Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control
Journal homepage: http://kinetik.umm.ac.id
ISSN: 2503-2267
Vol. 6, No. 3, August 2021, Pp. 187-194

The effect of error level analysis on the image forgery detection using deep learning

Wina Permana Sari[1], **Hisyam Fahmi**[*2]
Computer Science Department, School of Computer Science, Bina Nusantara University, Jakarta, Indonesia[1]
Universitas Islam Negeri Maulana Malik Ibrahim, Malang, Indonesia[2]

Article Info

Keywords:
Convolutional Neural Network, Copy-Move Image Forgery, Digital Image Forensics, Error Level Analysis

Article history:
Received: June 01, 2021
Accepted: August 05, 2021
Published: August 31, 2021

Cite:
Sari, W. P., & Fahmi, H. (2021). The Effect of Error Level Analysis on The Image Forgery Detection Using Deep Learning. Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control, 6(3).
https://doi.org/10.22219/kinetik.v6i3.1272

*Corresponding author
Hisyam Fahmi
E-mail address:
hisyam.fahmi@uin-malang.ac.id

Abstract

Digital image modification or image forgery is easy to do today. The authenticity verification of an image become important to protect the image integrity so that the image is not being misused. Error Level Analysis (ELA) can be used to detect the modification in image by lowering the quality of image and comparing the error level. The use of deep learning approach is a state-of-the-art in solving cases of image data classification. This study wants to know the effect of adding ELA extraction process in the image forgery detection using deep learning approach. The Convolutional Neural Network (CNN), which is a deep learning method, is used as a method to do the image forgery detection. The impacts of applying different ELA compression levels, such as 10, 50, and 90 percent, were also compared in this study. According to the results, adopting the ELA feature increases validation accuracy by about 2.7% and give the better test accuracy. However, the use of ELA will slow down the processing time by about 5.6%.

1. Introduction

Image data is extremely prone to manipulation in today's digital environment. Image editing software is widely available today, and it may be used not only on desktop computers and laptops, but also on handheld mobile devices [1]. A deep generative model is commonly used to create hyper-realistic face-swapping images and videos in some applications [2]. People commonly exploit the outcomes of this image manipulation on social media, in the commercial world, and even for criminal purposes. The use of image manipulation for illegal purposes should be a major source of concern, since it can pose a serious threat to society, government, and industry. As a result, the validity of the images in the internet must be confirmed. So that, maintaining the integrity of digital photographs is crucial [3]. In this situation, an image forgery detection method can be used to verify the validity of digital images [4].

The Digital Image Forensics (DIF) is a field to detect the authenticity of digital images, both in terms of the image content's integrity and the source [5]. Active and passive modification detection techniques are two types of algorithms for detecting picture forgery in DIF [6]. The method of passive forgery detection does not need any prior knowledge of the image's content [7]. The active technique, on the other hand, requires extracting watermarks and digital signatures embedded in images and then verifying them [8]. As a result, any modification to the image can disrupt the embedded watermark and digital signature, assisting in the detection of the image's validity. The copy-move (cloning) modification method is the passive image forgery that has the largest impact on the original image. [9][10][11].

Several studies on digital image forgery detection have been carried out with various approaches. Research Dehnie et al. [12] discussed digital image forensic techniques to distinguish images captured by digital cameras from computer-generated images. This difference is captured in terms of residual image properties (noise patterns in the case of digital camera images) extracted by a wavelet-based denoising filter. The results of this study indicate that the two types of residues obtained from different digital camera images and computer-generated images have some general characteristics that are not present in other types of images. Their results are based on images generated by Maya and 3D Studio Max software, and various digital camera images. Warbhe and Dharaskar [4], [13] present an active approach to identify and authenticate original digital images from forged or tampered with images. The experimental results show how the Independent Component Analysis (ICA) method is successful in extracting and detecting image forgery if it is in the image. While this method is good at detecting adulteration in images, the main limitation of this method is that it requires a faked image as well as an original forged image. This limitation can be overcome by using and applying single channel ICA to a single spurious image to extract the forgery. The singular value decomposition was developed by Liliana and Basaruddin [14] as a method for detecting visual forgery. The image preprocessing methodology provides two orthogonal vectors to the singular value vector prior to the detection operation, which are critical for detecting fraudulent images. Huynh et al. [15] proposes a model based on sharpness and blurriness to distinguish the actual altered locations from suspicious ones discovered in nearby locations. Shelke and Kasana [16] suggested a passive method for detecting and localizing numerous forgeries in video utilizing the Polar Cosine Transform (PCT) and Neighborhood Binary Angular Pattern (NBAP), as well as the GoogleNet model.

