

# Deepfake detection using convolutional neural networks: a deep learning approach for digital security

Fenina Adline Twince Tobing<sup>1</sup>, Adhi Kusnadi<sup>1</sup>, Ivransa Zuhdi Pane<sup>2</sup>, Rangga Winantyo<sup>1</sup>

<sup>1</sup>Department of Informatics, Faculty of Engineering and Informatics, Universitas Multimedia Nusantara, Tangerang, Indonesia

<sup>2</sup>Research Centre for Aviation Technology, National Research and Innovation Agency, Tangerang, Indonesia

## Article Info

### Article history:

Received Nov 17, 2024

Revised Mar 21, 2025

Accepted Jul 2, 2025

### Keywords:

Artificial intelligence

Authentication

Convolutional neural network

Deepfake

Face recognition

## ABSTRACT

The development of artificial intelligence technology, especially deep learning, has facilitated the emergence of increasingly sophisticated deepfake technology. Deepfakes utilize generative adversarial networks (GANs) to manipulate images or videos, making it appear as if someone said or did things that never actually happened. As a result, deepfake detection has become a critical challenge, particularly in the context of the spread of false information and digital crime. The purpose of this research is to create a method for detecting deepfakes using a convolutional neural network (CNN) approach, which has been proven effective in visual pattern recognition. Through training with a dataset of original facial images and deepfakes, the CNN model achieved an accuracy of 81.3% in detecting deepfakes. The evaluation results for metrics such as precision, recall, and F1-score indicated good performance overall, although there is still room for improvement. This study is expected to make a significant contribution to enhancing digital security, especially in detecting visual manipulations based on deepfakes.

*This is an open access article under the [CC BY-SA](#) license.*



## Corresponding Author:

Fenina Adline Twince Tobing

Department of Informatics, Faculty of Engineering and Informatics, Universitas Multimedia Nusantara

Tangerang, Indonesia

Email: fenina.tobing@umn.ac.id

## 1. INTRODUCTION

The development of artificial intelligence (AI) technology has opened up many opportunities in various fields [1], but it has also brought new challenges, one of which is the emergence of deepfakes [2], [3]. Deepfake technology utilizes AI, particularly deep learning techniques, to manipulate a person's face in a video or image, making it appear as if the individual is doing or saying things that never actually happened [4], [5]. This technology often employs generative adversarial networks (GANs) [6] to modify original content or generate new content that closely resembles real people [7]. The potential for misuse of deepfakes is very high, especially in the context of spreading false information, identity manipulation, and digital crimes such as fraud and extortion [8]. For example, cases of fraud using deepfakes have resulted in losses amounting to billions of rupiah in international business transactions [9].

As deepfake technology becomes more sophisticated, detecting fake content becomes increasingly difficult [10], posing a serious challenge for researchers, particularly in developing technology that can detect and identify fake content automatically and quickly. One of the most effective approaches for detecting deepfakes is the use of convolutional neural networks (CNNs), a deep learning architecture recognized for its effectiveness in image processing and complex visual pattern recognition [11].

Although various methods have been developed to detect deepfakes, their accuracy levels are still not optimal, especially when dealing with high-quality deepfake videos. This study aims to develop a deep

learning-based deepfake detection method using CNNs [12], [13]. With this approach, the detection system is expected to analyze facial features with high accuracy, distinguishing real faces from those generated by deepfake technology. In addition, this study also aims to evaluate the effectiveness of the CNN method under various image and video conditions.

Several previous studies, such as those by Sharma *et al.* [14], have shown that deep facial recognition technology has great potential in detecting high-quality deepfakes using the CNN method. This study holds significant importance in addressing the growing threat of deepfakes. The results of this study are expected to not only provide a more accurate solution for detecting deepfakes but also help enhance digital security across various sectors, particularly in identity authentication and cyber fraud prevention. With a more reliable detection method, the risks associated with the spread of fake content and identity misuse can be minimized [15].

