Science World Journal Vol. 20(No 3) 2025
www.scienceworldjournal.org
ISSN: 1597-6343 (Online), ISSN: 2756-391X (Print)
Published by Faculty of Science, Kaduna State University

https://dx.doi.org/10.4314/swj.v20i3.47

Full Length Research Article

AN ADAPTIVE COMPRESSION FACTOR ERROR LEVEL ANALYSIS FOR IMAGE FORGERY CLASSIFICATION

*Abdulqadir Hamza, Mustapha Aminu Bagiwa, Salisu Aliyu

Department of Computer Science, Ahmadu Bello University, Zaria, Nigeria

*Corresponding Author Email Address: abdulqadirhamza17@gmail.com

ABSTRACT

The intentional manipulation of visual data has been increasing due to the widespread use of image editing software and social media websites, challenging existing forgery detection methods. Error Level Analysis (ELA) based methods often struggle with JPEG compression, limiting their ability to detect tampering accurately. This paper proposes an adaptive compression mechanism to enhance ELA-based image forgery detection, particularly for augmented and expanded datasets. Using the CASIA V2 image forgery dataset with rotation, flipping, and scaling, ELA maps were derived and classified via a Convolutional Neural Network (CNN). The experimental results indicate that the proposed method achieved a better performance with accuracy, precision, recall, and F1-score of 96.6%, 96.8%, 96.3%, and 96.5%, respectively.

Keywords

Image forgery detection; Error Level Analysis (ELA); Adaptive compression; Convolutional Neural Network (CNN); CASIA V2 dataset; Digital image forensics

INTRODUCTION

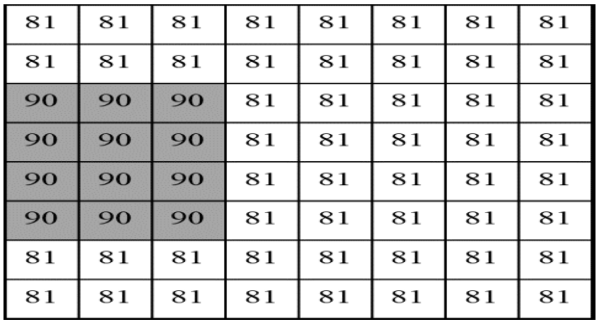
The global dissemination of smart devices with high-quality cameras, image-processing software, and affordable Internet connectivity has enabled individuals to capture, store, and process large volumes of digital visual data, such as images and videos, presenting both opportunities and risks (Zanardelli *et al*., 2022). The most common forms of image forgery are copy-move and splicing. In copy-move forgery, a part of an image is copied and pasted elsewhere within the same image (Bharti and Tandel, 2016). Image splicing, on the other hand, involves integrating parts of two or more different images to produce a single forged image.

Image forgery detection techniques are classified into two categories: active and passive. Active approaches involve embedding watermarks or digital signatures in an image for tamper detection, whereas passive approaches, also known as image forensics, do not rely on pre-embedded data. Instead, they examine inherent artifacts or inconsistencies within the image to identify tampering (Alencar *et al*., 2024).

Passive forgery detection techniques are further divided into conventional and deep learning-based methods. Conventional approaches rely on signal processing, geometry, statistics, and physics to identify inconsistencies and require little to no training data (Zanardelli *et al*., 2022). Deep learning, particularly Convolutional Neural Networks (CNNs), has emerged as a promising approach for image forgery detection. CNNs can automatically learn hierarchical features that capture tampering patterns in images. Their multi-layered structure, comprising convolutional, pooling, and dense layers, makes them highly suitable for image forensics tasks (Patil and Rane, 2021). Recent research combines both approaches; for example, Error Level Analysis (ELA), a conventional method, is applied in the preprocessing step, followed by a lightweight CNN to achieve a balance between detection accuracy and computational efficiency.

