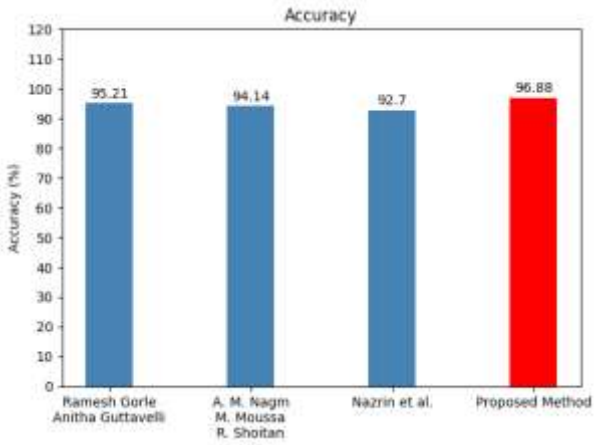


Fig 4.3 Comparison of proposed method

V. CONCLUSION

. In this work, a hybrid deep learning framework for digital image forgery detection was proposed by integrating image preprocessing, Error Level Analysis (ELA), deep feature extraction using the ResNet50 model, and feature optimization through Grey Wolf Optimization (GWO). The preprocessing stage improves image quality, while ELA highlights compression inconsistencies that may indicate image manipulation. ResNet50 extracts meaningful deep features from the processed images, and GWO selects the most relevant features to improve classification performance. The optimized feature set is then classified using a Softmax classifier to determine whether the image is authentic or tampered.

The proposed approach was evaluated using a dataset of 800 images collected from the Kaggle database. The dataset was divided into 60% for training and 40% for

testing to evaluate the performance of the model. Experimental results show that the proposed method achieved an accuracy of 96.88%, demonstrating its effectiveness in distinguishing between authentic and manipulated images. The obtained results indicate that the proposed framework provides a reliable and efficient solution for digital image forgery detection.

VI. REFERENCES

[1] Ramesh Gorle and Anitha Guttavelli (2025) proposed an image forgery detection framework using Error Level Analysis and Convolutional Neural Networks. The system highlights compression artifacts using ELA and classifies images using CNN, achieving 9521% accuracy on the CASIA v2.0 dataset.

[2] A. M. Nagm, M. Moussa, and R. Shoitan (2024) presented a deep learning approach combining ELA and CNN for detecting manipulated images. The CNN extracts texture and spatial features from ELA images and achieved 94.14% testing accuracy.

[3] Nazrin et al. (2023) developed a forgery detection system using ELA with deep CNN models such as VGG16 and MesoNet. Their method achieved 92.7% accuracy, demonstrating the effectiveness of ELA-based preprocessing.

[4] Nalluri Brahma Naidu, Thokala Kavyasree, and Ravi Teja (2024) proposed a forgery detection model using ResNet50 with ELA preprocessing. The deep residual network extracts hierarchical features to classify images as authentic or tampered.

[5] Li Lin, Jian Zhao, and Xiaofei Wang (2022) focused on detecting copy-move and image splicing forgeries using CNN. Their deep learning model extracts texture and edge features to accurately identify manipulated regions.

[6] Sukhmani Kaur, Nityaa Sinha, and Priyasha Jain (2024) proposed a hybrid system combining CNN for feature extraction and XGBoost for classification. The model achieved 96.82% accuracy on CASIA datasets.

[7] G. Anvesh Reddy and G. Srikanth Reddy (2025) developed a CNN-based digital image forgery detection system that learns manipulation patterns automatically from image data, achieving about 92% validation accuracy.

[8] Kaur and Singh (2022) proposed a transfer learning approach using the VGG16 architecture to detect image forgery. The model extracts deep features and achieved 92% detection accuracy. [9] Shelar and Patil (2023) introduced a hybrid CNN-LSTM model where CNN extracts spatial features and LSTM analyzes sequential patterns. The model achieved approximately 93% detection accuracy.

[9] Shelar and Patil (2023) introduced a hybrid CNN-LSTM model where CNN extracts spatial features and LSTM analyzes sequential patterns. The model achieved approximately 93% detection accuracy.

[10] Wu and Zhou (2022) proposed a multi-scale CNN architecture that analyzes images at multiple resolutions to detect subtle manipulation artifacts, achieving around 91% accuracy.

[11] Zhang and Li (2023) developed a forgery detection method using Residual Neural Networks (ResNet) to extract deep hierarchical features from images, achieving 94% detection accuracy.

[12] Kim and Park (2022) proposed a deep learning based image authentication system using CNN models. The network detects compression artifacts and texture inconsistencies to identify manipulated images.

[13] Chen and Liu (2023) introduced a feature fusion CNN model that combines multiple image features such as texture, color, and compression artifacts to improve forgery detection performance.

[14] Sharma and Gupta (2024) proposed an ELA-CNN based framework where ELA highlights compression inconsistencies and CNN performs classification, achieving 95% detection accuracy.

[15] Wang and Zhao (2023) focused on detecting image splicing forgery using CNN models that analyze texture, color, and illumination inconsistencies.

[16] Liu and Chen (2024) proposed a forgery detection system using the DenseNet deep learning architecture to extract deep features from manipulated images.

[17] Gupta and Sharma (2025) presented a deep neural network framework for digital image forensics that learns manipulation patterns automatically, achieving about 96% detection accuracy.

[18] K. Rao and J. Ni (2022) proposed a passive image forgery detection approach using CNN to analyze pixel-level inconsistencies without watermarking or embedded data.

[19] Bappy, Roy-Chowdhury, and Bunk (2021) developed a deep neural network model for image splicing detection by analyzing color mismatch, texture variation, and illumination differences.

[20] Amerini, Ballan, and Caldelli (2021) proposed a CNN-based method for detecting copy-move forgery, where duplicated regions within images are identified using deep features.

[21] Zhou, Han, and Morariu (2020) developed a CNN-based image manipulation detection model that learns editing artifacts such as resampling and compression traces.

[22] Bayar and Stamm (2020) proposed a CNN architecture designed to suppress image content and emphasize manipulation artifacts, improving forgery detection performance.