Deep learning research is the current trend for solving computer vision challenges such image classification. Because deep learning architecture, like the Convolutional Neural Network (CNN), is capable of extracting complicated statistical features from high-dimensional data, this is the case. Passive image forgery detection has also been done using deep learning approach [17][18][19]. Bayar and Stamm [20] have proposed a new form of CNN layer called the Constrained Convolutional Layer, which can learn characteristics to identify picture modification and is adaptive. The experiment reveals that the CNN architecture has a 99.97% accuracy in detecting various modification actions. Rao and Ni [17] proposed a new deep learning-based picture fraud detection system that uses the Convolutional Neural Network (CNN) to develop a hierarchical representation of an input RGB color image automatically. The fundamental high-pass filter set used in the construction of the residual map in the spatial rich model (SRM), which works as a regularizer to efficiently suppress the impacts of image content and capture undetectable modifications produced by tampering processes, is used to initialize the weights in the first layer of the network. Chen et al. [21] propose a hybrid features and semantic reinforcement network (HFSRNet). The model, which is based on long-short term memory with resampling features, was used to capture traces from image patches for the purpose of detecting and altering artifacts.

Traditional deep learning frameworks, on the other hand, should not be utilized directly because modified images are difficult to distinguish from original images with many existing image modification technologies, demanding the modification of the input and architecture [22]. Error Level Analysis (ELA) is one approach for determining whether or not an image has been modified. This approach finds errors by lowering image quality and then estimating the error level on an 8 by 8 grid. If the image isn't changed, all eight grids will have the same error level. [23]. For digital image forgery detection, a combination of ELA features and CNN architecture can be used [23]. However, no research has been done to determine how effective ELA is at performing this task. As a result, the goal of this study is to demonstrate how the addition of ELA features affects the effectiveness of image forgery detection results obtained through the use of CNN. Furthermore, the effects of applying different ELA compression levels, such as 10, 50, and 90 percent, were compared in this research.

2. Research Method

2.1 Image Datasets

This study used photo image data from high resolution digital cameras as dataset. A copy-move modification is performed on the original photo. Each of the original photos and their modifications has a total of 20 images. The Pattern Recognition Lab, Computer Science, Friedrich-Alexander-Universität Erlangen-Nürnberg (https://lme.tf.fau.de) provided a dataset of transformed images for this work, including 48 images for each category of original and modified images. The dataset from the CASIA ITDE database [24], which was also used in the Warif et al. [25][21] study, has been added as well, with a total of 510 images, 255 images for each category, original and modified. As a result, a total of 646 datasets were used, with 323 original images and 323 modified images. 596 images were utilized for training and the remaining 50 images were used for test from the dataset. The dataset received several modifications, including copy-moving, splicing, and resampling. Examples of original and modified photo images from digital camera can be seen in Figure 1 where a forgery image is obtained by adding objects from the same image (copy-move). Figure 2 shows an image that has been modified using copy-move and resampling, which is the process of mirroring, or flipping, scaling, and rotating picture objects. Figure 3 shows an image dataset that was modified via copy-move and splicing, which is the merging of two separate image objects.