Error Level Analysis (ELA) is an image forensic technique used to highlight differences between the original image and its compressed version in order to detect manipulations. This method is based on the fact that different parts of an image compress differently depending on their content. According to Gorle and Guttavelli (2025), ELA identifies such differences. The basic steps involved in ELA are as follows (Sudiatmika *et al*., 2019):

1. Compress the original image using a lossy compression technique, such as JPEG, with low compression settings. This technique introduces new compression artifacts while maintaining current ones.
2. Calculate the error levels by subtracting the compressed image from the original image to produce a difference image. This difference image represents the error levels presented during the compression.
3. Apply algorithms such as rescaling or high-pass filtering to intensify the error levels in the difference image. This intensification makes the inconsistencies more visible.
4. Observe the intensified error levels in the difference image. Areas with higher error levels
reflect possible manipulations or alterations.



81	81	81	81	81	81	81	81
81	81	81	81	81	81	81	81
90	90	90	81	81	81	81	81
90	90	90	81	81	81	81	81
90	90	90	81	81	81	81	81
90	90	90	81	81	81	81	81
81	81	81	81	81	81	81	81
81	81	81	81	81	81	81	81

Figure 1: The quality values in an ELA Map

The sample of the quality value of ELA is shown in Figure 1, where the difference error level in some blocks can define the modification area.

Therefore, this study introduces an adaptive compression factor within the ELA framework to improve the robustness of forgery detection against varying compression levels, aiming to enhance classification accuracy and efficiency in real-world image forensics applications.

A technique that can distinguish forged images and original images with ELA and deep learning was proposed by Sudiatmika *et al.* (2019). This technique uses ELA in the preprocessing stage, followed by VGG16. Using CASIA V2, the result of their experiment achieved an accuracy of 88.46% validation by going through 100 epochs. However, there is a need to explore other CNN architectures that can be trained with fewer epochs to reduce training time.

A hybrid feature image splicing detection scheme was proposed by Zhang *et al*. (2021). A passive detection method based on ELA and Local Binary Pattern (LBP) for detecting splicing and tampering in images. The output of ELA and LBP was fused, and the bagged trees algorithm was used to classify the images. Local Binary Pattern was used because it has significant advantages, such as grey scale invariance and rotation invariance. LBP can provide a global feature, and ELA can reflect the local tampering feature, so the two complement each other, and combining them can better improve the accuracy of the experiment. There is a need to evaluate this method using a challenging dataset like CASIA V2.

Sari and Fahmi (2021) evaluated the effect of error level analysis on image forgery detection using deep learning. The effect of applying ELA at different levels, such as 10, 50, and 90 percent, on the CASIA ITDE dataset. The accuracy of the training model on average reached 0.86 for the use of ELA 90%.

A combination of Error Level Analysis (ELA) and a concatenated ResNet and Xception Net architecture was proposed by Khachane and Mondal (2023). The concatenated model with ELA achieved an accuracy of 98.58% for classification on the CASIA V2 dataset. However, this approach uses concatenated ResNet and XceptionNet features, which makes it computationally intensive.

By evaluating the error rate resulting from image quality reduction, Kubal *et al*. (2023) and Sadanand *et al*. (2024) utilize the output of ELA as an input for the three-layer CNN model and the two-layer CNN. CASIA V2 image forgery database was used in the proposed techniques, achieving an accuracy of 92.10% for Kubal *et al*. (2023) and 99.7% for Sadanand *et al*. (2024), highlighting its effectiveness in accurately detecting image forgery. However, a fraction of CASIA V2 was used for these techniques, which limits the ability of the methods to generalize well to unseen data.

Nagm *et al*., (2024), proposed a method of detecting image manipulation with ELA and a two-layer CNN. The experiments were applied to the CASIA V2 dataset, and the simulation results showed that the proposed algorithm achieved strong performance metrics, including a training accuracy of 99.05%, testing accuracy of 94.14%, precision of 94.1%, and recall of 94.07%. Further research is needed to improve the accuracy of the model.

