VOL. 10. NO. 3 FEBRUARY 2025
P-ISSN: 2685-8223 | E-ISSN: 2527-4864
DOI: 10.33480 /jitk.v10i3.5992

JITK (JURNAL ILMU PENGETAHUAN DAN TEKNOLOGI KOMPUTER)

SMART ATTENDANCE TRACKING SYSTEM EMPLOYING DEEP LEARNING FOR FACE ANTI-SPOOFING PROTECTION

Bani Nurhakim[1]; Ahmad Rifai[2*]; Dian Ade Kurnia[3]; Dadang Sudrajat[4]; Ujang Supriatna[5]

Informatics Management[1, 3], Information Technology[2, 4, 5]
STMIK IKMI Cirebon, Cirebon, Indonesia[1, 2, 3, 4, 5]
www.ikmi.ac.id[1, 2, 3, 4, 5]
baninurhakim@gmail.com[1], rifai.ahmad90@gmail.com[2*], dianade2014@gmail.com[3],
dias_sudrajat@yahoo.com[4], ujangsupriatna125@gmail.com[5]

(*) Corresponding Author
(Responsible for the Quality of Paper Content)

Abstract— *Conventional attendance systems face challenges in accuracy and efficiency, often vulnerable to spoofing and data manipulation. This study addresses these issues by developing a smart attendance system integrating Deep Learning-based facial recognition with anti-spoofing technology. The system ensures secure and reliable attendance authentication while automating and enhancing management processes. Utilizing a convolutional neural network (CNN) architecture, the system processes raw facial images directly without additional feature extraction, improving accuracy and efficiency. A novel training strategy, termed 50 Random Samples-30 Sub-epochs Count-1 Epoch, is introduced to optimize the training process. This strategy involves random sampling during each forward pass and grouping 30 passes as one epoch, enabling the use of complex CNN architectures and automatic dataset expansion. The system achieves 98.90% accuracy in identifying genuine attendance, maintaining a confidence level above 80%, significantly reducing spoofing risks and errors. This innovative solution has significant implications, particularly for educational institutions. It automates attendance tracking, minimizes manual effort, reduces errors, and supports disciplinary enforcement through accurate data. Moreover, its scalability allows for application across various environments, offering benefits to a wide range of institutions. By enhancing data accuracy and operational efficiency, this system sets a foundation for smarter, more reliable attendance management, strengthening administrative practices in education and beyond.*

Keywords: *anti-spoofing, deep learning, openCV, smart attendance, system performance.*

Intisari— *Sistem absensi konvensional menghadapi tantangan dalam hal akurasi dan efisiensi, sering kali rentan terhadap pemalsuan dan manipulasi data. Studi ini mengatasi masalah tersebut dengan mengembangkan sistem absensi pintar yang mengintegrasikan pengenalan wajah berbasis Deep Learning dengan teknologi anti-pemalsuan. Sistem ini memastikan autentikasi absensi yang aman dan andal sekaligus mengotomatiskan serta meningkatkan proses pengelolaan. Menggunakan arsitektur convolutional neural network (CNN), sistem ini memproses gambar wajah mentah secara langsung tanpa memerlukan ekstraksi fitur tambahan, sehingga meningkatkan akurasi dan efisiensi. Strategi pelatihan baru, yang disebut 50 Random Samples-30 Sub-epochs Count-1 Epoch, diperkenalkan untuk mengoptimalkan proses pelatihan. Strategi ini melibatkan pengambilan sampel secara acak selama setiap forward pass dan mengelompokkan 30 forward pass sebagai satu epoch, memungkinkan penggunaan arsitektur CNN yang kompleks serta ekspansi dataset secara otomatis. Sistem ini mencapai tingkat akurasi 98,90% dalam mengidentifikasi kehadiran yang sah dengan tingkat kepercayaan lebih dari 80%, secara signifikan mengurangi risiko pemalsuan dan kesalahan data. Solusi inovatif ini memiliki dampak besar, khususnya bagi institusi pendidikan. Sistem ini mengotomatiskan pelacakan absensi, meminimalkan upaya manual, mengurangi kesalahan, dan mendukung penegakan disiplin melalui data yang akurat. Selain itu, skalabilitasnya memungkinkan penerapan di berbagai lingkungan, memberikan manfaat bagi berbagai institusi. Dengan meningkatkan* *akurasi data dan efisiensi operasional, sistem ini menjadi dasar pengelolaan absensi yang lebih cerdas dan andal, memperkuat praktik administrasi di sektor pendidikan dan lainnya.*

Kata Kunci: *anti-spoofing, deep learning, openCV, sistem kehadiran cerdas, kinerja sistem.*

INTRODUCTION

Effectively managing educational staff attendance in a university setting is essential and requires a focus on efficiency, accuracy, and transparency. Although conventional attendance systems are still widely used, the increasing complexity of modern higher education calls for a more advanced and adaptive solution. Implementing information technology (IT), specifically facial recognition and anti-spoofing technologies, offers a novel approach to overcoming these challenges [1] [2] [3].