## 2. METHOD

This study aims to develop a deepfake detection system using the CNN [16] architecture to distinguish between real and deepfake faces. The research methodology involves several key stages, including data collection, data processing, model training, and model performance evaluation. The following are the methodological steps taken in this study.

### 2.1. Data collection

The dataset used in this study consists of real and deepfake face images. The dataset is sourced from open platforms such as Kaggle [17], and it includes 140,000 face images, with an equal distribution of 70,000 real faces and 70,000 deepfake faces generated by GANs [18]. These images have a uniform resolution of 256×256 pixels to facilitate further processing.

### 2.2. Data Preprocessing

Before being used for model training, the image data is processed through the following stages:

- Normalization: the pixel values of the images are scaled to a range between 0 and 1 to facilitate the training process [19].
- Data augmentation [20]: techniques such as rotation, translation, and flipping are applied to increase the variation of training data and improve the model's generalization ability.
- Dataset division: the dataset is split into training and validation data with a ratio of 80:20 to maintain training quality and avoid overfitting [21].

### 2.3. CNN model architecture

The CNN model is used as the foundational architecture for the deepfake detection process [22]. CNN is chosen for its ability to recognize visual features hierarchically [23], [24], making it well-suited for detecting subtle differences between real faces and deepfakes. The stages in CNN [25], [26] include:

- Convolution layer: this layer functions to extract features from the input image using a filter that moves spatially over the image.
- Pooling: the pooling process reduces the dimensions of the image without removing important features, helping to minimize computational complexity.
- Fully connected layer: this layer performs the final classification, determining whether the image is a real face or a deepfake

### 2.4. Training parameters

The CNN model is trained using the following parameter configuration:

- Optimizer: Adam (adaptive moment estimation) [27] is used to accelerate the convergence process during training.
- Loss function [28]: binary cross-entropy is selected as the loss function since the problem is a binary classification.
- Batch size: a batch size of 64 is used, providing a balance between training time and memory usage.
- Number of epochs: the model is trained for 25 epochs, with validation loss monitoring to avoid overfitting.

### 2.5. Model evaluation

To measure the performance of the developed CNN model, several evaluation metrics [29] are used, including:

- Accuracy: measures the overall accuracy of the model in classifying images correctly.

- Precision, recall, F1-score: these metrics evaluate the balance between positive and negative predictions made by the model.
- Receiver operating characteristic (ROC) curve [30]: this curve is used to visualize the model's performance across various threshold values.

## 2.6. Testing and validation

The model is evaluated using validation data that is distinct from the training set. Performance is measured through metrics including accuracy, precision, recall, and F1-score [31]. Furthermore, a confusion matrix is employed to gain more insight into the model's accurate and erroneous predictions [32].

## 2.7. Error analysis

After the testing process, an analysis is conducted on cases where the model makes prediction errors [33]. This analysis helps in understanding the model's limitations and serves as a basis for further improvements.

# 3. RESULTS AND DISCUSSION

## 3.1. Experimental results

This study successfully developed a deepfake detection system based on a CNN using a dataset consisting of 140,000 facial images, divided into 70,000 real facial images and 70,000 deepfake facial images from Kaggle [17]. The CNN model was trained for 25 epochs with a batch size of 64 using the rectified linear unit (ReLU) activation function and the Adam optimizer. The results showed that this model has a relatively good performance in detecting deepfakes. The performance of the model is presented in Table 1.

Based on the results obtained from using the CNN model with a dataset of 140,000 images, an accuracy of 81.3% was achieved on the test data. The metrics show that the model successfully classifies most images, though there is potential to enhance its accuracy further. Besides accuracy, additional evaluation metrics like precision, recall, and F1-score are utilized to offer a more complete assessment of the model's effectiveness in detecting deepfakes.