A technique to detect image manipulation by generative adversarial networks (GANs) was proposed by Ulfah *et al*. (2025). The technique was evaluated using two scenarios: a stand-alone six-layer CNN and a combination of ELA and a six-layer CNN. Furthermore, the combined scenario has three sub-scenarios regarding the compression levels of the error-level analysis algorithm: 10%, 50%, and 90%. Based on the evaluation results, it was found that the highest quality convolutional neural network training was obtained when using 50% error level analysis compression because it could achieve 94% accuracy.

An Image forgery detection system was proposed by Choudhary *et al*. (2024). The system comprises of an ELA in the preprocessing stage in the Classification and Segmentation Phase. The model was evaluated on the CASIA V2 dataset, achieving an accuracy of 91.7% and a precision of 93.52% for the classification path. For the segmentation, an IoU of 80.6% and an F1 Score of 77.7%. However, there is a need to further improve the accuracy of the system.

This paper addresses forgery classification that is done using fixed compression factor ELA, CNN, and a limited dataset. We propose the use of Adaptive compression factor ELA, a lightweight two-layer CNN with an expanded CASIA V2 dataset for Image forgery classification.

MATERIALS AND METHODS

Proposed Adaptive Compression Factor ELA for Image Forgery Classification Model

This section presents the data analysis and adaptive compression factor. The comparative analysis of the proposed model is discussed, and the performance enhancement is also highlighted.

Dataset Analysis

The dataset for this study was collected from the Kaggle cloud repository, which is publicly available. It contains 12,614 images divided into two classes: Authentic and Forged. Specifically, there are 7,491 authentic images and 5,123 tampered images. Within the CASIA V2 dataset, 9,501 images are in JPEG format, consisting of 7,437 authentic and 2,064 tampered images. After applying data augmentation to the JPEG images, the dataset size increased to 14,874 images. Data augmentation is a technique used to artificially expand the size of a dataset by applying transformations to existing images (Azuri *et al*., 2021). The augmentation techniques used in this study include rotation, where images are rotated within a range of ±20° to simulate different orientations; shifting, which involves moving the images horizontally and vertically by up to 20% to improve robustness against positional variations; and flipping, where images are mirrored horizontally.

Adaptive Compression Factor

The Adaptive Compression Factor method dynamically assigns a JPEG compression quality factor to each image based on its file size. The rationale is that smaller-sized images are likely the result of prior strong compression and thus should be recompressed with a higher quality factor to help preserve subtle forgery traces. Conversely, larger-sized images, which are likely less compressed, are assigned a lower quality factor to amplify compression artifacts and enhance the visibility of tampered regions during Error Level Analysis (ELA). The compression quality factor is adaptively computed using the formula:

$$\text{Scale} = \frac{F - F_{min}}{F_{max} - F_{min}} \qquad (1)$$

where:

F is the file size of the current image,
$\boldsymbol{F_{min}}$ is the smallest file size in the dataset (6 KB),
$\boldsymbol{F_{max}}$ is the largest file size in the dataset (600 KB).

$$\text{Quality} = Q_{max} - \text{Scale} \times (Q_{max} - Q_{min}) \qquad (2)$$

Where:

$\boldsymbol{Q_{max}}$ is the maximum quality factor (95),
$\boldsymbol{Q_{min}}$ is the minimum quality factor (85).

Sari and Fahmi (2021) evaluated the performance of CASIA ITDE at 10%, 50% and 90% on CASIA ITDE, and 90% gave the highest accuracy. CASIA ITDE is a dataset that contains images that have undergone both copy-move and splicing forgery. Compression factors of 95% and 85% were adopted due to observed performance decrease when other compression levels were applied during training and evaluation.

