Literasi Nusantara
vol.5 no. 3, July 2025 – October 2025
https://journal.citradharma.org/index.php/literasinusantara/index

ISSN 2746 8208 (Online)
ISSN 2746 3575 (Print)

Face Anti-Spoofing Security: A Fusion of FaceNet and Blink Detection

Ryan Reynickha Fatullah [1], I Gede Susrama Mas Diyasa [2], Achmad Junaidi [3]

[1,2,3] Universitas Pembangunan Nasional Veteran, Jawa Timur, Surabaya, Indonesia
21081010214@student.upnjatim.ac.id , igsusrama.if@upnjatim.ac.id , achmadjunaidi.if@upnjatim.ac.id

DOI : *https://doi.org/10.56480/jln.v5i2.1592*

Received: April 28, 2025
Revised: May 25, 2025
Accepted: June 07, 2025

Abstract

This research aims to develop a face recognition system that can distinguish between real and fake faces, using FaceNet for face recognition, Support Vector Machine (SVM) for model building, and Dlib for eye blink detection as an anti-spoofing method. The system is designed to enhance security in identity verification applications, such as online exams. In this study, face images taken from 15 student identities were tested to identify the system's ability to recognize real and fake faces. The test results show that FaceNet successfully recognizes recognized faces with high probability, while Dlib is effective in detecting eye blinks used to distinguish real faces from potential spoofing. The system distinguishes unrecognized faces with low probability and detects fake faces through static Eye Aspect Ratio (EAR) values, demonstrating the ability to detect spoofing. The overall accuracy of the system reached 97%, although some improvements are still needed, especially for extreme lighting conditions and face positions. This research shows great potential in the use of face recognition and blink detection technologies to enhance security in online identity verification applications.

Keywords– *Facenet, Dlib, MTCNN, SVM, OpenCV*

© 2025 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution ShareAlike (CC BY SA) license (https://creativecommons.org/licenses/by sa/4.0/).

Literasi Nusantara. vol.5 no. 3, July 2025 – October 2025
ISSN 2746 8208 (Online) and ISSN 2746 3575 (Print)

1. Introduction

Face recognition, as a major branch of computer vision, has undergone remarkable advancements due to the integration of deep learning techniques. These improvements have significantly enhanced the accuracy and reliability of facial recognition systems across various industries, including security, social media, and healthcare. For instance, real-time facial identification is now widely used to strengthen security systems, authenticate social media accounts, and even assist in medical diagnostics by analyzing facial structures (H. Li, 2024). The ability to instantly verify identities has revolutionized these sectors, making processes more efficient and secure.

Beyond traditional applications, facial recognition technology is increasingly being adopted in the education sector (Purnomo, 2017). One notable implementation is in online examinations, which offer flexibility but also introduce risks such as cheating. A growing concern is “contract cheating” (Lancaster & Cotarlan, 2021), where students hire others to take exams on their behalf, exploiting weak supervision in digital learning environments (Pramadi et al., 2017). To combat this, institutions are turning to biometric verification methods, including facial recognition, to ensure that the registered student is the one actually taking the exam.

To address the challenges of online exam fraud, machine learning-based facial recognition systems, such as FaceNet, have emerged as an innovative solution (Ganidisastra & Bandung, 2021). FaceNet generates unique facial embeddings, significantly improving identification accuracy and system security (William et al., 2019). Unlike traditional methods that rely on simple image comparisons, FaceNet uses deep learning to create highly discriminative facial representations, reducing the likelihood of false matches. This makes it particularly effective for high-stakes assessments where identity verification is critical.

Despite its effectiveness, facial recognition alone is not foolproof, as fraudsters may attempt to bypass the system using photos or videos of the legitimate user. To counter such spoofing attacks, additional security measures

like blink detection using Dlib have been integrated (Akhdan et al., 2023). These anti-spoofing techniques help distinguish real users from static or dynamic forgeries, though they are not yet fully effective against sophisticated attacks. Combining facial recognition with liveness detection ensures a more robust authentication process, making it harder for imposters to deceive the system.

Research has demonstrated that deep learning-based models like FaceNet, particularly when pre-trained on large datasets such as VGGFace2, outperform traditional facial recognition methods like PCA or LDA (William et al., 2019). In some cases, these models achieve near-perfect accuracy rates of up to 100% on standardized datasets. This superiority stems from their ability to learn intricate facial features and generalize across different lighting conditions, angles, and expressions. As a result, deep learning models have become the preferred choice for applications requiring high precision, such as financial services and border control.