The results for these metrics are as follows: a precision value of 95%, indicating that the model has a low error rate in misclassifying fake faces as real faces; a recall value of 98%, showing that the model is highly sensitive to deepfake images and can detect most deepfake faces in the dataset; and an F1-score of 97%, this indicates the model's strong capability in distinguishing between real and deepfake faces in a binary classification task. To gain deeper insights into the model's performance across different classification thresholds, a ROC curve and the area under the curve (AUC) [34] are generated, as illustrated in Figure 1.

Table 1. Training evaluation of each model

Model	Dataset	Test accuracy	F1-score	Precision	Recall
CNN	140,000 real and fake faces	0.813	0.97	0.95	0.98

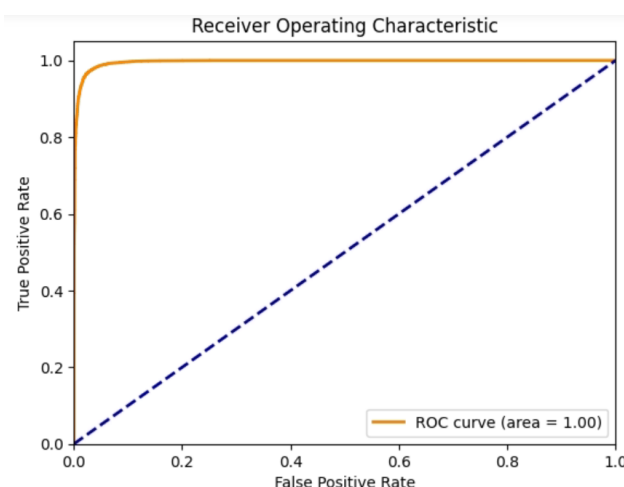


Figure 1. ROC curve CNN

Based on the generated ROC curve, the CNN model shows an AUC of 91% on a dataset containing 140,000 real and fake face images, indicating good performance in distinguishing real and deepfake faces. Experiments were conducted to evaluate the accuracy of the proposed approach. Fake and real photos from each model were used in this experiment. As shown in Figure 2, almost all photos were successfully identified and correctly classified as either "Real" or "Fake". The real and fake photos were randomly selected from the validation folder.

Figure 3 shows the decrease in training loss and validation loss against the number of epochs in the CNN model. At the beginning of training, both the training loss and validation loss decreased sharply, indicating that the CNN model quickly learned from the data. However, after several epochs, the validation loss of the CNN model began to increase, indicating potential overfitting, while the training loss continued to decrease, approaching zero, suggesting that the model was able to learn the training data well.

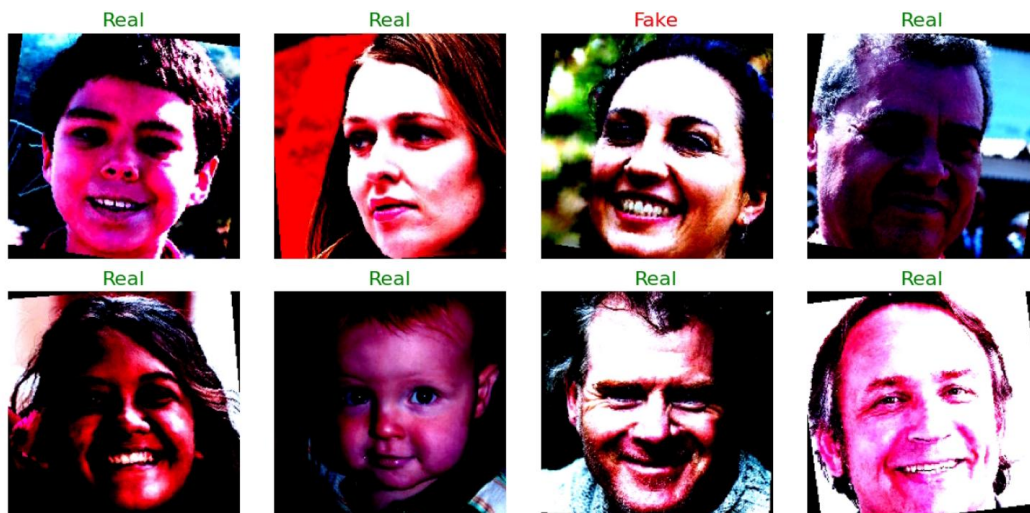


Figure 2. Example of a real image in the first row and a fake image in the second row