https://dx.doi.org/10.4314/swj.v20i3.47

Architecture of the Proposed Model

Figure 2 illustrates the architecture of the proposed system. The model uses only JPEG images, as ELA is a format-based image forgery detection technique. In the data pre-processing stage, data augmentation was applied to increase the dataset size, followed by ELA with an adaptive compression factor. The images were then resized to 128 × 128 pixels and normalized to ensure stable and accurate training. The pre-processed data was fed into a CNN consisting of two convolutional layers of 5 × 5 × 32 each, followed by a max pooling layer of 5 × 5 and a dropout of 0.25. After the max pooling layer, flattening was applied to convert the multidimensional feature maps into a one-dimensional vector, which was then passed to a fully connected layer of 256 neurons. Finally, the fully connected layer was followed by a dropout of 0.5 to prevent overfitting, and an output layer with a Sigmoid activation function with binary cross-entropy as loss function was used for image forgery classification. RMSprop optimizer was employed with a learning rate of 0.0001.

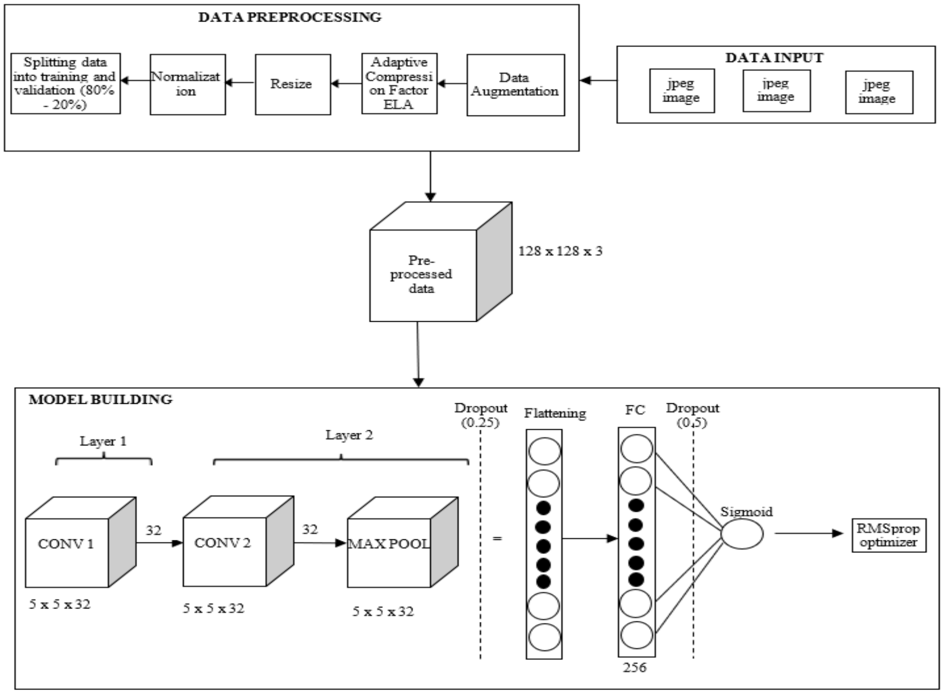


Figure 2: Architecture of the Proposed Model

EXPERIMENTAL RESULTS

The proposed model was fine-tuned on images from the 14,874 CASIA V2 forgery dataset. The Error Level Analysis (ELA) was replaced with an adaptive compression factor ELA. The purpose of replacing the ELA was to enable the model to adapt the compression factor relative to image sizes. The two convolutional layers have a kernel size of (5x5) and the same padding, followed by a max pooling layer of kernel size (5x5) with a dropout of 0.25. The last block contains the fully connected layer, a dropout rate of 0.5, and the output layer for Binary classification. The ReLU activation function was used throughout the training, except for the output layer, which uses the sigmoid activation function.

Accuracy was used as the metric to calculate the performance of the model with binary cross-entropy as the loss function. Furthermore, the RMSprop optimizer was used with a learning rate of 0.0001. The model was then fine-tuned with 30 epochs and a batch size of 16. All these hyperparameters were chosen after multiple training runs, and these hyperparameters produce the best performance in terms of accuracy.

From Figure 3, the blue curve indicates the training loss, while the orange curve indicates the validation accuracy. The training loss steadily decreases over the epochs, converging towards 0.05, while the validation initially decreases steadily but spikes to 0.17 around the 12th epoch. Afterward, it stabilizes at around 0.10. Overall, the downward trend in both training and validation loss confirms that the model is learning effectively.