The performance of facial recognition systems heavily depends on the quality of the input data (Hernandez-Ortega et al., 2019). Factors such as image resolution, lighting, and occlusions can significantly affect accuracy. To mitigate these issues, preprocessing techniques like alignment and normalization are often applied. Additionally, using high-quality datasets during model training ensures better generalization in real-world scenarios. As biometric systems become more widespread, maintaining data integrity will remain a critical factor in their reliability and adoption.

The combination of facial recognition and anti-spoofing technologies presents a promising solution for securing online examinations (Yu et al., 2020). By continuously improving liveness detection and refining deep learning models, institutions can minimize cheating while maintaining the convenience of remote assessments. Future advancements may include multi-modal biometric systems that integrate facial recognition with voice or behavioral analysis for even stronger authentication. As these technologies evolve, they will play an increasingly vital role in upholding academic integrity in digital learning environments.

Literasi Nusantara. vol.5 no. 3, July 2025 – October 2025
ISSN 2746 8208 (Online) and ISSN 2746 3575 (Print)

2. Method

The methods used in this research include the Python library MTCNN for facial feature extraction, FaceNet for identity recognition (Qi et al., 2022), as well as eye blink detection using Dlib which is applied as an anti-spoofing mechanism to enhance the system's security against static image spoofing attacks. The flow of this methodology is described in Figure 1 below.

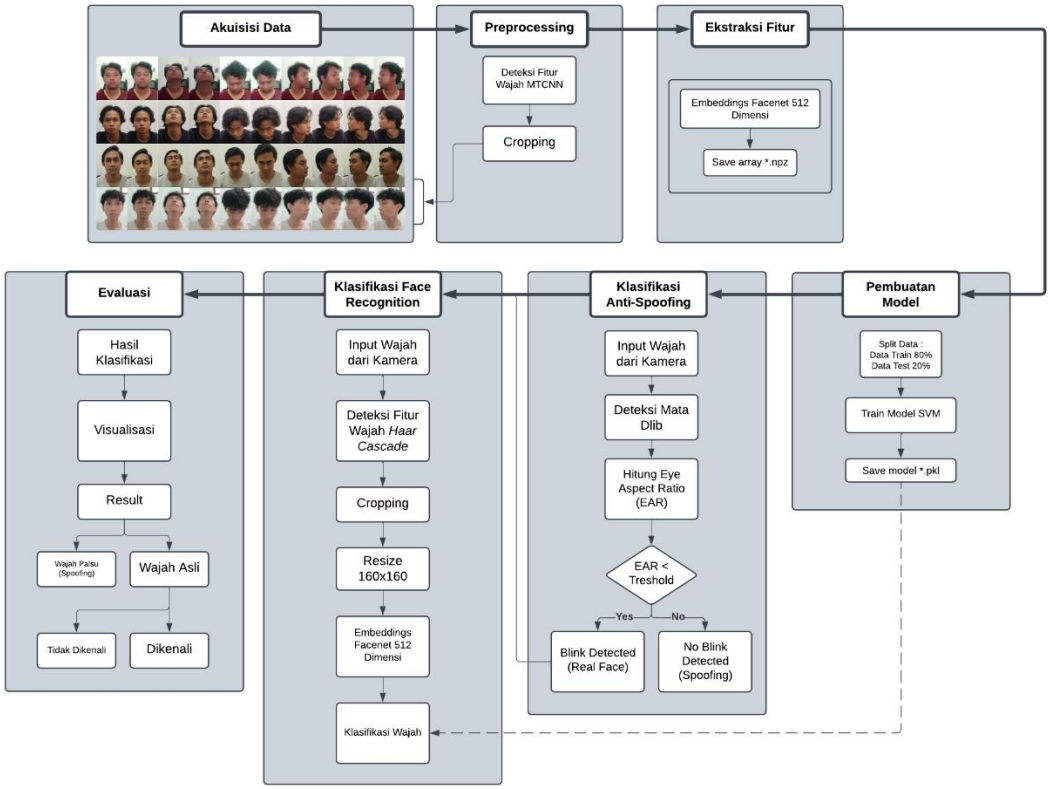

Figure 1. Research Flow

Based on Figure 1, this research starts with the data acquisition stage, where facial images are taken from 15 student identities with 10 images for each identity. These facial images were extracted from videos recorded using a smartphone with a 48MP camera, from which the ten best images for each identity were selected. The images were taken in several positions: facing the front, looking right, left, up, and down. This resulted in a total of 150 images ready for use.