Key challenges in attendance management include low efficiency and the susceptibility of manual recording systems to errors, which makes them less adaptable to the needs of modern educational institutions [4] [5]. Traditional methods are inadequate for ensuring accurate, efficient, and responsive attendance tracking in the evolving landscape of higher education[6][2]. This research aims to develop and implement an intelligent attendance system utilizing facial recognition technology with anti-spoofing capabilities through the Deep Learning method [3] [7]. The study focuses on improving the recording of educational staff attendance in higher education institutions, with the goal of enhancing efficiency, accuracy, and responsiveness to the dynamic nature of contemporary academia [8][9] [10].

This study utilizes a Deep Learning approach for facial recognition in an attendance system based on facial features, enhanced with anti-spoofing techniques. The method involves breaking down the facial detection process into multiple complex stages to boost efficiency and speed [11]. Detection accuracy is improved by training a classifier with both positive and negative facial images and employing the Adaboost technique [12]. The inclusion of anti-spoofing techniques ensures the authenticity of detected faces, providing an added layer of security to the recognition process. This results in fast, efficient, and secure facial recognition, facilitating effective management of educational staff attendance [13] [2].

The research results show that the facial recognition-based attendance system, which incorporates anti-spoofing and uses Deep Learning methods, achieved an average accuracy rate of 98.90%. This technology ensures reliable and precise attendance recording. Confidence levels exceeding 80% reflect a thorough facial identification process, effectively addressing various challenges and reinforcing the integrity of attendance data. Additionally, this research fosters further discussion and collaboration in facial recognition technology at STMIK IKMI Cirebon, potentially leading to improved and more dependable innovations in attendance management at the institution[3].

This study contributes by applying facial texture detection for anti-spoofing technology using the Local Binary Patterns (LBP) method. LBP was chosen for its effectiveness in detecting fine texture patterns on real human faces, as opposed to static images or video [6][13]. This technique works by dividing the face into small cells and analyzing pixel intensity changes within each cell. The patterns generated from LBP analysis can distinguish a real face from a manipulated one, as real faces exhibit more complex and natural texture variations [4].

Overall, the study is crucial for advancing the understanding and application of facial recognition technology in managing attendance at STMIK IKMI Cirebon.

MATERIALS AND METHODS

The stages of research involved in developing an attendance system that utilizes facial recognition technology and anti-spoofing measures include:

Data Collection

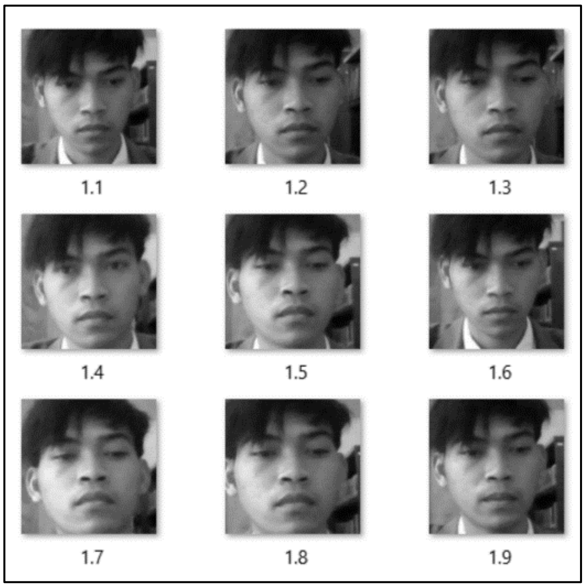
The data for developing the attendance system was gathered by sampling facial images of the educational staff at STMIK IKMI Cirebon, who served as the study's subjects. The images were captured using a camera integrated with facial recognition software, automatically generating 100 images per user [14][15].

This process in Figure 1 forms the core foundation for building and testing the reliability of the attendance system under development.

Source: (Research Results, 2024)
Figure 1. Sample Results of Image Acquisition

Pre-processing of Data

The image processing in the system consists of several stages, including image normalization, facial detection, and filtering out images that do not meet the criteria. RGB images typically have a bit depth of 24, with 8 bits allocated to each color channel (red, green, and blue). In contrast, grayscale images generally have a single 8-bit depth [16] [17]. This difference highlights the complexity of color information processed in the system. Each image is 300x300 pixels in size, saved under the name 'image_id' and sequenced accordingly, such as Figure 2.



Source: (Research Results, 2024)
Figure 2. Example of Image Processing of Data

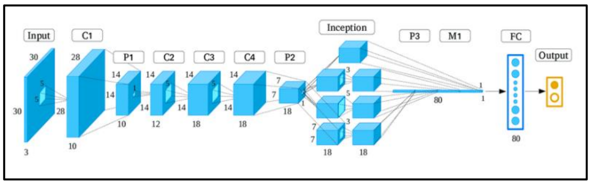
Development of Facial Recognition Model

The architecture consists of several main layers, namely the input layer, hidden layers that may include convolutional layers, pooling layers, and fully connected layers [4].

This study utilizes a convolutional neural network (CNN) architecture designed as an end-to-end system specifically for *face anti-spoofing*. This approach processes raw facial images directly as input to the corresponding output class without requiring additional feature extraction steps. Furthermore, an innovative training strategy has been developed to enable the use of more complex convolutional neural network architectures for *face anti-spoofing* detection while simultaneously facilitating the automated expansion of the training dataset.

The applied training strategy, known as *50 Random Samples-30 Sub-epochs Count-1 Epoch*, involves random sampling of the training data during each forward pass through the convolutional neural network. Subsequently, 30 forward passes are counted as one complete epoch.

