Faktor Exacta
Vol. 17, No. 3, Sept 2024, pp. 262~274
eISSN: 2502-339X, pISSN: 1979-276X, DOI: 10.30998/faktorexacta.v17i3.21166

Brilliant Attendance With Face Anti-Spoofing Technology Using Haar Cascade Classifier

Ujang Supriatna[1], Dian Ade Kurnia[2], Tati Suprapti[3]
[123]Department of Informatic, STMIK IKMI Cirebon, Indonesia

Article Info

Article history:

Received 27 Nov 2023
Revised 23 Sept 2024
Accepted 2 Oct 2024

Keywords:

Smart Attendance
Haar Cascade Classifier
Anti-Spoofing
OpenCV
System Performance

ABSTRACT

Traditional attendance systems often encounter challenges related to efficiency and accuracy. This research proposes an innovative solution by developing an intelligent attendance system incorporating facial recognition technology with anti-spoofing features, using the Haar Cascade Classifier as the core detection algorithm. The system addresses the inefficiencies of conventional attendance methods by ensuring accurate tracking and preventing fraud through reliable facial identification. The system utilizes image processing techniques to detect vital facial features, leveraging the Haar Cascade Classifier for robust and efficient facial recognition. The proposed method achieves an impressive average accuracy of 98.90% in attendance tracking, with confidence levels consistently exceeding 80%, ensuring precise identification and mitigating common errors. In addition to high accuracy, the system efficiently logs and verifies attendance, providing rapid results. Beyond its technical advantages, this research significantly contributes to developing more innovative attendance systems by enhancing accountability and promoting discipline among educational staff. Moreover, implementing this system at STMIK IKMI Cirebon showcases its potential to improve attendance management and evaluation across academic institutions. The study highlights the benefits of incorporating face anti-spoofing technology into attendance systems. It paves the way for broader applications in automating administrative tasks and ensuring data integrity in educational settings.

Corresponding Author:

Ujang Supriatna,
Department of Informatic,
STMIK IKMI Cirebon,
Jl. Perjuangan No.10B, Karyamulya, Kec. Kesambi, Kota Cirebon, Jawa Barat.
Email: ujangsupriatna125@gmail.com

1. INTRODUCTION

The management of educational staff attendance within the university environment is a crucial aspect that demands particular attention to efficiency, accuracy, and transparency [1],[2]. While traditional attendance systems have been commonly utilized, the complexity of modern higher education necessitates a more sophisticated and responsive approach. The use of information technology (IT), particularly in the context of facial recognition and anti-spoofing technology, presents an innovative solution to address these challenges [3]. Previous research, such as the work by Septyanto et al. (2020), implemented facial recognition attendance systems using the Haar Cascade Classifier to improve upon fingerprint-based attendance systems. Their study highlighted the limitations of fingerprint systems and achieved a recognition success rate of 87%, although the system struggled under certain lighting conditions and with facial accessories [4]. Similarly, Susim and Darujati (2021) applied image processing with Eigenface and OpenCV to achieve a recognition rate of 85%, but their method was constrained to identifying faces within a predefined database [5]. Another study by Fadli and Desmulyati (2021) explored the use of Haar Cascade Classifier for face detection in an educational environment, achieving an accuracy rate above 50% [6]. In contrast, this research introduces several advancements to existing methods. The implementation of anti-spoofing technology adds an additional layer of security that previous studies did not incorporate. Additionally, by integrating the Haar Cascade Classifier with the Adaboost algorithm, this study enhances detection accuracy, achieving a significantly higher average accuracy rate of 98.90%. This marks a substantial improvement over the baseline studies mentioned, particularly in addressing issues related to lighting and facial accessories. The combination of facial recognition and anti-spoofing further ensures the reliability and integrity of attendance data, offering a robust solution for educational institutions.