In the preprocessing stage, each face image is processed through feature detection using a Multi Task Cascaded Neural Network (MTCNN), which

detects faces and extracts key keypoints, followed by cropping the image based on the detected bounding box. The image is then resized to 160x160 pixels for consistency with the standard FaceNet model input (Schroff et al., 2015). These processed facial features are then converted into embedding vectors with a dimension of 512, which will be used for further facial identification.

Model building using Support Vector Machine (SVM) algorithm optimized to handle embedding vectors from FaceNet (Ryando, C., Sigit, R., & Dewantara, 2023). SVM works by finding a hyperplane or boundary between classes that enables accurate face recognition (Susrama et al., 2024). Thus, when a new face is entered, the system can classify it based on the database that has been created. (Afifudin et al., 2024). The face dataset is divided into 80% for training and 20% for testing. After training, the model is tested to classify the recognized faces based on the database that has been created. This classification process uses a combination of OpenCV and Haar Cascade for face detection (Singh et al., 2024). Haar Cascade, especially haarcascade_frontalface_default.xml, was chosen because it has been widely applied in various face recognition applications (Susrama et al., 2022). Dlib to detect eye blinks as an anti-spoofing method. Eye blink is measured using the Eye Aspect Ratio (EAR) (X. Li et al., 2021) to distinguish between real faces and spoofing attacks.

The evaluation was conducted by measuring the accuracy of the system in recognizing registered faces and rejecting unregistered faces, as well as testing the spoofing detection capability with EAR parameters and probability levels. The results of this evaluation show that the model can accurately recognize identities while detecting spoofing, improving the security of the system in face-based identity verification applications.

3. Result and Discussion

The output of this research is the result of blink detection and classification of recognized or unrecognized faces.

Literasi Nusantara. vol.5 no. 3, July 2025 – October 2025
ISSN 2746 8208 (Online) and ISSN 2746 3575 (Print)

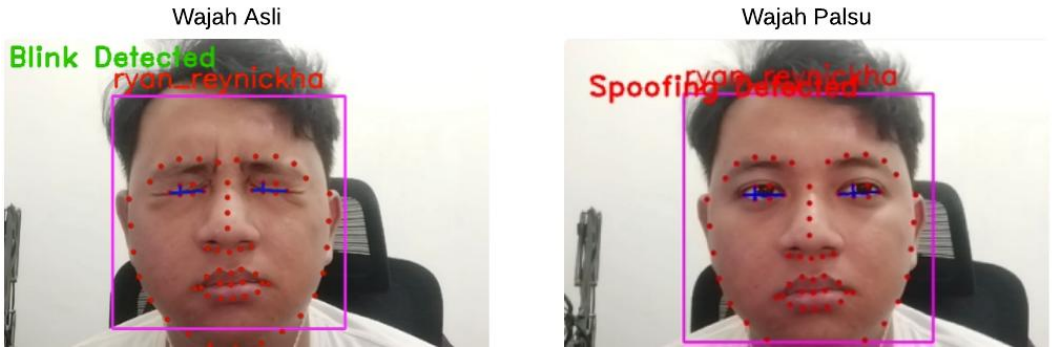

Figure 2. Classification Results of FaceNet and Dlib

As shown in Figure 2, this study presents a visualization of the results of eye blink detection and face classification. The eye blink detection process is performed using Dlib, which serves to verify the authenticity of the input face with an eyeblink detection approach. This approach plays an important role in distinguishing between real faces and potential spoofing attacks that use static images. After the blink detection phase, the detected faces are then classified as recognized or unrecognized based on the data that has been registered in the system.