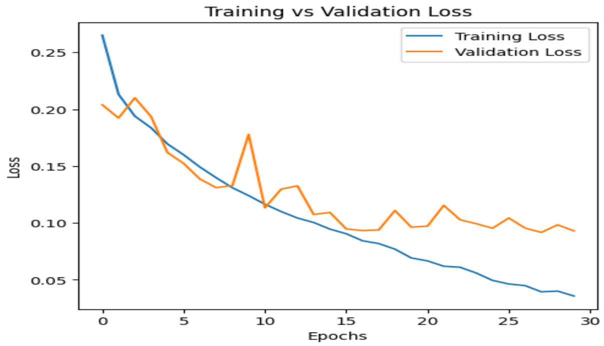


Figure 3: Graph of Training and Validation Loss of the Proposed Model

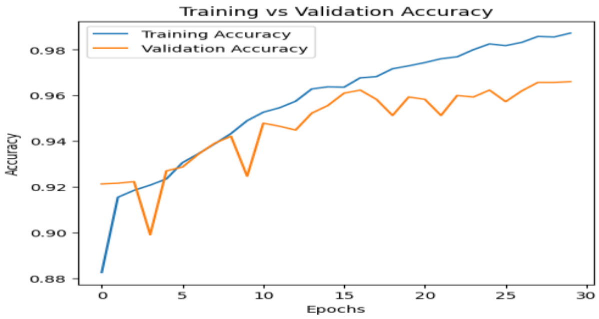


Figure 4: Graph of Training and Validation Accuracy

From Figure 4, the blue curve represents the training accuracy, while the orange curve represents the validation accuracy. Both curves show an upward trend, with the training accuracy starting around 0.88 and the validation accuracy around 0.92. The validation accuracy drops to 0.88 at the 4th epoch but recovers to 0.92 by the 10th epoch. Despite these fluctuations, the validation curve reaches a peak accuracy at 0.96, indicating that the model generalizes well. Overall, the graph shows that the model is learning effectively, with both the training and validation accuracy converging toward high values.

Figure 5 shows the confusion matrix illustrating the performance of the proposed model in classifying two classes: Authentic and Forged. The colour intensity reflects prediction frequency; darker shades represent higher counts, and lighter shades represent lower counts. The diagonal cells indicate correct predictions, while off-diagonal cells represent misclassifications. The model correctly predicted 'Forgery' 1464 times, but misclassified it as 'Authentic' 54 times. Similarly, 'Authentic' was correctly predicted 1410 times, but misclassified it as 'Forgery' 47 times. The confusion matrix shows strong performance with the model having few false positives (47) and false negatives (54), suggesting the model generalizes well.

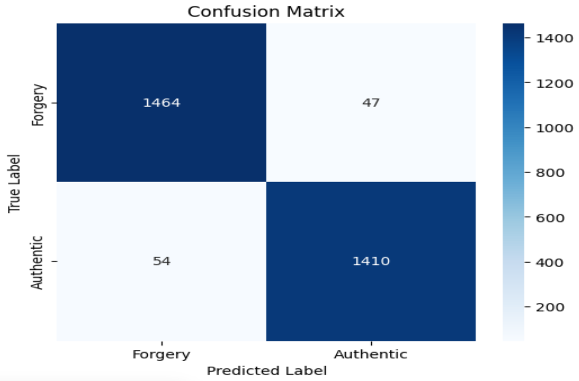


Figure 1: Confusion Matrix of the Proposed Model

Comparative Analysis

The performance of the proposed model is compared with that of Choudhary *et al.* (2024). The proposed model outperforms Choudhary *et al*. (2024) across all performance metrics, as shown in Table 1.