Fundamental issues in attendance management encompass low efficiency and vulnerability in manual recording systems, which tend to be error-prone and less responsive to the dynamics of modern educational institutions [6]. These traditional systems no longer suffice in meeting the needs for accurate, efficient, and responsive attendance recording amidst the changing scale of higher education institutions [3],[7]. The objective of this research is to develop and implement an intelligent attendance system based on facial recognition technology with anti-spoofing using the Haar Cascade Classifier method [8],[6]. This study focuses on recording the attendance of educational staff within higher education institutions, aiming to enhance efficiency, accuracy, and responsiveness to the dynamics of modern academia [6].

This research approach applies the Haar Cascade Classifier method for facial recognition in a facial-based attendance system, complemented by anti-spoofing techniques. This approach breaks down the facial detection process into a series of complex stages to improve efficiency and speed. By training the classifier using positive and negative facial images alongside the Adaboost technique, detection accuracy is heightened [9]. The integration of anti-spoofing validates facial authenticity, adding a layer of security to the recognition process. The result is swift, efficient, and secure facial recognition, supporting the practical management of educational staff attendance [3]. The research findings indicate that the implementation of a facial recognition-based attendance system with anti-spoofing using the Haar Cascade Classifier method achieved an average accuracy rate of 98.90%. The implemented facial recognition technology ensures reliability and accuracy in attendance recording. Confidence levels above 80% indicate a meticulous facial identification process, successfully overcoming various challenges and instilling confidence in attendance data integrity. Furthermore, this research stimulates further debate and collaboration in the field of facial recognition technology at STMIK IKMI Cirebon, with the potential to generate better and more reliable innovations in attendance management within this institution. Overall, this study holds significant importance in developing the understanding and application of facial recognition technology in attendance management at STMIK IKMI Cirebon.

2. THEORETICAL BASIS

2.1 Haar Cascade Classifier

The Haar Cascade Classifier is a pivotal tool in computer vision, employing a machine learning-based approach for image object detection. Operating on a principle of analyzing distinct features organized as rectangular regions at varied scales within an image, its efficiency stems from an algorithm designed for swift processing [10],[11],[12]. This technique's success lies in its ability to efficiently recognize patterns, making it ideal for identifying facial features within images.

2.2 Anti-Spoofing

In the realm of facial recognition, anti-spoofing safeguards systems against deceptive attempts using counterfeit images or videos. It encompasses multifaceted techniques such as liveness detection, texture analysis, and motion detection to discern and thwart such fraudulent endeavors [13], [14]. The aim is to ensure the system's robustness against falsification, maintaining its integrity and reliability in authenticating individuals.

2.3 Python

Python stands as a versatile programming language, widely adopted in diverse domains, notably in machine learning and computer vision. Its comprehensive libraries and frameworks, notably OpenCV, empower the development of intricate face recognition systems, leveraging its simplicity and efficacy [15], [16],[5], [1]. Python's readability and extensibility make it an optimal choice for implementing complex algorithms required for facial recognition tasks.

2.4 OpenCV

OpenCV an acronym for Open Source Computer Vision Library, serves as a robust open-source software library for computer vision and machine learning applications. Equipped with an array of tools and algorithms, it facilitates image processing, including vital functions like face detection and recognition. This capability is pivotal in constructing intelligent attendance systems that rely on facial recognition for identification and authentication purposes [15], [1], [8].

2.5 Flask

Flask a Python-based web framework, offers a platform for creating web applications. Within the context of a smart attendance system, Flask's utility emerges in crafting user-friendly web interfaces for managing attendance data and facilitating seamless interactions with the system. Its simplicity and scalability enable the creation of intuitive interfaces for efficient attendance management [3].

3. METHOD

The research stages used in developing an attendance system using facial recognition technology and anti-spoofing are:

3.1 Data Collection

The data for the attendance system development was collected by sampling facial images of educational staff at STMIK IKMI Cirebon, who were the subjects of the study. Image capture was performed using a camera integrated with facial recognition software. The data collection process involved automatic imaging of 100 pictures for each user. This method serves as the primary foundation in building and testing the reliability of the ongoing development of the attendance system.