To evaluate the effectiveness of this approach, the VGG-11 network and two of its variants were trained using the CASIA-FASD dataset for *face anti-spoofing* detection. The experimental results demonstrate that this approach significantly improves accuracy across various *spoofing* scenarios. The proposed method achieved a minimum Error Rate (EER) of 5%, highlighting its great potential for broader applications.

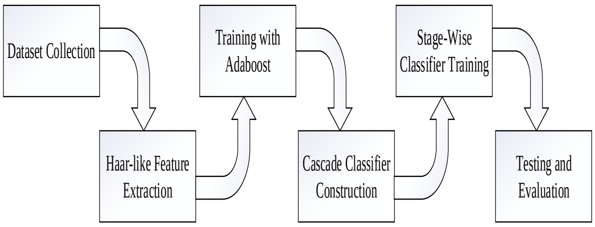


Source: (Research Results, 2024)
Figure 3. Architecture

The neural network architecture in deep learning in Figure 3 is designed for image or face recognition. This network starts with an input layer that receives an image of 32 x 32 pixels with 3 color channels (RGB) [17]. Then, the network is equipped with several convolutional layers that function to extract features from the input image using specific filters. Each convolutional layer produces an output with lower resolution but higher depth, allowing the network to capture more specific features from the image. After several convolutional layers, there is a pooling layer that serves to reduce the spatial dimensions of the convolutional output while retaining important information. Pooling, usually max pooling, takes the maximum value from a certain window to simplify the data and improve processing efficiency.

This architecture also includes an inception module, which is a module with parallel convolutional paths that use filters of various sizes (such as 1x1, 3x3, and 5x5). This module enables the network to capture information at different scales, generating richer and more complex feature representations from the input data. After passing through the convolutional, pooling, and inception layers, the network forwards the results to the fully connected layer, which connects all neurons from the previous layer to perform classification [18].

Face recognition is implemented using the Deep Learning approach. This method involves training a classifier with a dataset of both positive and negative face images. The Adaboost technique is applied to improve detection accuracy [10]. The Adaboost process starts by assigning equal initial weights to each data sample. At each iteration, weak models, such as decision stumps, which are simple classifiers based on a single feature, are generated. These weak models are selected based on their ability to minimize prediction errors, with their weights adjusted according to their error rates. Misclassified samples have their weights updated to focus on correcting errors as shown in Figure 4. In the end, the combination of all weak models and their respective weights creates a stronger model, representing the final result of the Adaboost iteration [6].


Dataset Collection
Haar-like Feature Extraction
Training with Adaboost
Cascade Classifier Construction
Stage-Wise Classifier Training
Testing and Evaluation

Source: (Research Results, 2024)

Figure 4. Phases of Facial Recognition Model Development

Integration of Anti-Spoofing Technology

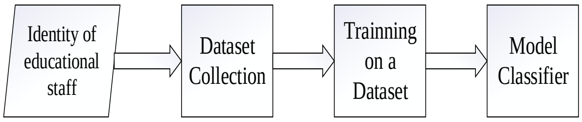
In addition to facial recognition, the system is enhanced with anti-spoofing technology, which ensures the authenticity of detected faces and prevents image manipulation or falsification. The anti-spoofing algorithm analyzes the texture of the detected face to verify its genuineness [19]. This process includes extracting, analyzing, and verifying features, then determining authenticity by comparing patterns to the characteristics of faces in the dataset. For instance, when tested with a facial photo displayed on a mobile phone, the system will not validate it as authentic [20].

Testing & Evaluation

Upon completing system development, testing was carried out using a separate dataset that was not used during training. The evaluation focused on assessing the accuracy of facial recognition, the security level of anti-spoofing, and the overall system performance [21][22]. The results revealed instances where certain images were not recognized by the classifier model, leading to an "Unknown" status. This means the system was unable to identify or verify those images as either genuine or spoofed faces, indicating potential areas for improvement in both facial recognition and anti-spoofing functionality [23][9].

Implementation & Result Analysis

After testing, the system was implemented in the environment of STMIK IKMI Cirebon. The attendance data of educational staff was recorded and evaluated using the developed system as shown in Figure 5. The results were analyzed to assess the system's reliability in accurately and efficiently recording attendance within this institution [11][24].



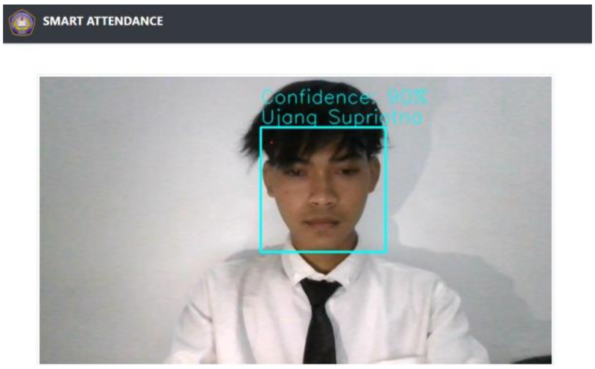
Source: (Research Results, 2024)

Figure 5. Implementation of Dataset Collection

RESULTS AND DISCUSSION

Face Detection Utilizing the Deep Learning Approach

Over the course of 10 experimental trials, the Deep Learning-based face detection method achieved an average accuracy of 90%. These results highlight the method's reliability in recognizing faces across various testing conditions and scenarios as shown in Figure 6.