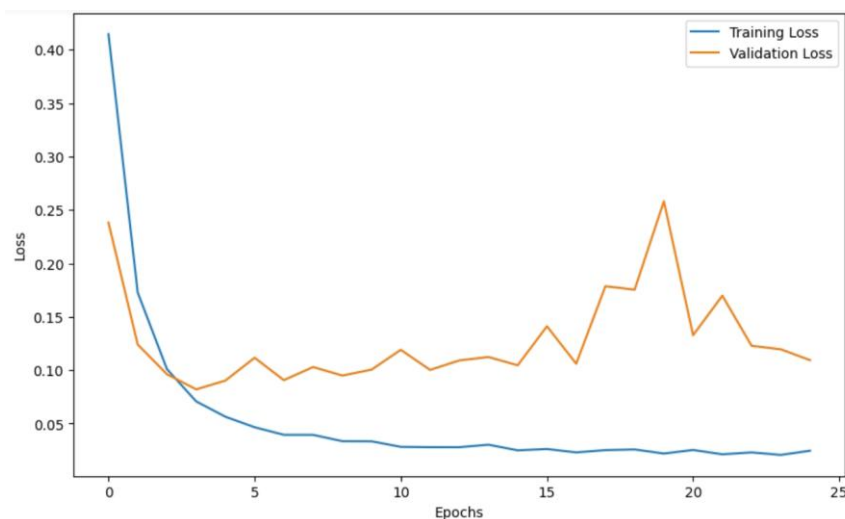


Figure 3. Loss over epoch CNN

Figure 4 presents the confusion matrix for binary classification using this CNN model, illustrating the comparison between the expected predictions and the actual classification results. The diagonal elements represent the number of true positives (correct predictions for real faces) and true negatives (correct predictions for fake faces). In Figure 4, it can be seen that the model produced 9,583 correct predictions for real faces (true positives) and 9,827 correct predictions for fake faces (true negatives). However, the model

also produced 417 incorrect predictions for real faces that were classified as fake (false negatives) and 173 fake faces that were incorrectly classified as real faces (false positives). Although the number of errors is relatively small, this indicates that the model is better at detecting fake faces than real faces, as reflected in the high recall value.

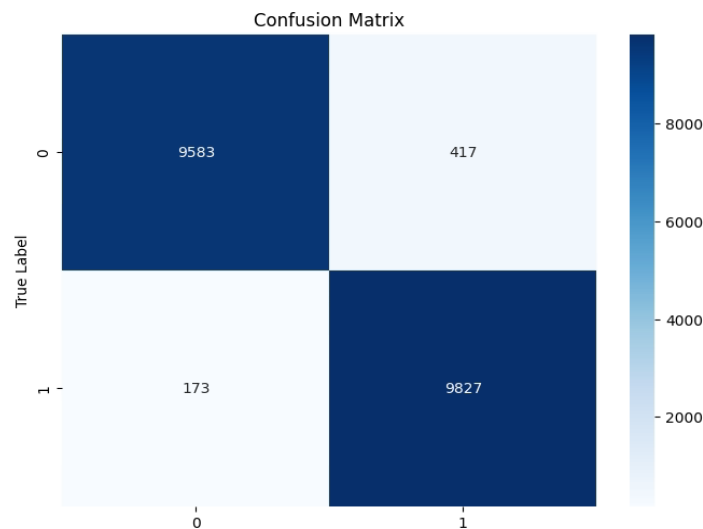


Figure 4. CNN confusion matrix results

### 3.2. Discussion

The results of this study indicate that CNN can be effectively used to detect deepfakes, although there are still some challenges that need to be addressed. The accuracy of 81.3% obtained is still below the optimal performance, which may be attributed to several factors, such as limited datasets or model parameters that have not been fully optimized. In future research, various approaches, such as increasing the amount of data or using more complex optimization techniques, can be explored to improve model performance. CNN has been shown to recognize complex visual patterns in images, making it suitable for tasks such as deepfake detection that require a deep understanding of visual features. CNN successfully distinguishes deepfake faces from real faces with a reasonable level of accuracy and offers advantages in terms of ease of implementation and flexibility in modifying the architecture.