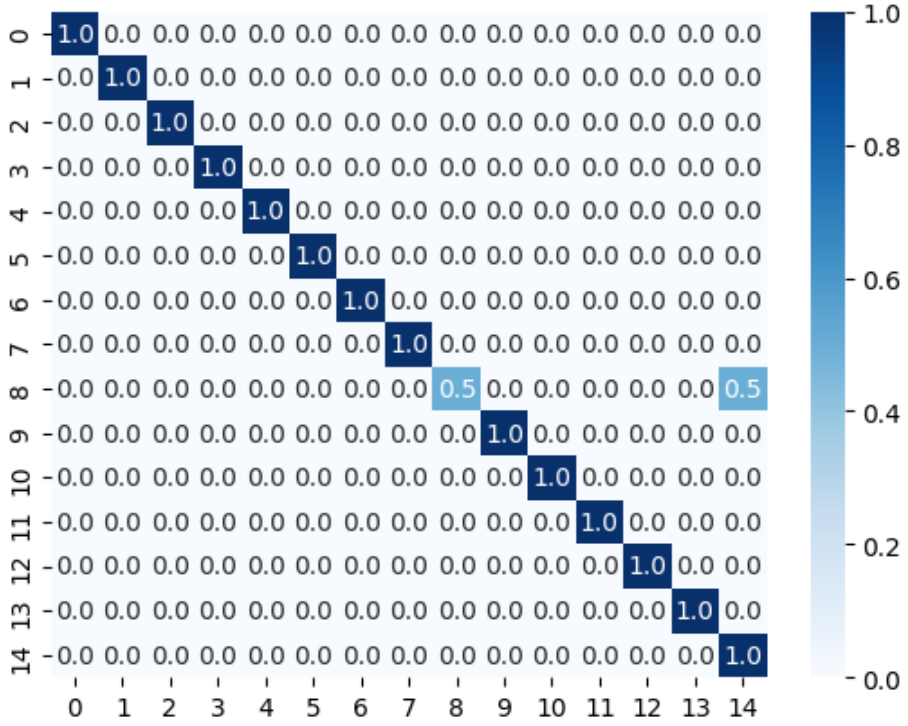

Figure 3. Confussion Matrix FaceNet

Based on Figure 3, the confusion matrix results, there is one significant misprediction, which is label 8 predicted as label 14. This indicates an error in the classification of student identities, which may be influenced by factors such as data quality or model limitations in distinguishing between very similar identities. Nonetheless, the accuracy obtained from the system was 97%. This indicates that the model has a very good accuracy in classifying student identities, despite the slight prediction error.

Table 1. Clasification report

	Precision	Precision	F1-Score	Support
AND	1.00	1.00	1.00	2
BUD	1.00	1.00	1.00	2
CTR	1.00	1.00	1.00	2
DAN	1.00	1.00	1.00	2
EKA	1.00	1.00	1.00	2
FJR	1.00	1.00	1.00	2
GNA	1.00	1.00	1.00	2
HNDR	1.00	1.00	1.00	2
IND	1.00	0.50	0.67	2
JKO	1.00	1.00	1.00	2
KKI	1.00	1.00	1.00	2
LNA	1.00	1.00	1.00	2
MRA	1.00	1.00	1.00	2
NNA	1.00	1.00	1.00	2
OMR	0.67	1.00	1.00	2
accuracy			0.97	30
macro avg	0.98	0.97	0.96	30
weighted avg	0.98	0.97	0.96	30

Based on the results shown in Table 1, the classification report shows that most of the labels have precision, recall, and F1-Score values of 1.00, indicating excellent model performance in classifying identities with high accuracy. However, there is one exception to the label ‘Beautiful’, where the recall value obtained is 0.50 and F1-Score 0.67, indicating an error in detecting the label. Nonetheless, overall, the model had an accuracy of 97%, with macro-averaged and weighted average values of 0.98 and 0.96, respectively.