Source: (Research Results, 2024)

Figure 6. The Face Detection Accuracy Test

Accredited Rank 2 (Sinta 2) based on the Decree of the Dirjen Penguatan RisBang Kemenristekdikti No.225/E/KPT/2022, December 07, 2022. Published by LPPM Universitas Nusa Mandiri

The system recognizes a face only when its confidence level is 80% or higher. If the confidence falls below this threshold, the face is labeled as "UNKNOWN." The identity verification process uses a classification model to detect faces in an image and assess the confidence of the predicted identities.

Table 1. The Accuracy O Face Recognition Detection

Detection	Accuracy (%)
Trial-1	88
Trial-2	89
Trial-3	89
Trial-4	90
Trial-5	89
Trial-6	91
Trial-7	90
Trial-8	91
Trial-9	91
Trial-10	92
Average	90

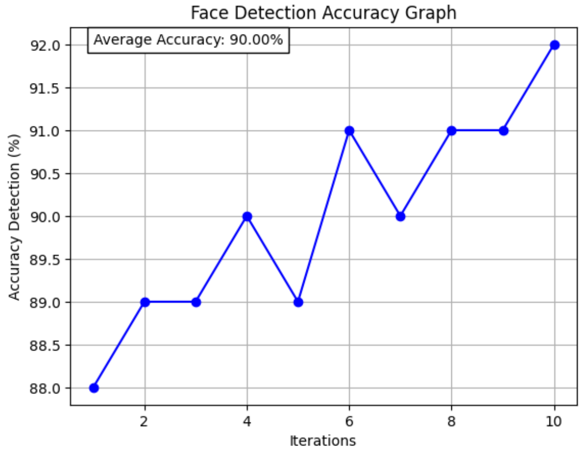
Source: (Research Results, 2024)

$$\bar{x} = \frac{x_1 + x_2 + \ldots + xn}{n}$$

$$\bar{x} = \frac{88 + 89 + 89 + 90 + 89 + 91 + 90 + 91 + 91 + 92}{10}$$

$$= 90$$

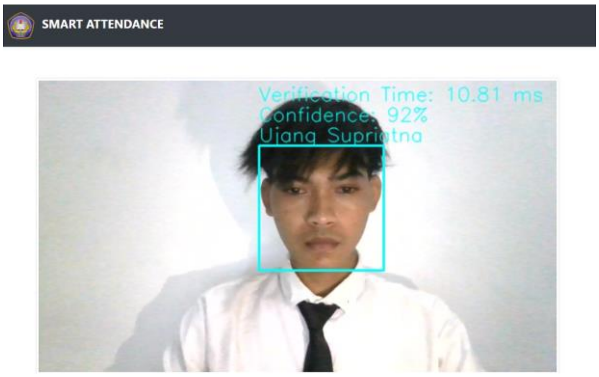
In the evaluation using the Deep Learning method, it was found that face detection is effective with an average accuracy of 90% as shown in Table 1. This indicates a strong capability in identifying individual faces within the test dataset. Accuracy is calculated as the percentage of correctly detected faces compared to the total number of faces in the dataset, showcasing the method's effectiveness in face recognition-based attendance systems as shown in Figure 7.



Source: (Research Results, 2024)
Figure 7. The Graph of Face Detection Accuracy

Identity Verification and Verification Time

At this stage, the system must confirm that the recognized face matches the correct identity. In this study, the identity verification accuracy reached about 90%, demonstrating the system's effectiveness in confirming identities. Additionally, the verification process is relatively quick, taking only around 7 to 11 milliseconds, with an average of 9.56 milliseconds per verification in Figure 8.



Verification Time: 10.81 ms
Confidence: 92%
Ujang Supriatna

Source: (Research Results, 2024)
Figure 8. Identity Verification and Detection Speed

The duration of identity verification using a classification method is measured by recording the time before and after face verification in Table 2. The total verification time is calculated in milliseconds. This data is then stored in a list for further analysis.

Table 2. Face Recognition Verification Time

Detection	Accuracy (%)	Time (ms)
Trial-1	88	10
Trial-2	89	8,50
Trial-3	89	8,70
Trial-4	90	8,90
Trial-5	89	8,60
Trial-6	91	10
Trial-7	90	10,50
Trial-8	91	10,60
Trial-9	91	10,80
Trial-10	92	11
Average	90	9,56

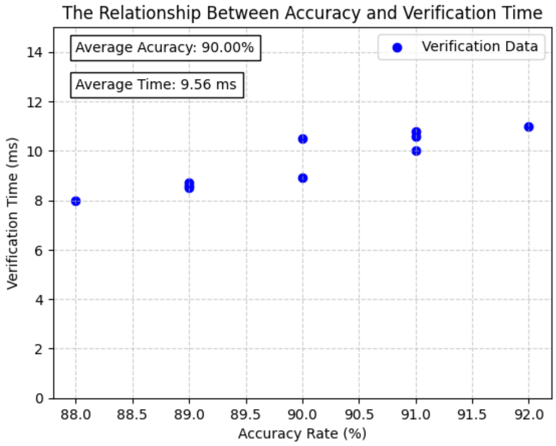
Source: (Research Results, 2024)

$$\bar{x} = \frac{x_1 + x_2 + \ldots + xn}{n}$$

$$\bar{x} = \frac{8 + 8{,}50 + 8{,}70 + 8{,}90 + 8{,}60 + 10 + 10{,}50 + 10{,}60 + 10{,}80 + 11}{10}$$

$$= 9{,}56$$

The reasonably high accuracy rate of approximately 90%, coupled with a relatively fast verification time of around 9.56 milliseconds per verification, constitutes a positive achievement in the context of developing a face recognition-based attendance system as shown in Figure 9.