Although CNN's performance in detecting deepfakes is quite satisfactory, there are several limitations that need to be considered. One major challenge is the potential for overfitting on the existing datasets, where the model may learn to classify the training data too specifically but fail to generalize well to new data. Furthermore, although data augmentation has been applied, a wider variety of datasets is needed to handle different types of deepfakes that may be more difficult to detect.

The results of this study have significant implications in efforts to prevent the misuse of deepfake technology. As deepfake technology continues to advance, deep learning-based detection methods such as CNNs can be an essential tool in mitigating the spread of fake content on the internet. Potential future developments include combining CNNs with other, more complex architectures or ensemble techniques to improve performance, as well as applying these methods to real-time video data for further detection.

The results of the CNN model in this study are generally consistent with previous studies using similar methods. For example, research by Sharma *et al.* [14] also showed that CNNs are able to detect deepfakes with an accuracy of over 80%, particularly on high-resolution images. However, this study also indicates that the use of more complex models, such as ResNet or ensemble learning techniques, can further improve accuracy, highlighting an opportunity for future research.

## 4. CONCLUSION

This study successfully developed a deepfake detection method based on a CNN architecture, achieving a fairly good accuracy rate of 81.3%. This method has been proven capable of identifying the differences between real faces and deepfakes using visual features extracted by the CNN. However, these results indicate that there is still room for improvement, particularly in handling high-quality and more

complex deepfakes. The evaluation metrics, such as precision and recall values exceeding 95%, demonstrate that the model is highly effective in detecting deepfake faces, but it is slightly less optimal in detecting real faces. For future research, further development can focus on expanding the variety of datasets and implementing more complex deep learning techniques, such as ensemble learning or the use of more advanced neural network architectures. The results of this study have the potential to help mitigate the risk of spreading fake content, particularly in applications that require identity authentication and digital security.

## ACKNOWLEDGEMENTS

Our appreciation to Universitas Multimedia Nusantara for providing the essential resources that made this research possible. Finally, we would like to thank our dedicated students for their invaluable assistance throughout the research process.

## FUNDING INFORMATION

This research was funded by Universitas Multimedia Nusantara. The authors gratefully acknowledge the support provided by the university.

## AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Fenina Adline Twince Tobing	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Adhi Kusnadi	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Ivranza Zuhdi Pane	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Rangga Winantyo	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

C : **C**onceptualization

M : **M**ethodology

So : **S**oftware

Va : **V**alidation

Fo : **F**ormal analysis

I : **I**nvestigation

R : **R**esources

D : **D**ata Curation

O : Writing - **O**riginal Draft

E : Writing - Review & **E**editing

Vi : **V**isualization

Su : **S**upervision

P : **P**roject administration

Fu : **F**unding acquisition

## CONFLICT OF INTEREST STATEMENT

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

## INFORMED CONSENT

We have obtained informed consent from all individuals included in this study.

## ETHICAL APPROVAL

The research related to human use has been complied with all the relevant national regulations and institutional policies in accordance with the tenets of the Helsinki Declaration and has been approved by the authors' institutional review board or equivalent committee

## DATA AVAILABILITY

The authors confirm that the data supporting the findings of this study are available within the article.




## REFERENCES

- [1] H. Benbya, T. H. Davenport, and S. Pachidi, "Artificial intelligence in organizations: current state and future opportunities," *SSRN Electronic Journal*, vol. 19, no. 4, pp. ix–xxi, 2020, doi: 10.2139/ssrn.3741983.