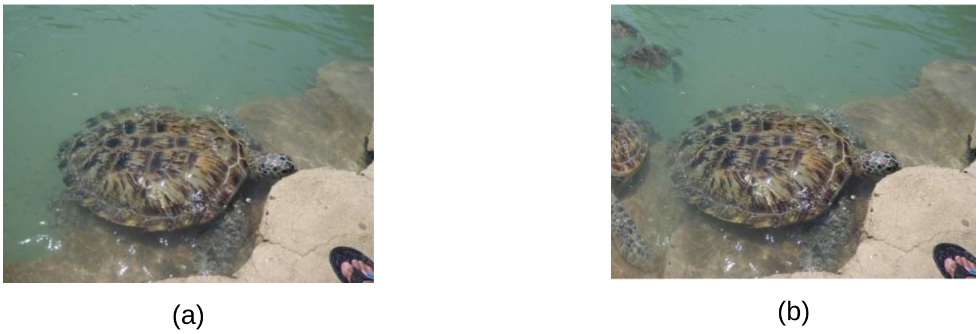
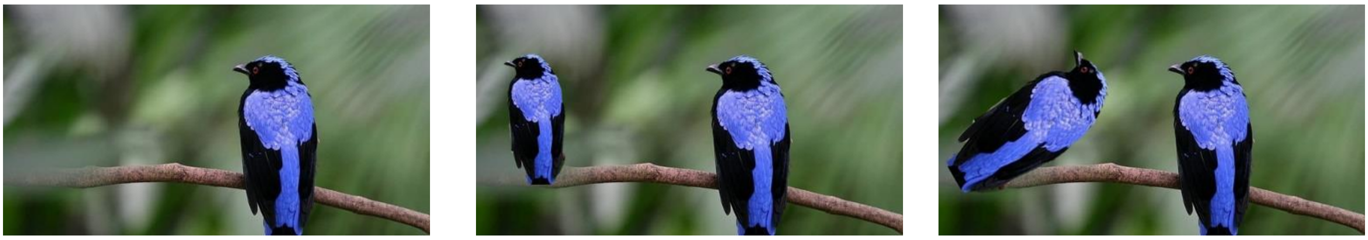
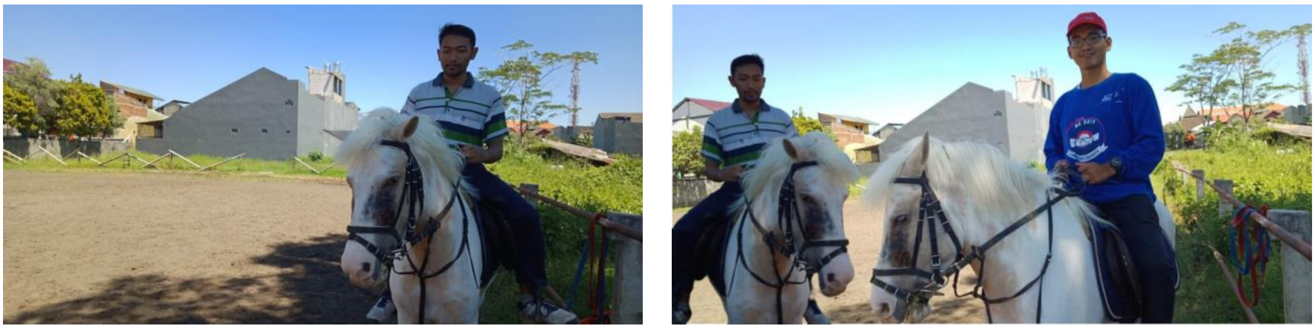

(a) (b)

Figure 1. Image dataset Example of Copying and Moving Parts of Image; (a) the Original Image and (b) Forgery Image



(a) (b) (c)

Figure 2. Dataset Example of Copy-Move and Resampling; (a) the Original Image, (b) Copy-Move and Scaling Object, and (c) Copy-Move and Rotating Object



(a) (b)

Figure 3. Dataset Example of Image Resampling and Splicing; (a) the Original Image and (b) Forgery Image

2.2 Error Level Analysis (ELA)

Error Level Analysis is a technique used to detect image manipulation by restoring the image at a certain quality level and calculating the ratio between compression levels [26]. In general, this technique is performed on images that are in a lossy format (lossy compression). The image type used in data mining is JPEG. In JPEG images, compression is performed independently for every 8 × 8 pixel in the image. If an image is not manipulated, every 8 × 8 pixels in the image must have the same error rate [23]. Three different levels of image compression were examined in this article, namely 10%, 50%, and 90% compression.

2.3 Deep Learning Architecture

In this research, it has been tried to detect modified images using deep learning methods CNN, which is inspired by the visual cortex. Technically, this network is designed to extract relevant features for classification, namely those that minimize loss function. Network parameter - kernel weight trained by the Gradient Descent method to produce the most discriminating features of the rendered image to the network. These features are then assigned to the fully connected layer to perform classification.

The architecture used is based on the previous studies which compares two arhitecture of deep learning for digital image forgery detection [27], the best CNN architecture has been used in this study. The image size used in this study is 128 × 128 × 3 with 3 convolutional layers with a 3 × 3 kernel and 2 pooling layers followed by a fully connected layer of 64 units and a sigmoid activation function. Figure 4 shows the architecture in the experiment.