Literasi Nusantara. vol.5 no. 3, July 2025 – October 2025
ISSN 2746 8208 (Online) and ISSN 2746 3575 (Print)

Table 2. Testing using a recognized real face

No	Name	Face Recognition (FaceNet)			EyeBlink Detection (Dlib)		
		Recognized?		Probability	Blink Detected?		Eye Aspect Ratio (EAR)
		Yes	No		Yes	No	
1	AND	✓	-	45.89	✓	-	0.482 – 1.053
2	BUD	✓	-	35.26	✓	-	0.260 – 0.634
3	CTR	✓	-	41.77	✓	-	0.440 – 0.838
4	DAN	✓	-	39.68	✓	-	0.420 – 0.948
5	EKA	✓	-	36.67	✓	-	0.390 – 0.879
6	FJR	✓	-	39.43	✓	-	0.257 – 0.925
7	GNA	✓	-	40.17	✓	-	0.448 – 0.934
8	HNDR	✓	-	39.65	✓	-	0.303 – 1.197
9	IND	✓	-	38.90	✓	-	0.312 – 0.812
10	JKO	✓	-	45.09	✓	-	0.468 – 1.039
11	KKI	✓	-	33.65	✓	-	0.312 – 1.055
12	LNA	✓	-	31.78	✓	-	0.271 – 0.909
13	MRA	✓	-	52.30	✓	-	0.359 – 0.994
14	NNA	✓	-	35.81	✓	-	0.453 – 0.742
15	OMR	✓	-	42.06	✓	-	0.240 – 0.797

Based on Table 2, the test results using recognized real faces show that the FaceNet face recognition system successfully recognizes all faces, as seen in Andi's probability value which reaches 45.89. In addition, eye blink detection using Dlib shows changes in the Eye Aspect Ratio (EAR) value, which serves to distinguish real faces from potential spoofing. The EAR value varies between individuals, as in Hendra (0.303 - 1.197), which indicates the effectiveness of eye blink detection as an anti-spoofing mechanism.

Table 3. testing using recognized fake faces

No	Name	Face Recognition (FaceNet)			EyeBlink Detection (Dlib)		
		Recognized?		Probability	Blink Detected?		Eye Aspect Ratio (EAR)
		Yes	No		Yes	No	
1	AND	✓	-	45.45	-	✓	0.586
2	BUD	✓	-	35.55	-	✓	0.447
3	CTR	✓	-	42.19	-	✓	0.678
4	DAN	✓	-	39.95	-	✓	0.477
5	EKA	✓	-	36.82	-	✓	0.408
6	FJR	✓	-	39.58	-	✓	0.667
7	GNA	✓	-	39.97	-	✓	0.715
8	HNDR	✓	-	39.39	-	✓	1.114
9	IND	✓	-	38.44	-	✓	0.617
10	JKO	✓	-	44.94	-	✓	0.751
11	KKI	✓	-	33.55	-	✓	0.390
12	LNA	✓	-	31.34	-	✓	0.358
13	MRA	✓	-	52.63	-	✓	0.956
14	NNA	✓	-	35.44	-	✓	0.539
15	OMR	✓	-	42.28	-	✓	0.614

Based on Table 3, the test results show that the FaceNet face recognition system successfully recognizes fake faces in all tested individuals, as seen in Andi's probability value which reaches 45.45. However, eye blinks are not detected in every individual, which is characterized by no change in the Eye Aspect Ratio (EAR) value which is below the threshold. The detected EAR remains in a static range, such as Budi who has an EAR value of 0.447. This shows that even though the EAR value is below the threshold, the absence of change in the EAR value indicates that the face is detected as spoofing.

Literasi Nusantara. vol.5 no. 3, July 2025 – October 2025
ISSN 2746 8208 (Online) and ISSN 2746 3575 (Print)

Table 4. Testing using an unrecognized real face

No	Name	Face Recognition (FaceNet)			EyeBlink Detection (Dlib)		
		Recognized ?		Probability	Blink Detected?		Eye Aspect Ratio (EAR)
		Yes	No		Yes	No	
1	AND	-	✓	13.39	✓	-	0.528 – 1.065
2	BUD	-	✓	13.92	✓	-	0.293 – 0.596
3	CTR	-	✓	19.29	✓	-	0.446 – 0.871
4	DAN	-	✓	19.22	✓	-	0.387 – 0.976
5	EKA	-	✓	14.55	✓	-	0.401 – 0.843
6	FJR	-	✓	12.04	✓	-	0.248 – 0.967
7	GNA	-	✓	15.50	✓	-	0.452 – 0.927
8	HNDR	-	✓	16.89	✓	-	0.296 – 1.208
9	IND	-	✓	18.49	✓	-	0.315 – 0.859
10	JKO	-	✓	17.09	✓	-	0.478 – 0.992
11	KKI	-	✓	13.62	✓	-	0.273 – 1.083
12	LNA	-	✓	15.80	✓	-	0.268 – 0.928
13	MRA	-	✓	18.78	✓	-	0.340 – 1.036
14	NNA	-	✓	14.42	✓	-	0.453 – 0.697
15	OMR	-	✓	16.26	✓	-	0.201 – 0.838