Figure 1. Example of image acquisition results

3.2 Pre-processing of Data

The image processing within the system involves a series of steps, including image normalization, facial detection, and elimination of images that do not meet the criteria. Typically, RGB format images have a bit depth of 24, with each color channel (red, green, blue) utilizing 8 bits. Conversely, grayscale images often have a single-bit depth, commonly 8 bits [17], [18],[19]. This distinction is crucial as it signifies the complexity of color information processed within the system. Each image measures 300x300 pixels, stored with the name 'image_id' and ordered according to their sequence, such as image 1.1.

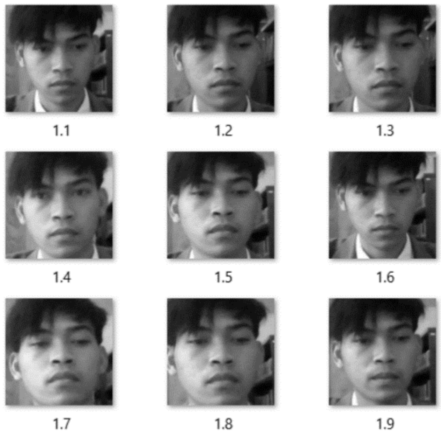

Figure 2. Example of image processing of data

3.3 Development of Facial Recognition Model

The research methodology for face recognition using the Haar Cascade Classifier follows a structured process, which begins with dataset collection and proceeds through various stages to achieve optimal facial detection and recognition [4],[3], [20]. The process involves the following key steps :

1. Dataset Collection: The first step involves gathering a dataset that includes both positive images (faces) and negative images (non-faces). This data forms the foundation for the training of the face recognition model.
2. Haar-like Feature Extraction: After collecting the dataset, the Haar-like features of the images are extracted. These features are crucial for identifying the distinctive patterns in the facial images that the model will use for detection.
3. Training with Adaboost: The extracted features are then used to train a classifier using the Adaboost algorithm. Adaboost enhances detection accuracy by combining weak classifiers (decision stumps) into a strong classifier. At each iteration, Adaboost adjusts the weights of misclassified samples, refining the model to reduce errors.
4. Cascade Classifier Construction: Once the classifiers are trained, they are assembled into a cascade classifier. This structure allows for faster processing by sequentially applying classifiers at different stages, filtering out non-face regions early in the detection process.
5. Stage-Wise Classifier Training: The classifiers are trained in stages, where each stage refines the previous one to improve detection accuracy and speed. This process ensures that the model can efficiently and accurately detect faces in the images.
6. Testing and Evaluation: After the classifier is fully trained, it is tested and evaluated for accuracy. The system's performance is measured in terms of its ability to correctly identify faces while avoiding false positives [9].

The following figure illustrates the overall process flow for developing the face recognition model using the Haar Cascade Classifier method. Each stage is crucial for building an accurate and efficient face detection system, from data collection to evaluation. The figure summarizes the steps involved in the model's development, providing a visual representation of the process explained above.

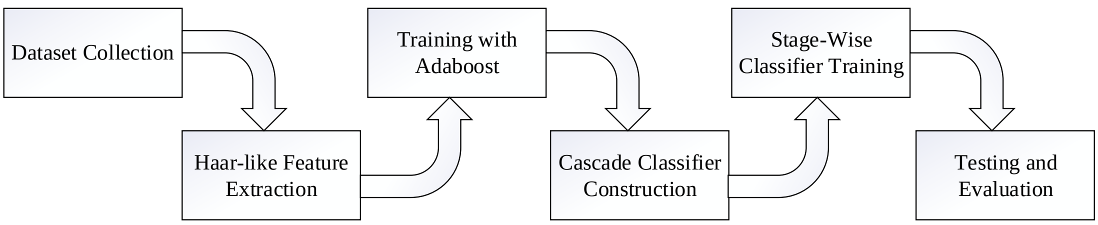

Figure 3. The stages of Face Recognition Model Development

3.4 Integration of Anti-Spoofing Technology

In addition to facial recognition, this system is fortified with anti-spoofing technology. This technology verifies the authenticity of the detected face to prevent manipulation or falsification of images within the system. The anti-spoofing algorithm checks the detected face's texture for authenticity[14]. The process involves extraction, analysis, verification, and determination of authenticity based on patterns matching the characteristic features of faces in the dataset. When tested using a facial photo from a mobile phone, the system won't recognize its authenticity.