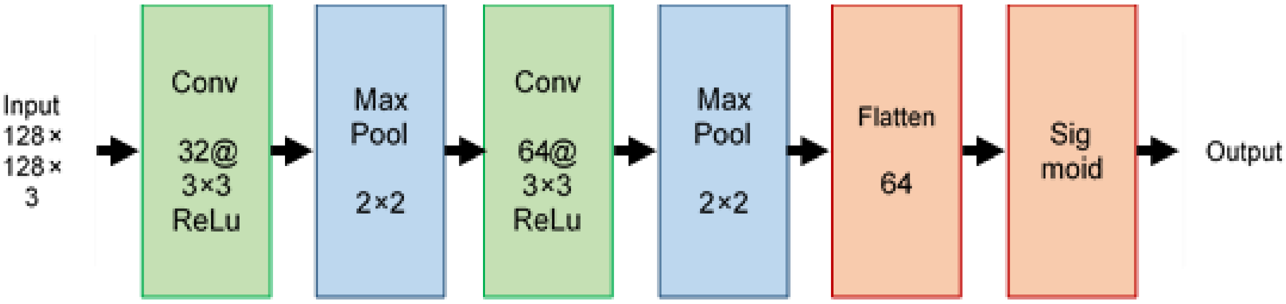


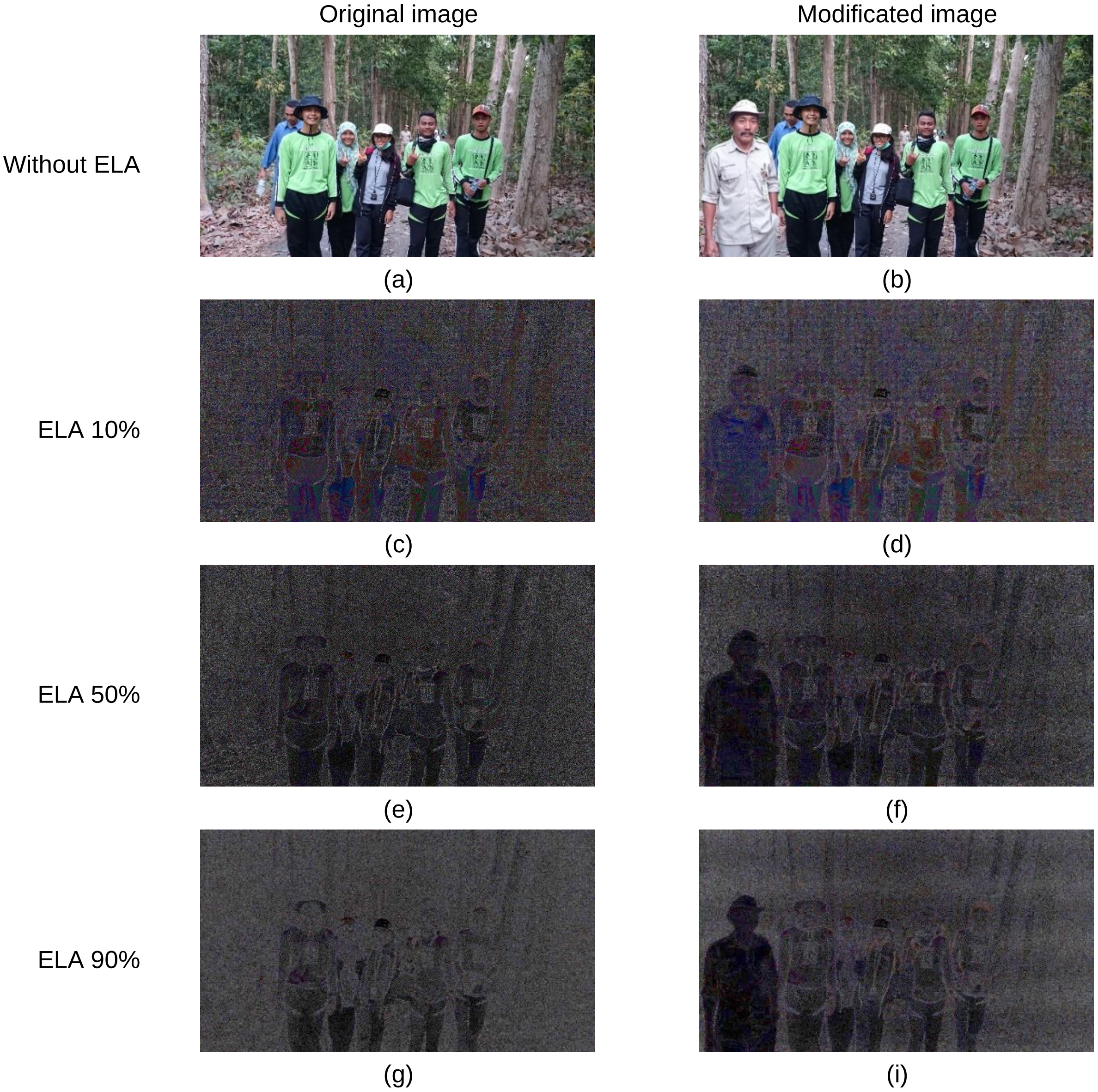
Figure 4. CNN Architecture for the Experiment