Source: (Research Results, 2024)

Figure 9. The Graph of Relationship between Accuracy and Verification Time

Utilization of Deep Learning Method in Attendance Management System

The system's high accuracy and almost 0% False Positive Rate (FPR) and False Negative Rate (FNR) demonstrate its effectiveness in ensuring accurate attendance. It's important to note that the FPR and FNR can reach 0% when the system is exclusively used by individuals included in the training data as shown in Table 3.

Table 3. Evaluation of the Experiment Results

Detection	Accuracy (%)	Time (ms)	Identification Results	FPR	FNR
Trial-1	88	10	True	0	0
Trial-2	89	8,50	True	0	0
Trial-3	89	8,70	True	0	0
Trial-4	90	8,90	True	0	0
Trial-5	89	8,60	True	0	0
Trial-6	91	10	True	0	0
Trial-7	90	10,50	True	0	0
Trial-8	91	10,60	True	0	0
Trial-9	91	10,80	True	0	0
Trial-10	92	11	True	0	0
Average	90	9,56	100	0	0

Source: (Research Results, 2024)

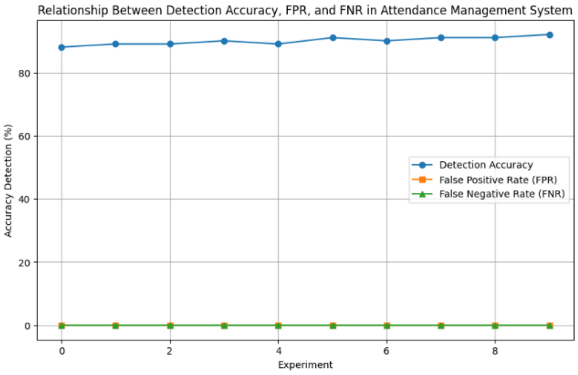
$$FPR = \frac{False\ Positives}{False\ Positives + True\ Negatives}$$

$$FPR = \frac{0}{0+10} = 0$$

$$FNR = \frac{False\ Negatives}{False\ Negatives + True\ Fositives}$$

$$FPR = \frac{0}{0+10} = 0$$

Based on the evaluation results, the use of the Deep Learning Method in attendance management has yielded highly positive outcomes. This system achieves a detection accuracy of around 90% with rapid detection times as shown in Figure 10. The near 0% false positive (FPR) and false negative (FNR) rates indicate the system's high accuracy in avoiding false positive and false negative identification errors.



Source: (Research Results, 2024)

Figure 10. Graph of Accuracy, FPR, and FNR Evaluation

Contribution to Attendance Management in the Educational Setting

Implementing a confidence level above 80% has been a pivotal strategy to enhance attendance accuracy. With this confidence level, the system has achieved an outstandingly high accuracy rate of 98.90% as shown in Table 4. This outcome indicates an exceptionally precise attendance recording based on facial identification. Furthermore, the low error rate of approximately 1.10% demonstrates the system's reliability in identifying individual attendance.

Table 4. The Results of The Smart Attendance Verification.

Detection	Accuracy (%)
Trial-1	93
Trial-2	96
Trial-3	100
Trial-4	100
Trial-5	100
Trial-6	100
Trial-7	100
Trial-8	100
Trial-9	100
Trial-10	100
Average	98,90

Source: (Research Results, 2024)

$$\boldsymbol{x}^{-} = \frac{x_1 + x_2 + \ldots + xn}{n}$$

$$\bar{x} = \frac{93 + 96 + 100 + 100 + 100 + 100 + 100 + 100 + 100 + 100}{10}$$

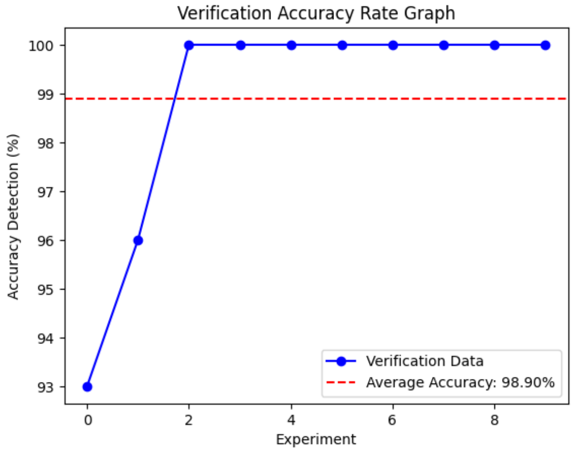
$$= 98,90$$

Table 5. The Accuracy Rate of Face Recognition Attendance Technology

Attendance Accuracy	Rate Recording Error Rate
98,90%	1.10%

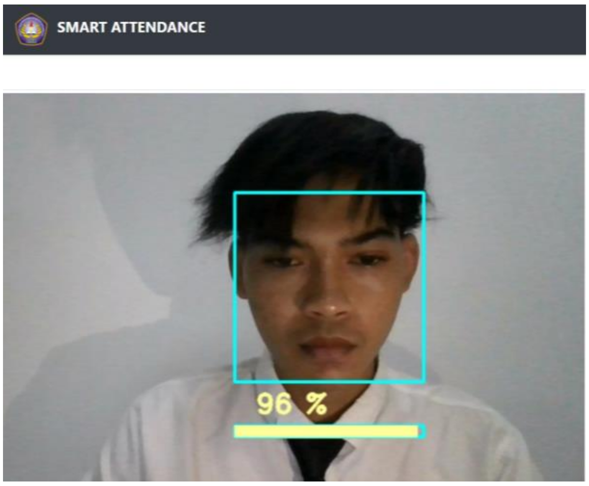
Source: (Research Results, 2024)