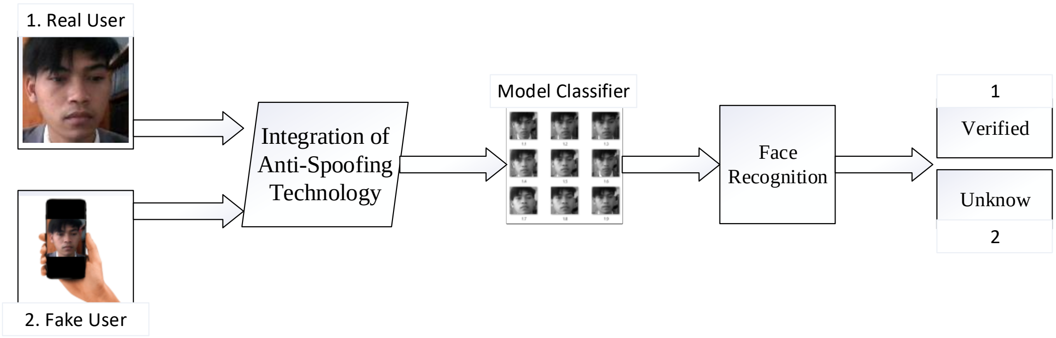

Figure 4. The stages of integration of Anti-Spoofing

3.5 Testing and Evaluation

After the system development, testing was conducted using a separate dataset not utilized during the training process. Evaluation aimed to measure facial recognition accuracy, anti-spoofing security level, and overall system effectiveness. The test results indicated instances where the images tested were unrecognized by the classifier model, resulting in an "Unknown" status. This indicates that the system couldn't identify or verify those images as known or spoofed faces, suggesting a need for improvement in facial recognition or anti-spoofing within the system.

3.6 Implementation and Results 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. The results were analyzed to assess the system's reliability in accurately and efficiently recording attendance within this institution.

Fase 1:

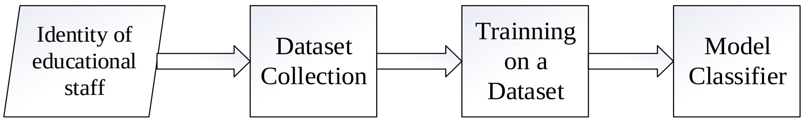

Figure 5. Implementation of dataset collection

Fase 2 :

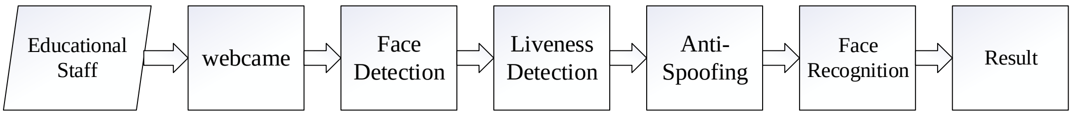

Figure 6. Implementation of attendance in the system

4. RESULT AND DISCUSSION

4.1 Face Detection using the Haar Cascade Classifier Method

Across 10 experimental trials, the face detection using the Haar Cascade Classifier method achieved an average accuracy of 90%. These outcomes demonstrate the reliability of this approach in identifying faces across diverse testing conditions and contexts.