Cite: Sari, W. P., & Fahmi, H. (2021). The Effect of Error Level Analysis on The Image Forgery Detection Using Deep Learning. Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control, 6(3). https://doi.org/10.22219/kinetik.v6i3.1272

3. Results and Discussion

From the dataset used, 596 images were used for training data, and the remaining 50 images were used for testing. K-fold cross validation is used during the training process to validate the model, so that validation accuracy is obtained at each epoch. After obtaining the optimal model, an evaluation using data testing is conducted to determine the test accuracy. Experiments were conducted to demonstrate the effectiveness of a deep-learning approach using CNN for image forgery detection. Also compared with the addition of ELA features before processing in CNN. The device used for testing has an Intel Core-I7 4702MQ specification with 12 GB RAM. The implementation of the CNN architecture uses the Keras library in Python.

In the preprocessing stage, each image is applied ELA feature extraction, before entering the CNN architecture. The ELA stage begins with the image compression process to reduce image quality and is saved in the JPEG format. In this experiment the input image was compressed to 10%, 50%, and 90% of the initial image quality. Then the difference between the initial image and the compression result is calculated. An example of the ELA extraction result is shown in Figure 5. The modified area will look quite different from the original image when the ELA compression level is higher. Furthermore, the image is processed on the CNN architecture by conducting a training and testing process to evaluate classification model.



(a) (b)

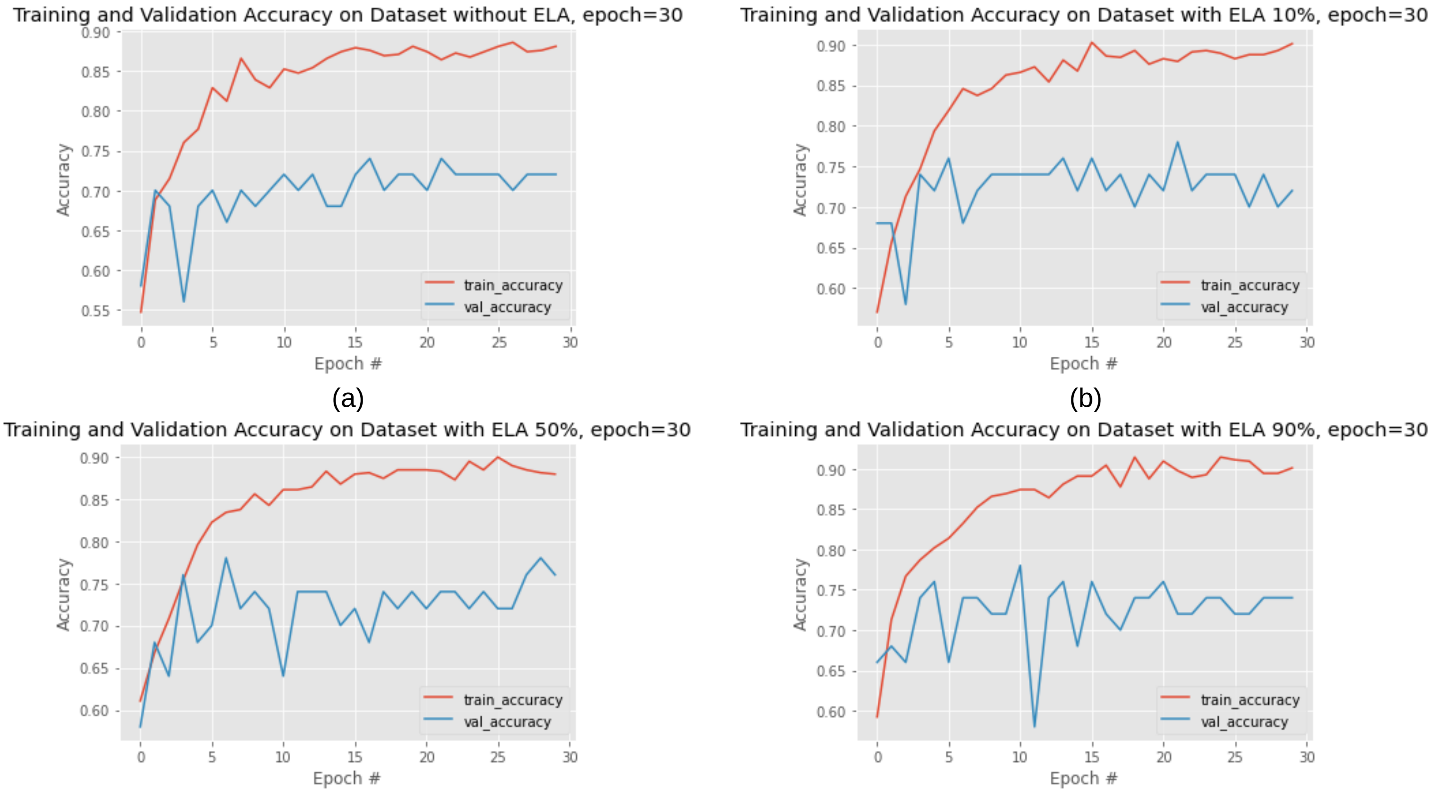
(c) (d)