Facial recognition technology, with an accuracy rate of 98.90% as shown in Figure 11, guarantees reliable and precise attendance tracking. A confidence level above 80% reflects a thorough facial identification process that successfully addresses various challenges, ensuring the integrity of the attendance data.

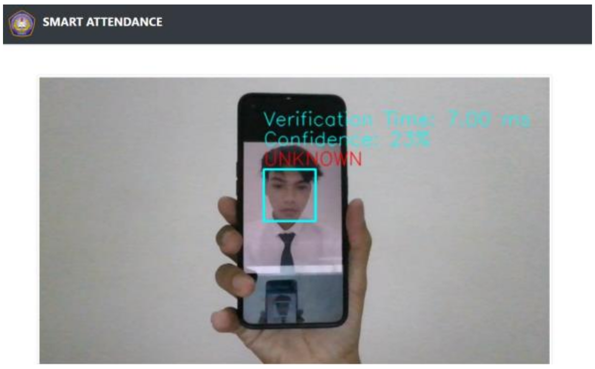


Source: (Research Results, 2024)
Figure 11. Accuracy Rate of Face Recognition-Based Attendance System

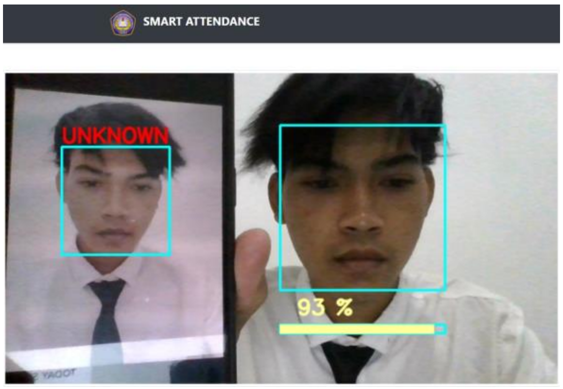
The facial recognition system, enhanced with anti-spoofing technology, can differentiate between real faces and non-authentic images. When a genuine face is recognized, the system logs the user's presence. However, if the system detects an image from devices such as smartphones, it will label the user as "unknown as shown in Figure 12, Figure 13, and Figure 14.



Source: (Research Results, 2024)
Figure 12. Face Recognition Using Original Images



Source: (Research Results, 2024)
Figure 13. Face Recognition Using Photos on a Mobile Phone

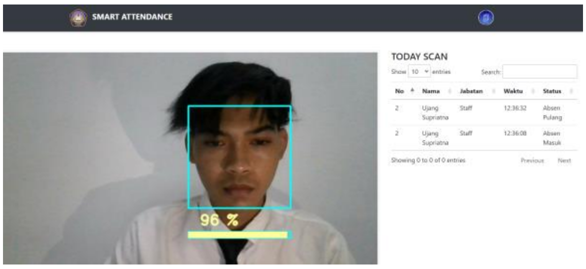


Source: (Research Results, 2024)
Figure 14. Facial Recognition in Multiple-Image Scenarios

Upon successful recognition, the attendance information is recorded in the database as attendance data. This stored information can be accessed later, showing detailed records, including the identity of the educational staff and the time of

Accredited Rank 2 (Sinta 2) based on the Decree of the Dirjen Penguatan RisBang Kemenristekdikti No.225/E/KPT/2022, December 07, 2022. Published by LPPM Universitas Nusa Mandiri

attendance as shown in Figure 15, Figure 16, and Figure 17 .



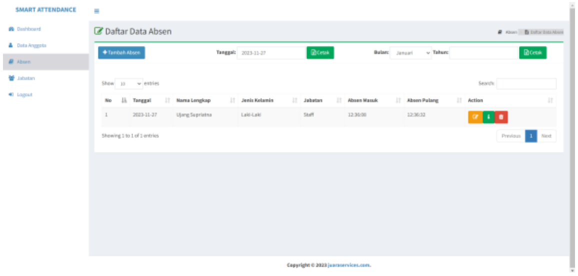
TODAY SCAN

Show 10 entries Search:

No	Nama	Jabatan	Waktu	Status
2	Ujang Supriatna	Staff	12:36:32	Absen Pulang
2	Ujang Supriatna	Staff	12:36:08	Absen Masuk