Based on Table 4, the test results of the FaceNet face recognition system successfully distinguish the original unrecognized face with a low probability, as in Identity 1 with a value of 13.39. An eye blink is detected in each identity, which is characterized by a change in the Eye Aspect Ratio (EAR) value. The detected EAR values remain below the threshold, such as in Identity 2 (0.293 - 0.596), which indicates that even though eye blinks are detected, the system still identifies the face as a fully unrecognized original.

Table 5. Tests using unrecognized fake faces

No	Name	Face Recognition (FaceNet)			EyeBlink Detection (Dlib)		
		Recognized?		Probability	Blink Detected?		Eye Aspect Ratio (EAR)
		Yes	No		Yes	No	
1	AND	-	✓	13.17	-	✓	0.796
2	BUD	-	✓	13.52	-	✓	0.445
3	CTR	-	✓	19.15	-	✓	0.658
4	DAN	-	✓	19.53	-	✓	0.681
5	EKA	-	✓	14.67	-	✓	0.622
6	FJR	-	✓	12.06	-	✓	0.607
7	GNA	-	✓	15.58	-	✓	0.690
8	HNDR	-	✓	16.88	-	✓	0.752
9	IND	-	✓	18.23	-	✓	0.587
10	JKO	-	✓	16.63	-	✓	0.735
11	KKI	-	✓	13.49	-	✓	0.678
12	LNA	-	✓	16.15	-	✓	0.598
13	MRA	-	✓	18.39	-	✓	0.688
14	NNA	-	✓	14.67	-	✓	0.575
15	OMR	-	✓	16.60	-	✓	0.519

Based on the test results shown in Table 5, the system successfully differentiates the fake unrecognized faces well. In each identity, the wink is not detected with a static Eye Aspect Ratio (EAR) value, and the system identifies the face as unrecognized with a low probability, such as in Identity 1 which has a probability of 13.17. The detected EAR remained static, such as in Identity 2 with an EAR of 0.445, which did not change significantly.

4. Conclusion

Based on the research results presented, the face recognition system using FaceNet and eye blink detection with Dlib shows significant performance in identifying real and fake faces. In tests with recognized real faces, the system successfully detects eye blinks and classifies faces with a high probability, and

Literasi Nusantara. vol.5 no. 3, July 2025 – October 2025
ISSN 2746 8208 (Online) and ISSN 2746 3575 (Print)

shows changes in Eye Aspect Ratio (EAR) values that can distinguish real faces from potential spoofing. However, there was one exception with the label 'Beautiful' that showed an error in detecting the eye blink, which affected the recall and F1-Score values.

In the test with recognized fake faces, the system also successfully recognized fake faces, even though eye blinks were not detected with significant changes in the EAR values that were below the threshold. This indicates that the system can distinguish the fake faces based on the low probability and static EAR value, even if the wink is detected in each identity.

In conclusion, the system is effective in identifying both real and fake faces, with a high accuracy rate of 97%. However, there are some areas that need improvement, especially in detecting faces in a wide variety of lighting conditions and extreme face positions that can affect the performance of the model.

References

Afifudin, M., Junaedi, A., Nugroho, A., Fithriyah, I., Pembangunan, U., Veteran, N., Timur, J., & Anyar, G. (2024). *GWO-SVM : An Approach To Improving Svm Performance Using Grey Wolf Optimizer In Intellectual Disability Classification*. *12*(3), 4440–4453. https://doi.org/10.23960/jitet.v12i3S1.5359

Akhdan, S. R., Supriyanti, R., & Nugroho, A. S. (2023). Face recognition with anti spoofing eye blink detection. *AIP Conference Proceedings*, *2482*(February). https://doi.org/10.1063/5.0113512

Ganidisastra, A. H. S., & Bandung, Y. (2021). An Incremental Training on Deep Learning Face Recognition for M-Learning Online Exam Proctoring. *Proceedings - 2021 IEEE Asia Pacific Conference on Wireless and Mobile, APWiMob 2021*, 213–219. https://doi.org/10.1109/APWiMob51111.2021.9435232