(e) (f)

(g) (i)

Figure 5. The Example of ELA Feature Extraction; (left) Original Image and (right) Modified Image; Images in the first Row is the Image without ELA (note: the Image Brightness is Increased to Make it More Visible)

Extensive experiments were conducted on several image datasets using an epoch 30 times and a batch size of 25. Using the same data as the training data, a classification model was created and the accuracy and loss values were determined. The model was then validated using cross validation as explained before. Then, using new data, perform the evaluation to determine the test accuracy. The testing results were compared between using ELA features and without ELA features on CNN. The different level of ELA feature also been compared. Figure 6 displays the line charts of training and validation accuracy for each epoch. Figure 6 (a) shows a test chart for image forgery detection using just CNN. The other three charts shows the accuracy of CNN with ELA features for image forgery detection, which is using compression level of 10%, 50%, and 90% respectively. A summary of the comparison of the testing results is shown in Table 1. As the value of validation loss decreases, the value of validation accuracy increases. This indicates that the model being built is learning and functioning properly. There is no noticeable difference in the test accuracy.



(a) (b)

(c) (d)

Figure 6. Training and Validation Results; (a) CNN without ELA, (b) with ELA 10%, (c) with ELA 50%, and (d) with ELA 90%

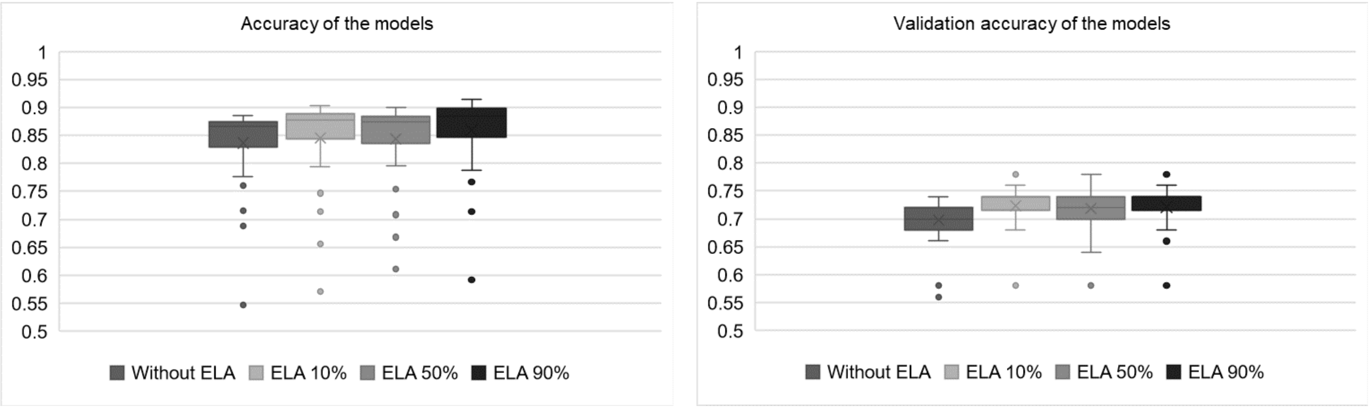
Table 1. Comparison of Testing Result Image Forgery Detection using CNN with and without ELA

	Without ELA	With ELA 10%	With ELA 50%	With ELA 90%
Accuracy	0.8360	0.8452	0.8438	0.8589
Loss	0.4477	0.3518	0.3529	0.3011
Validation Accuracy	0.6973	0.7233	0.7187	0.7207
Validation *Loss*	0.7178	0.5344	0.5901	0.6858
Test Accuracy	0.7400	0.7200	0.7600	0.7400
Time (s)	31.5333	44.8333	41.3667	33.4000

When these results are compared, it is clear that detection with the ELA feature produces a model with higher average accuracy than detection without ELA. Similarly, when using test data, detection without ELA produces results that are less accurate than detection with ELA, whether at 10%, 50%, or 90% ELA. The box plot of accuracy and validation accuracy from the experiment results is shown in Figure 7. This plot shows that the difference between the four models is not excessive. Although the difference in accuracy and validation accuracy is not particularly large, when examined using a t-test, the difference in validation accuracy between using ELA and without ELA is quite significant, with a p-value less than 0.05. The difference in the use of different ELA levels is not very significant here. However,

Cite: Sari, W. P., & Fahmi, H. (2021). The Effect of Error Level Analysis on The Image Forgery Detection Using Deep Learning. Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control, 6(3). https://doi.org/10.22219/kinetik.v6i3.1272

when 90% ELA is used, the highest rating is 0.86, and the best test accuracy is 0.76 when 50% ELA is used. The use of ELA features will slow down the detection process by around 5.6% when compared to not using them.