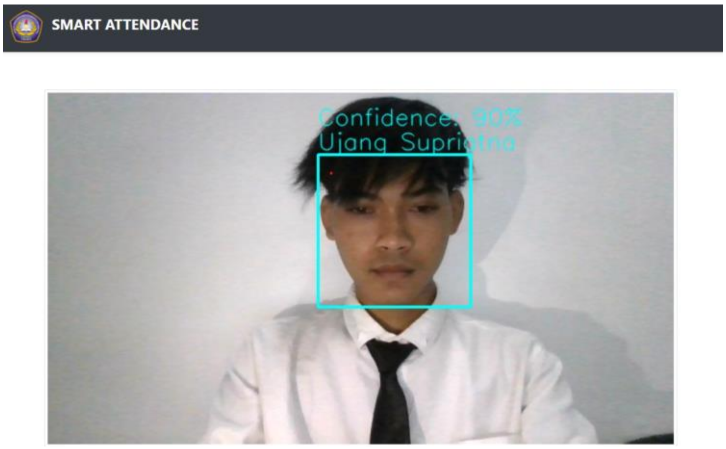

Figure 7. The face detection accuracy test

The system only recognizes a face if its confidence reaches 80% or higher. Anything less than that, the face will be labeled as "UNKNOWN". The identity verification process employs a classification model to identify faces in an image and evaluate the confidence level of predictions regarding the classified identities.

Table 1. The accuracy of 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

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

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

The evaluation using the Haar Cascade Classifier method found that face detection is effective, with an average accuracy of 90%. This indicates a strong capability to identify 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.

 DOI: 10.30998/faktorexacta.v17i3.21166

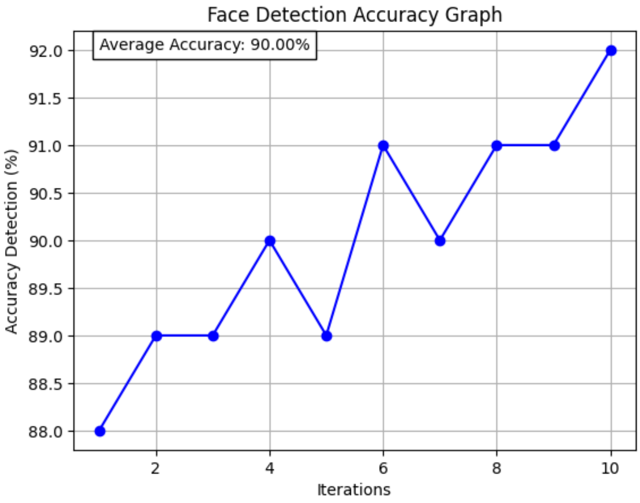

Figure 8. The graph of face detection accuracy

4.2 Identity Verification and Verification Time

During this stage, the system must ensure that the recognized face corresponds to the correct identity. In this research, the accuracy rate of identity verification reached approximately 90%, indicating the system's proficiency in verifying identities. Furthermore, the verification time required is relatively fast, only around 7 to 11 milliseconds or averaging at 9.56 per verification.

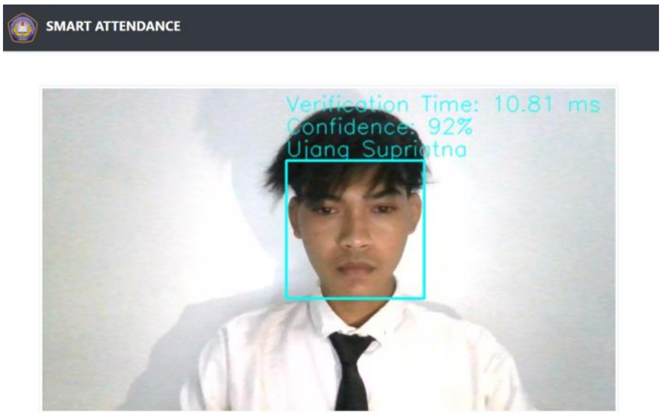

Figure 9. Identity verification and detection speed

There is a process for measuring the duration of identity verification using a classification method. By recording time before and after face verification, the overall duration of verification is calculated in milliseconds. Verification time data is 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

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

$$\bar{x} = \frac{8 + 8{,}50 + 8{,}70 + 8{,}90 + 8{,}60 + 10 + 10{,}50 + 10{,}60 + 10{,}80 + 11}{10} = 9{,}56$$

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 developing a face recognition-based attendance system.