- [2] S. Kingra, N. Aggarwal, and N. Kaur, "Emergence of deepfakes and video tampering detection approaches: a survey," *Multimedia Tools and Applications*, vol. 82, no. 7, pp. 10165–10209, Mar. 2023, doi: 10.1007/s11042-022-13100-x.
- [3] S. Karnouskos, "Artificial Intelligence in Digital Media: The Era of Deepfakes," in *IEEE Transactions on Technology and Society*, vol. 1, no. 3, pp. 138–147, Sept. 2020, doi: 10.1109/TTS.2020.3001312.
- [4] J. T. Hancock and J. N. Bailenson, "The social impact of deepfakes," *Cyberpsychology, Behavior, and Social Networking*, vol. 24, no. 3, pp. 149–152, Mar. 2021, doi: 10.1089/cyber.2021.29208.jth.
- [5] K. A. Pamtselev, "The malicious use of AI-based deepfake technology as the new threat to psychological security and political stability," in *Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity*, Springer Publishing, 2020, pp. 37–55.
- [6] H. Navidan *et al.*, "Generative adversarial networks (GANs) in networking: a comprehensive survey & evaluation," *Computer Networks*, vol. 194, p. 108149, Jul. 2021, doi: 10.1016/j.comnet.2021.108149.
- [7] B. Khoo, R. C. -W. Phan, and C. Lim, "Deepfake attribution: on the source identification of artificially generated images," *WIREs Data Mining and Knowledge Discovery*, vol. 12, no. 3, May 2022, doi: 10.1002/widm.1438.
- [8] A. de Rancourt-Raymond and N. Smaili, "The unethical use of deepfakes," *Journal of Financial Crime*, vol. 30, no. 4, pp. 1066–1077, May 2023, doi: 10.1108/JFC-04-2022-0090.
- [9] O. M. Davey and L. Sauerwein, "Deepfake in online fraud cases: the haze of artificial intelligence's accountability based on the international law," *Sriwijaya Crimen and Legal Studies*, vol. 1, no. 2, p. 89, Dec. 2023, doi: 10.28946/scls.v1i2.2654.
- [10] Y. Patel *et al.*, "Deepfake generation and detection: case study and challenges," *IEEE Access*, vol. 11, pp. 143296–143323, 2023, doi: 10.1109/ACCESS.2023.3342107.
- [11] S. R. Ahmed, E. Sonuc, M. R. Ahmed, and A. D. Duru, "Analysis survey on deepfake detection and recognition with convolutional neural networks," in *2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, Jun. 2022, pp. 1–7, doi: 10.1109/HORA55278.2022.9799858.
- [12] Z. Li, F. Liu, W. Yang, S. Peng, and J. Zhou, "A survey of convolutional neural networks: analysis, applications, and prospects," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 33, no. 12, pp. 6999–7019, Dec. 2022, doi: 10.1109/TNNLS.2021.3084827.
- [13] A. Karandikar, "Deepfake video detection using convolutional neural network," *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 9, no. 2, pp. 1311–1315, Apr. 2020, doi: 10.30534/ijatcse/2020/62922020.
- [14] J. Sharma, S. Sharma, V. Kumar, H. S. Hussein, and H. Alshazly, "Deepfakes classification of faces using convolutional neural networks," *Traitement du Signal*, vol. 39, no. 3, pp. 1027–1037, Jun. 2022, doi: 10.18280/ts.390330.
- [15] S. Rao, A. K. Verma, and T. Bhatia, "A review on social spam detection: challenges, open issues, and future directions," *Expert Systems with Applications*, vol. 186, p. 115742, Dec. 2021, doi: 10.1016/j.eswa.2021.115742.
- [16] T. Kattenborn, J. Leitloff, F. Schiefer, and S. Hinz, "Review on convolutional neural networks (CNN) in vegetation remote sensing," *ISPRS Journal of Photogrammetry and Remote Sensing*, vol. 173, pp. 24–49, Mar. 2021, doi: 10.1016/j.isprsjprs.2020.12.010.
- [17] "140k real and fake faces," *Kaggle*, 2020. <https://www.kaggle.com/xhlulu/140k-real-and-fake-faces> (accessed May 30, 2021).
- [18] D. Saxena and J. Cao, "Generative adversarial networks (GANs)," *ACM Computing Surveys*, vol. 54, no. 3, pp. 1–42, Apr. 2022, doi: 10.1145/3446374.
- [19] K. Maharana, S. Mondal, and B. Nemade, "A review: data pre-processing and data augmentation techniques," *Global Transitions Proceedings*, vol. 3, no. 1, pp. 91–99, Jun. 2022, doi: 10.1016/j.gltp.2022.04.020.