(a) (b)

Figure 7. Box Plot of (a) Accuracy and (b) Validation Accuracy

4. Conclusion

According to the experiment, ELA can be applied to the CNN to increase the accuracy results of digital image forgery detection. The accuracy of the training model on average reached 0.86 for the use of ELA 90%. The use of ELA 10% and 50% resulted in an accuracy of 0.85 and 0.84 respectively. Meanwhile, the detection accuracy using CNN without ELA is 0.83. When compared with the results without ELA, the accuracy of the training model is better using the ELA feature. Likewise, when viewed from the accuracy validation, it will show the superiority of using the ELA feature with a significant difference using the t-test. The best accuracy is obtained when using ELA 90%, whereas the maximum accuracy is obtained when using ELA 10% in validation. Similarly, when evaluating using test data, ELA 50% produces the highest test accuracy value, despite the fact that it is not significantly different from the others. However, using the ELA function will slow down the detection process slightly as compared to not using it. In addition to classification or image forgery detection, future research is intended to provide information on the modified pixel region with better accuracy.

Acknowledgement

Thank you to Ministry of Religious Affairs Indonesian Republic which has gave a funding to do this research. Hopefully, this research can make a major contribution to the advancement of technology in Indonesia.

References

[1] R. Ahmed and R. V Dharaskar, “Study of Mobile Botnets: An Analysis from the Perspective of Efficient Generalized Forensics Framework for Mobile Devices General Terms,” in National Conference on Innovative Paradigms in Engineering & Technology (NCIPET), 2012, pp. 5–8.

[2] M. Yu, J. Zhang, S. Li, J. Lei, F. Wang, and H. Zhou, “Deep forgery discriminator via image degradation analysis,” *IET Image Process.*, May 2021. https://doi.org/10.1049/ipr2.12234

[3] D. Chauhan, D. Kasat, S. Jain, and V. Thakare, “Survey on Keypoint Based Copy-move Forgery Detection Methods on Image,” in *Procedia Computer Science*, 2016, vol. 85. https://doi.org/10.1016/j.procs.2016.05.213

[4] A. D. Warbhe and R. V Dharaskar, “An Active Approach based on Independent Component Analysis for Digital Image Forensics.”.

[5] H. Farid, “Image forgery detection,” *IEEE Signal Processing Magazine*, vol. 26, no. 2. Institute of Electrical and Electronics Engineers Inc., pp. 16–25, 2009.https://doi.org/10.1109/MSP.2008.931079

[6] V. Conotter, G. Boato, and H. Farid, “Active and Passive Multimedia Forensics,” 2011.

[7] T. Kumar and G. Khurana, “Towards recent developments in the field of digital image forgery detection,” *Int. J. Comput. Appl. Technol.*, vol. 58, no. 1, p. 1, 2018. https://doi.org/10.1504/IJCAT.2018.094064

[8] W. S. Sari and C. A. Sari, “A High Result in Wavelet Watermarking Using Singular Value Decomposition,” *Kinet. Game Technol. Inf. Syst. Comput. Network, Comput. Electron. Control*, vol. 4, no. 3, pp. 269–276, Jul. 2019. https://doi.org/10.22219/kinetik.v4i3.729

[9] M. Mishra and M. C. Adhikary, “Digital Image Tamper Detection Techniques - A Comprehensive Study,” Int. J. Comput. Sci. Bus. Informatics, vol. 2, no. 1, 2013.