Showing 0 to 0 of 0 entries Previous Next

Source: (Research Results, 2024)
Figure 15. Smart Daily Attendance Recording



Daftar Data Absen

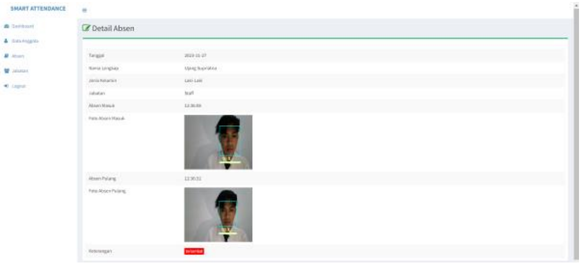
Tanggal: 2023-11-27 Bulan: Januari Tahun:

Show 10 entries Search:

No	Tanggal	Nama Lengkap	Jenis Kelamin	Jabatan	Absen Masuk	Absen Pulang	Action
1	2023-11-27	Ujang Supriatna	Laki-Laki	Staff	12:36:08	12:36:32	

Showing 1 to 1 of 1 entries

Source: (Research Results, 2024)
Figure 16. List of Educational Staff Attendance Data



Detail Absen

Tanggal	2023-11-27
Nama Lengkap	Ujang Supriatna
Jenis Kelamin	Laki-Laki
Jabatan	Staff
Absen Masuk	12:36:08
Foto Absen Masuk	
Absen Pulang	12:36:32
Foto Absen Pulang	
Keterangan	[illegible]

Source: (Research Results, 2024)
Figure 17. Details of Educational Staff Attendance Based on ID

CONCLUSION

Conventional attendance systems often face challenges related to accuracy and data security, especially with risks of data manipulation and identity spoofing. Manual attendance systems become less reliable, particularly in educational environments that require transparent and efficient attendance management. To address these limitations, this study developed a smart attendance system based on facial recognition using Deep Learning, equipped with anti-spoofing technology to prevent forgery. The research methodology included data collection in the form of facial images from educational staff at STMIK IKMI Cirebon, which were then processed through several stages, including normalization and face detection. The facial recognition model was built using a deep neural network architecture consisting of convolutional layers, pooling, and an inception module to extract features. Anti-spoofing technology was applied using the Local Binary Patterns (LBP) method, which effectively detects genuine facial textures, while the Adaboost technique was used to enhance detection accuracy.

The research results showed that this system achieved a high accuracy rate of 98.90% with an 80% confidence threshold in detecting genuine attendance, as well as an average verification time of 9.56 milliseconds per verification, reflecting the system's efficiency. The near-zero False Positive Rate (FPR) and False Negative Rate (FNR) indicate that the system is highly reliable in avoiding identification errors. With high accuracy and security levels, this system significantly contributes to advancing facial recognition technology for attendance management in educational settings. This study also opens opportunities for further application in various educational institutions through integration with IoT technology and the use of CCTV cameras, expanding the system's scope and reliability in attendance monitoring. In conclusion, the facial recognition-based attendance system with Deep Learning-based anti-spoofing technology has proven effective in enhancing attendance recording accuracy and security, supporting stronger administrative practices in the educational sector.

Future recommendations for system improvement include integrating IoT technology for broader usage and utilizing CCTV cameras for face detection, enabling seamless implementation across multiple rooms, particularly for tracking attendance during exit checks.

ACKNOWLEDGMENT

This research was made possible through the funding support from the Regular Beginner Lecturer Research Program (PDP) provided by the Ministry of Education, Culture, Research, and Technology through the Directorate of Research, Technology, and Community Service. We express our deep gratitude to STMIK IKMI Cirebon for their support in providing facilities and an inspiring academic environment, as well as to the administrative staff and faculty members for offering the opportunity and location for the implementation of this research. The results of this research are expected to improve the efficiency of the attendance system and contribute to the development of quality human resources.

REFERENCES

[1] Z. Zulkifli and A. I. Pawelloi, “Implementasi Opencv Face Recognition Pada Sistem Presensi Karyawan Koperasi Simpan Pinjam,” *J. Sintaks Log.*, vol. 3, no. 1, pp. 58–61, 2023, doi: 10.31850/jsilog.v3i1.2095.

[2] T. V. Dang, “Smart Attendance System based on Improved Facial Recognition,” *J. Robot. Control*, vol. 4, no. 1, 2023, doi: 10.18196/jrc.v4i1.16808.

[3] M. W. Septyanto, H. Sofyan, H. Jayadianti, O. S. Simanjuntak, and D. B. Prasetyo, “Aplikasi Presensi Pengenalan Wajah Dengan Menggunakan Algoritma Haar Cascade Classifier,” *Telematika*, vol. 16, no. 2, p. 87, 2020, doi: 10.31315/telematika.v16i2.3182.

[4] Z. Wang, “Higher Education Management and Student Achievement Assessment Method Based on Clustering Algorithm,” *Comput. Intell. Neurosci.*, vol. 2022, 2022, doi: 10.1155/2022/4703975.

[5] R. Bairagi, R. Ahmed, S. A. Tisha, M. S. Sarder, M. S. Islam, and M. A. Islam, “A Real-time Face Recognition Smart Attendance System with Haar Cascade Classifiers,” *Proc. 3rd Int. Conf. Inven. Res. Comput. Appl. ICIRCA 2021*, no. October, pp. 1417–1425, 2021, doi: 10.1109/ICIRCA51532.2021.9544872.

[6] C. Fadli and D. Desmulyati, “Implementasi Perhitungan Face Detection Dengan Metode Haar Cascade Classifier,” *J. Nas. Komputasi dan Teknol. Inf.*, vol. 4, no. 6, pp. 535–542, 2021, doi: 10.32672/jnkti.v4i6.3721.