Hernandez-Ortega, J., Galbally, J., Fierrez, J., Haraksim, R., & Beslay, L. (2019). FaceQnet: Quality Assessment for Face Recognition based on Deep Learning. *2019 International Conference on Biometrics, ICB 2019*. https://doi.org/10.1109/ICB45273.2019.8987255

Lancaster, T., & Cotarlan, C. (2021). Contract cheating by STEM students through a file sharing website: a Covid-19 pandemic perspective. *International*

Journal for Educational Integrity, *17*(1), 1–17. https://doi.org/10.1007/s40979-021-00070-0

Li, H. (2024). *The application and challenges of different face recognition technologies in the three major fields of security , social media , and medical care*. *0*, 174–181. https://doi.org/10.54254/2755-2721/95/2024CH0051

Li, X., Luo, J., Duan, C., Zhi, Y., & Yin, P. (2021). Real-time detection of fatigue driving based on face recognition. *IOP Conference Series: Earth and Environmental Science*, *1802*(2). https://doi.org/10.1088/1742-6596/1802/2/022044

Pramadi, A., Pali, M., Hanurawan, F., & Atmoko, A. (2017). Academic Cheating in School: A Process of Dissonance Between Knowledge and Conduct. *Mediterranean Journal of Social Sciences*, *8*(6), 155–162. https://doi.org/10.1515/mjss-2017-0052

Purnomo, D. (2017). Model Prototyping Model Prototyping Pada Pengembangan Sistem Informasi. *JIMP-Jurnal Informatika Merdeka Pasuruan*, *2*(2), 54–61. https://doi.org/10.37438/jimp.v2i2.67

Qi, S., Zuo, X., Feng, W., & Naveen, I. G. (2022). Face Recognition Model Based on MTCNN and Facenet. *2022 IEEE 2nd International Conference on Mobile Networks and Wireless Communications, ICMNWC 2022*, 1–5. https://doi.org/10.1109/ICMNWC56175.2022.10031806

Ryando, C., Sigit, R., & Dewantara, B. S. B. (2023). Comparison of Machine Learning Algorithms for Face Classification Using FaceNet Embeddings. *Indonesian Journal of Computer Science*, *12*(2), 284–301. http://ijcs.stmikindonesia.ac.id/ijcs/index.php/ijcs/article/view/3135

Schroff, F., Kalenichenko, D., & Philbin, J. (2015). FaceNet: A unified embedding for face recognition and clustering. *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, *07-12-June*, 815–823. https://doi.org/10.1109/CVPR.2015.7298682

Singh, A. K., Krishna, S., & Poongodi, T. (2024). Face Recognition System Using Haar Cascade and LBP Classifier. *Proceedings of International Conference on Communication, Computer Sciences and Engineering, IC3SE 2024*, 99–104. https://doi.org/10.1109/IC3SE62002.2024.10593491

Susrama, I. G., Diyasa, M., Arman, D., Ayu, H., & Kuswardhani, C. (2024). *Detection of Abnormal Human Sperm Morphology Using Support Vector Machine (SVM) Classification*. *2*(2), 57–63. https://doi.org/10.33005/itij.v2i2.36

Susrama, I. G., Diyasa, M., Putra, A. H., Rafka, M., & Ariefwan, M. (2022). *Feature Extraction for Face Recognition Using Haar Cascade Classifier*. *2022*, 197–206. https://doi.org/10.11594/nstp.2022.2432

William, I., Ignatius Moses Setiadi, D. R., Rachmawanto, E. H., Santoso, H. A., & Sari, C. A. (2019). Face Recognition using FaceNet (Survey, Performance

Literasi Nusantara. vol.5 no. 3, July 2025 – October 2025
ISSN 2746 8208 (Online) and ISSN 2746 3575 (Print)

Test, and Comparison). *Proceedings of 2019 4th International Conference on Informatics and Computing, ICIC 2019*. https://doi.org/10.1109/ICIC47613.2019.8985786

Yu, Z., Zhao, C., Wang, Z., Qin, Y., Su, Z., Li, X., Zhou, F., & Zhao, G. (2020). Searching central difference convolutional networks for face anti-spoofing. *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, 5294–5304. https://doi.org/10.1109/CVPR42600.2020.00534