[10] S. Sadeghi, S. Dadkhah, H. A. Jalab, G. Mazzola, and D. Uliyan, “State of the art in passive digital image forgery detection: copy-move image forgery,” *Pattern Anal. Appl.*, vol. 21, no. 2, pp. 291–306, May 2018. https://doi.org/10.1007/s10044-017-0678-8

[11] B. Soni and D. Biswas, “Image Forensic using Block-based Copy-move Forgery Detection,” 2018. https://doi.org/10.1109/SPIN.2018.8474287

[12] S. Dehnie, T. Sencar, and N. Memon, “Digital image forensics for identifying computer generated and digital camera images,” in *Proceedings - International Conference on Image Processing, ICIP*, 2006, pp. 2313–2316. https://doi.org/10.1109/ICIP.2006.312849

[13] A. D. Warbhe, R. V. Dharaskar, and V. M. Thakare, “Computationally Efficient Digital Image Forensic Method for Image Authentication,” in *Procedia Computer Science*, 2016, pp. 464–470. https://doi.org/10.1016/j.procs.2016.02.089

[14] D. Y. Liliana and T. Basaruddin, “Deteksi Pemalsuan Citra Berbasis Dekomposisi Nilai Singulir,” *MAKARA Sci. Ser.*, vol. 13, no. 2, pp. 180–184, 2010. https://doi.org/10.7454/mss.v13i2.422

[15] K.-T. Huynh, T.-N. Ly, and P.-T. Nguyen, "Improving the Accuracy in Copy-Move Image Detection: A Model of Sharpness and Blurriness," *SN Comput. Sci.*, vol. 2, no. 4, p. 278, Jul. 2021. https://doi.org/10.1007/s42979-021-00682-w

[16] N. A. Shelke and S. S. Kasana, "Multiple forgery detection and localization technique for digital video using PCT and NBAP," *Multimed. Tools Appl.*, pp. 1–29, May 2021. https://doi.org/10.1007/s11042-021-10989-8

[17] Y. Rao and J. Ni, "A deep learning approach to detection of splicing and copy-move forgeries in images," Jan. 2017. https://doi.org/10.1109/WIFS.2016.7823911

[18] H. Phan-Xuan, T. Le-Tien, T. Nguyen-Chinh, T. Do-Tieu, Q. Nguyen-Van, and T. Nguyen-Thanh, "Preserving Spatial Information to Enhance Performance of Image Forgery Classification," in *International Conference on Advanced Technologies for Communications*, Oct. 2019, vol. 2019-October, pp. 50–55. https://doi.org/10.1109/ATC.2019.8924504

[19] C. Chen, S. McCloskey, and J. Yu, "Image splicing detection via camera response function analysis," in *Proceedings - 30th IEEE Conference on Computer Vision and Pattern Recognition, CVPR 2017*, 2017, vol. 2017-January. https://doi.org/10.1109/CVPR.2017.203

[20] B. Bayar and M. C. Stamm, "Constrained Convolutional Neural Networks: A New Approach Towards General Purpose Image Manipulation Detection," *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 11, pp. 2691–2706, Nov. 2018. https://doi.org/10.1109/TIFS.2018.2825953

[21] H. Chen, C. Chang, Z. Shi, and Y. Lyu, "Hybrid features and semantic reinforcement network for image forgery detection," *Multimed. Syst.*, pp. 1–12, May 2021. https://doi.org/10.1007/s00530-021-00801-w

[22] Y. Zhang, J. Goh, L. L. Win, and V. Thing, "Image region forgery detection: A deep learning approach," in *Cryptology and Information Security Series*, 2016, vol. 14, pp. 1–11. https://doi.org/10.3233/978-1-61499-617-0-1

[23] T. S. Gunawan, S. A. M. Hanafiah, M. Kartiwi, N. Ismail, N. F. Za'bah, and A. N. Nordin, "Development of photo forensics algorithm by detecting photoshop manipulation using error level analysis," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 7, no. 1, pp. 131–137, Jul. 2017. http://doi.org/10.11591/ijeecs.v7.i1.pp131-137

[24] J. Dong, W. Wang, and T. Tan, "CASIA image tampering detection evaluation database," in *2013 IEEE China Summit and International Conference on Signal and Information Processing, ChinaSIP 2013 - Proceedings*, 2013, pp. 422–426. https://doi.org/10.1109/ChinaSIP.2013.6625374

[25] N. B. A. Warif, A. W. A. Wahab, M. Y. I. Idris, R. Salleh, and F. Othman, "SIFT-Symmetry: A robust detection method for copy-move forgery with reflection attack," *J. Vis. Commun. Image Represent.*, vol. 46, pp. 219–232, Jul. 2017. https://doi.org/10.1016/j.jvcir.2017.04.004

[26] N. Krawetz, "A Picture's Worth... Digital Image Analysis and Forensics," 2007. Accessed: Sep. 28, 2020.

[27] H. Fahmi and W. P. Sari, "Effectiveness of Deep Learning Architecture for Pixel-Based Image Forgery Detection," Apr. 2021, pp. 302–307. https://dx.doi.org/10.2991/assehr.k.210421.044