[7] K. Marzuki, N. Hanif, and I. P. Hariyadi, “Application of Domain Keys Identified Mail, Sender Policy Framework, Anti-Spam, and Anti-Virus: The Analysis on Mail Servers,” *International* …. download.garuda.kemdikbud.go.id, 2022.

[8] A. P. Nanda, D. E. H. Pramono, and S. Hartati, “Menentukan Tingkat Kepuasan Mahasiswa Terhadap Pelayanan Akademik Menggunakan Metode Algoritma K-Means,” *J. Sist. Inf. dan Telemat.*, vol. 11, no. 1, pp. 23–28, 2020.

[9] Y. Hartiwi, E. Rasywir, Y. Pratama, and P. A. Jusia, “Eksperimen Pengenalan Wajah dengan fitur Indoor Positioning System menggunakan Algoritma CNN,” *Paradig. - J. Komput. dan Inform.*, vol. 22, no. 2, pp. 109–116, 2020, doi: 10.31294/p.v22i2.8906.

[10] I. K. S. Buana, “Penerapan Pengenalan Wajah Untuk Aplikasi Absensi dengan Metode Viola Jones dan Algoritam LBPH,” *J. MEDIA Inform. BUDIDARMA*, vol. 5, no. 3, 2021, doi: 10.30865/mib.v5i3.3008.

[11] M.A Thalor and Omkar S. Gaikwad, “Facial Recognition Attendance Monitoring System using Deep Learning Techniques,” *Int. J. Integr. Sci. Technol.*, vol. 2, no. 1, 2024, doi: 10.59890/ijist.v2i1.1290.

[12] J. Ilmiah and R. Darmawan, “Perancangan Sistem Absensi menggunakan Face Recognition dengan Haar Cascade Classifier,” vol. 5, no. 2, pp. 1–8, 2023.

[13] T. Susim and C. Darujati, “Pengolahan Citra untuk Pengenalan Wajah (Face Recognition) Menggunakan OpenCV,” *J. Syntax Admiration*, vol. 2, no. 3, pp. 534–545, 2021, doi: 10.46799/jsa.v2i3.202.

[14] F. Fahraini and R. Syarif, “Pengaruh Kompensasi, Disiplin Kerja dan Komunikasi Terhadap Kinerja Karyawan PT. Nikos Distribution Indonesia,” *Ikraith-Ekonomika*, vol. 5, no. 1, pp. 20–30, 2022.

[15] D. N. P. Sari, *ANALISIS CLUSTER DENGAN METODE K-MEANS PADA PERSEBARAN KASUS COVID-19 BERDASARKAN PROVINSI DI INDONESIA*. 2020.

[16] D. A. Kurnia, A. Setiawan, D. R. Amalia, R. W. Arifin, and D. Setiyadi, “Image Processing Identifacation for Indonesian Cake Cuisine using CNN Classification Technique,” *J. Phys. Conf. Ser.*, vol. 1783, no. 1, 2021, doi: 10.1088/1742-6596/1783/1/012047.

[17] A. Info and D. I. Signature, “Application of 2DPCA and SOM Algorithms to Identification of Digital Signature Ownership,” vol. 16, no. 3, pp. 208–218, 2023, doi: 10.30998/faktorexacta.v16i3.17504.

[18] E. Muningsih, I. Maryani, and V. R. Handayani, “Penerapan Metode K-Means dan Optimasi Jumlah Cluster dengan Index Davies Bouldin untuk Clustering Propinsi Berdasarkan Potensi Desa,” *J. Sains dan Manaj.*, vol. 9, no. 1, p. 96, 2021, [Online]. Available: www.bps.go.id

[19] Q. Aini, W. Febriani, C. Lukita, S. Kosasi, and ..., “New normal regulation with face recognition technology using attendx for student attendance algorithm,” *… Sci. …*, 2022.

[20] R. Liu, “Data Analysis of Educational Evaluation Using K-Means Clustering Method,” *Comput. Intell. Neurosci.*, vol. 2022, 2022, doi: 10.1155/2022/3762431.

[21] Z. Trabelsi, F. Alnajjar, M. M. A. Parambil, M. Gochoo, and L. Ali, “Real-Time Attention Monitoring System for Classroom: A Deep Learning Approach for Student’s Behavior Recognition,” *Big Data Cogn. Comput.*, vol. 7,

no. 1, pp. 1–17, 2023, doi: 10.3390/bdcc7010048.

[22] U. Muhammad, M. Z. Hoque, M. Oussalah, and J. Laaksonen, “Deep Ensemble Learning with Frame Skipping for Face Anti-Spoofing,” 2023. doi: 10.1109/IPTA59101.2023.10320013.

[23] Q. Aini, W. Febriani, C. Lukita, S. Kosasi, and U. Rahardja, “New Normal Regulation with Face Recognition Technology Using AttendX for Student Attendance Algorithm,” 2022. doi: 10.1109/ICOSTECH54296.2022.9829079.

[24] R. P. K. Banu Santoso, “IMPLEMENTASI PENGGUNAAN OPENCV PADA FACE RECOGNITION UNTUK SISTEM PRESENSI PERKULIAHAN MAHASISWA,” *Andrew’s Dis. Ski. Clin. Dermatology.*, vol. 9, pp. 352–361, 20AD.