Table 1: Comparative analysis of the performance metrics of the proposed and existing models

Model	Accuracy	Precision	Recall	F1 Score
Choudhary *et al*., (2024)	91.7	93.5	89.9	91.7
Proposed Model	**96.6**	**96.8**	**96.3**	**96.5**

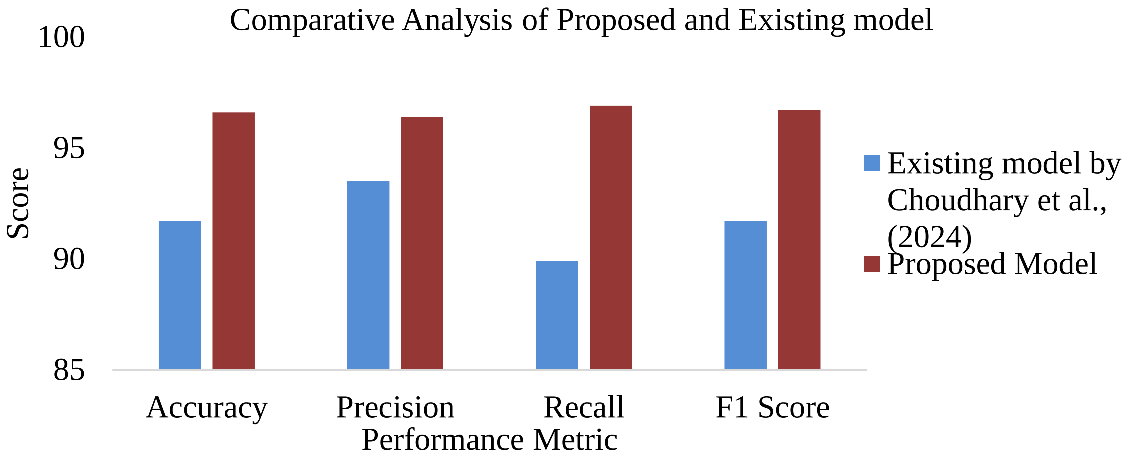


Figure 6: Comparative analysis of the performance of the Proposed Model with the Existing Model

Conclusion

This study demonstrated the enhanced image forgery detection technique by utilizing Error Level Analysis (ELA) with an adaptive compression factor applied to a large and diverse dataset. Traditional ELA-based methods often rely on a static JPEG compression factor, which limits their efficiency across varying image sizes and qualities. To address this limitation, an adaptive technique was introduced that dynamically adjusts the compression quality according to the file size of each image, compressing smaller images at higher quality and larger images at lower quality to ensure consistent exposure of compression artifacts. The images used in this study were obtained from the

CASIA V2 image forgery dataset, which contains both authentic and forged images. Data augmentation techniques that include rotation, flipping, and scaling were applied to enhance the model's generalization ability. Pre-processed ELA maps were then resized and normalized before being fed into a Convolutional Neural Network (CNN) for binary classification. Performance evaluation based on classification metrics showed that the proposed model significantly outperformed the method by Choudhary *et al*. (2024). While the benchmark model achieved 91.7% accuracy, 93.5% precision, 89.9% recall, and 91.7% F1-score, the proposed adaptive model attained 96.6% accuracy, 96.8% precision, 96.3% recall, and 96.5% F1-score.

REFERENCES

Alencar, A. L., Lopes, M. D., Fernandes, A. M. da R., Anjos, J. C. S. dos, de Paz Santana, J. F., and Leithardt, V. R. Q. (2024). Detection of Forged Images Using a Combination of Passive Methods Based on Neural Networks. *Future Internet*, *16*(3). https://doi.org/10.3390/fi16030097

Azuri, I., Goldian, I., Regev-Rudzki, N., Fantner, G., and Cohen, S. (2021). The role of convolutional neural networks in scanning probe microscopy: a review. *Beilstein Journal of Nanotechnology*, *12*, 878–901. https://doi.org/10.3762/bjnano.12.66

Bharti, C. N., and Tandel, P. (2016). A survey of image forgery detection techniques. *Proceedings of the 2016 IEEE International Conference on Wireless Communications, Signal Processing and Networking, WiSPNET 2016*, *d*, 877–881. https://doi.org/10.1109/WiSPNET.2016.7566257