- [20] C. Shorten, T. M. Khoshgofaar, and B. Furht, "Text data augmentation for deep learning," *Journal of Big Data*, vol. 8, no. 1, p. 101, Dec. 2021, doi: 10.1186/s40537-021-00492-0.
- [21] A. Nurhopyah and U. Hasanah, "Dataset splitting techniques comparison for face classification on CCTV images," *IJCCS (Indonesian Journal of Computing and Cybernetics Systems)*, vol. 14, no. 4, p. 341, Oct. 2020, doi: 10.22146/ijccs.58092.
- [22] A. H. Khalifa, N. A. Zaher, A. S. Abdallah, and M. W. Fakhr, "Convolutional neural network based on diverse gabor filters for deepfake recognition," *IEEE Access*, vol. 10, pp. 22678–22686, 2022, doi: 10.1109/ACCESS.2022.3152029.
- [23] A. Rajesh, S. Tiwari, V. Gotecha, and N. Y. Kapadnis, "Deepfake detection using CNN," *Bulletin for Technology and History Journal*, vol. 24, no. 2, pp. 72–76, 2024, [Online]. Available: <https://www.researchgate.net/publication/378609583>.
- [24] A. Kusnadi, F. A. T. Tobing, M. Dafa, R. A. Zamzami, M. Tio, and A. A. Nurpasha, "Optimizing 3D face recognition with PCA and CNN for enhanced accuracy," in *2024 9th International Conference on Mechatronics Engineering (ICOM)*, Aug. 2024, pp. 20–26, doi: 10.1109/ICOM61675.2024.10652466.
- [25] W. H. Lopez Pinaya, S. Vieira, R. Garcia-Dias, and A. Mechelli, "Convolutional neural networks," in *Machine Learning*, Elsevier, 2020, pp. 173–191.
- [26] H. Hardjadinata, R. S. Oetama, and I. Prasatiawan, "Facial expression recognition using xception and DenseNet architecture," in *2021 6th International Conference on New Media Studies (CONMEDIA)*, Oct. 2021, pp. 60–65, doi: 10.1109/CONMEDIA53104.2021.9617173.
- [27] N.-D. Hoang, "Image processing-based spall object detection using gabor filter, texture analysis, and adaptive moment estimation (Adam) optimized logistic regression models," *Advances in Civil Engineering*, vol. 2020, no. 1, Jan. 2020, doi: 10.1155/2020/8829715.
- [28] Z. Xiong, Q. Guo, M. Liu, and A. Li, "Pan-sharpening based on convolutional neural network by using the loss function with no-reference," *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, vol. 14, pp. 897–906, 2021, doi: 10.1109/JSTARS.2020.3038057.
- [29] J. Zhou, A. H. Gandomi, F. Chen, and A. Holzinger, "Evaluating the quality of machine learning explanations: a survey on methods and metrics," *Electronics*, vol. 10, no. 5, p. 593, Mar. 2021, doi: 10.3390/electronics10050593.
- [30] F. S. Nahm, "Receiver operating characteristic curve: overview and practical use for clinicians," *Korean Journal of Anesthesiology*, vol. 75, no. 1, pp. 25–36, Feb. 2022, doi: 10.4097/kja.21209.
- [31] R. Yacouby and D. Axman, "Probabilistic extension of precision, recall, and F1 score for more thorough evaluation of classification models," in *Proceedings of the First Workshop on Evaluation and Comparison of NLP Systems*, 2020, pp. 79–91, doi: 10.18653/v1/2020.eval4nlp-1.9.
- [32] M. Hasnain, M. F. Pasha, I. Ghani, M. Imran, M. Y. Alzahrani, and R. Budiarto, "Evaluating trust prediction and confusion matrix measures for web services ranking," *IEEE Access*, vol. 8, pp. 90847–90861, 2020, doi: 10.1109/ACCESS.2020.2994222.
- [33] P. Arora, H. Kumar, and B. K. Panigrahi, "Prediction and analysis of COVID-19 positive cases using deep learning models: a descriptive case study of India," *Chaos, Solitons & Fractals*, vol. 139, p. 110017, Oct. 2020, doi: 10.1016/j.chaos.2020.110017.
- [34] I. M. Mannaa, O. N. El Gazayerly, A. A. Abdelbary, S. S. Saleh, and D. A. Mostafa, "Validated green spectroscopic manipulation of area under the curve (AUC) for estimation of Simvastatin: application to nano-structured lipid carriers and niosomal systems," *Journal of Research in Pharmacy*, vol. 27(1), no. 27(1), pp. 30–42, 2023, doi: 10.29228/jrp.285.