Choudhary, R. R., Paliwal, S., and Meena, G. (2024). Image Forgery Detection System using VGG16 UNET Model. *Procedia Computer Science*, *235*, 735–744. https://doi.org/10.1016/j.procs.2024.04.070

Gorle, R., and Guttavelli, A. (2025). Enhanced Image Tampering Detection using Error Level Analysis and a CNN. *Technology and Applied Science Research*, *15*(1), 19683–19689. https://doi.org/10.48084/etasr.9593

Khachane, S., and Mondal, D. (2023). Image Tampering Detection using Error Level Analysis and Concatenated Neural Networks. *International Journal for Research in Applied Science and Engineering Technology*, *11*(7), 2011–2018. https://doi.org/10.22214/ijraset.2023.55067

Krawetz, N. (2007). *A Image's Worth... Digital Image Analysis and Forensics*. www.hackerfactor.com

Kubal, P., Mane, V., and Pulgam, N. (2023). Image Manipulation Detection Using Error Level Analysis and Deep Learning. *International Journal of Intelligent Systems and Applications in Engineering IJISAE* (Vol. 2023, Issue 4). www.ijisae.org

Lubna, J., and Abrar, S. (2020). *Detecting Fake Image: A Review for Stopping Image Manipulation* (pp. 146–159). https://doi.org/10.1007/978-981-15-3666-3_13

Nagm, A. M., Moussa, M. M., Shoitan, R., Ali, A., Mashhour, M., Salama, A. S., and AbdulWakel, H. I. (2024). Detecting image manipulation with ELA-CNN integration: a powerful framework for authenticity verification. *Peer Journal of Computer Science*, *10*, 1–18. https://doi.org/10.7717/PEERJ-CS.2205

Patil, A., and Rane, M. (2021). Convolutional Neural Networks: An Overview and Its Applications in Pattern Recognition. *Smart Innovation, Systems and Technologies*, *195*, 21–30. https://doi.org/10.1007/978-981-15-7078-0_3

Raković, D. (2023). Error level analysis (ELA). *Tehnika*, *78*(4), 445–451. https://doi.org/10.5937/tehnika2304445r

Sadanand, V. S., Janardhana, S. S., Purushothaman, S., Hande, S., and Prakash, R. (2024). Convolutional neural network-based techniques and error level analysis for image tamper detection. *Indonesian Journal of Electrical Engineering and Computer Science*, *33*(2), 1100–1107. https://doi.org/10.11591/ijeecs.v33.i2.pp1100-1107

Sari, W. P., and Fahmi, H. (2021). Effect of Error Level Analysis on The Image Forgery Detection Using Deep Learning. *Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control*. https://doi.org/10.22219/kinetik.v6i3.1272

Sudiatmika, I. B. K., Rahman, F., Trisno, and Suyoto. (2019). Image forgery detection using error level analysis and deep learning. *Telkomnika (Telecommunication Computing Electronics and Control)*, *17*(2), 653–659. https://doi.org/10.12928/TELKOMNIKA.V17I2.8976

Ulfah, S. M., Nurochman, N., Setianingrum, H. A., Larasati, D., Santoso, W., and Dhea Stefany, M. (2025.). *International Journal on Informatics Visualization*: A Better Performance of GAN Fake Face Image Detection Using Error Level Analysis-CNN. www.joiv.org/index.php/joiv

Zanardelli, M., Guerrini, F., Leonardi, R., and Adami, N. (2022). Image forgery detection: a survey of recent deep-learning approaches. *Multimedia Tools and Applications*, *82*, 17521–17566. https://doi.org/10.1007/s11042-022-13797

Zhang, Y. J., Shi, T. T., and Lu, Z. M. (2021). Image Splicing Detection Scheme Based on Error Level Analysis and Local Binary Pattern. *Taiwan Ubiquitous Information*, *6*(2).