**BIOGRAPHIES OF AUTHORS**

**Fenina Adline Twince Tobing, S.Kom., M.Kom.,**    graduated with a Master's degree from the University of North Sumatra (USU) in 2015. Currently, she is an active Informatics lecturer at Universitas Multimedia Nusantara (UMN) in Jakarta, where she also serves as the Research Coordinator for the Faculty of Engineering and Informatics. She is a member of several professional associations such as IEEE (Institute of Electrical and Electronics Engineers), APTIKOM (Indonesian Association of Higher Education in Computer Science), and ASPPI (Association for Synergy of Service and Empowerment in Indonesia). In addition to her involvement in professional organizations, she is also active in social and community organizations, including the Dharma Wanita Persatuan (DWP) at the Jakarta Class II Correctional Institution. She can be contacted at email: fenina.tobing@umn.ac.id.






**Dr. Adhi Kusnadi, ST., M.Si.**    completed his undergraduate degree (S1) at Sriwijaya University in Palembang in 1996. He continued his education at IPB Bogor, majoring in computer science, and graduated with a Master's degree (S2) in 2008. He finished doctoral studies (S3) in computer science at IPB in 2024. He works as a permanent lecturer at Universitas Multimedia Nusantara in the Department of Informatics. He is actively involved in various professional associations, including the Indonesian Association of Lecturers and the National Education Commission. He can be contacted at email: adhi.kusnadi@umn.ac.id.



**Dr. Ivransa Zuhdi Pane, B.Eng., M.Eng.,**    completed his undergraduate (S1) and master's (S2) degrees at Kyushu Institute of Technology, Japan, in the field of computer science and systems engineering in 1992 and 1994, respectively. He obtained his doctoral degree (S3) from Kyushu University, Japan, in the field of electronics in 2010. Currently, he works as a Senior Expert Engineer at the National Research and Innovation Agency and as a lecturer in the Informatics Program at Universitas Multimedia Nusantara. He is actively engaged in research and development activities in the fields of information system engineering and expert systems. He can be contacted at email: ivransa.zuhdi@lecturer.umn.ac.id.



**Dr. Rangga Winantyo Ph.D. MSc, BCS,**    graduated with a Master's degree from the Digital Media, Universitat Lubeck, Germany. He obtained his doctoral degree (S3) Optoelektronics and Nanostructure Science, Shizuoka University, Japan. Currently, he works as a Senior lecturer in the Informatics Program at Universitas Multimedia Nusantara. He can be contacted at email: rangga.winantyo@umn.ac.id.