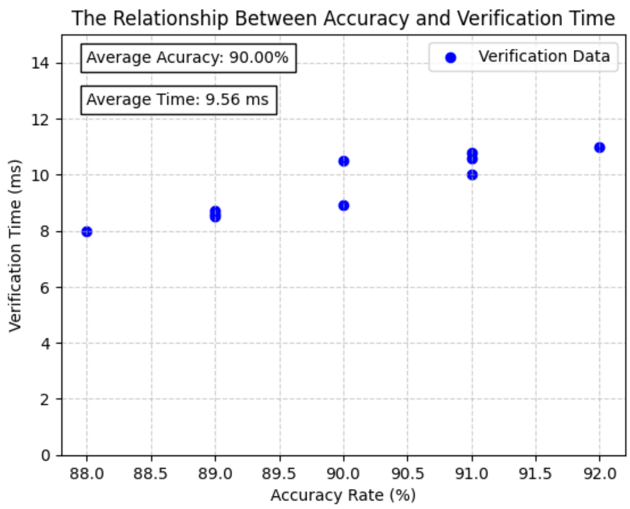

Figure 10. The graph of the relationship between accuracy and verification time

4.3 Utilization of Haar Cascade Classifier Method in Attendance Management System

The high accuracy rate and near 0% False Positive Rate (FPR) and False Negative Rate (FNR) indicate the system's success in ensuring accurate attendance. It should be noted that the FPR and FNR rates can reach 0% if the system is only used by individuals already in the training data.

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

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

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

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

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

Based on the evaluation results, using the Haar Cascade Classifier Method in attendance management has yielded highly positive outcomes. This system achieves a detection accuracy of around 90% with rapid detection times. The near 0% false positive (FPR) and false negative (FNR) rates indicate the system's high accuracy in avoiding false positive and false harmful identification errors.

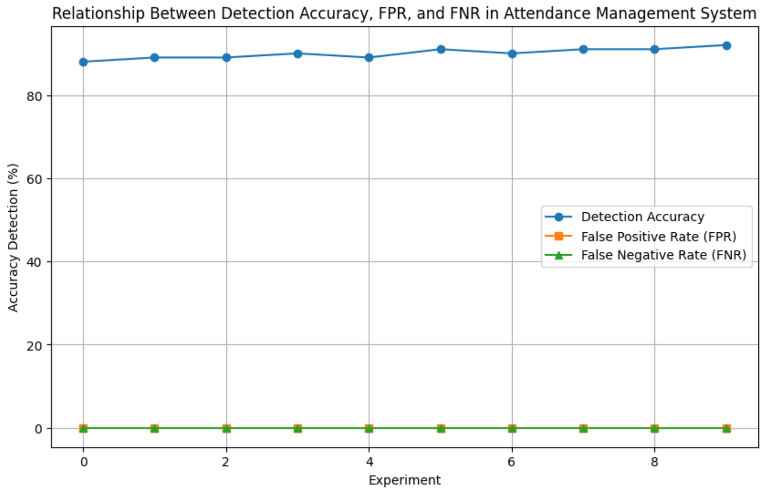

Figure 11. Graph of Accuracy, FPR, and FNR Evaluation

4.4 Contribution to Attendance Management in an Educational Context

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%. This outcome indicates an exact 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

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

$$\bar{x} = \frac{93 + 96 + 100 + 100 + 100 + 100 + 100 + 100 + 100 + 100}{10} = 98{,}90$$

Table 5. The Accuracy Rate of Face Recognition Attendance Technology

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

With an accuracy rate of 98.90%, facial recognition technology ensures the reliability and precision of attendance recording. A confidence level above 80% indicates a meticulous facial identification process that effectively overcomes various challenges, instilling confidence in the integrity of attendance data.

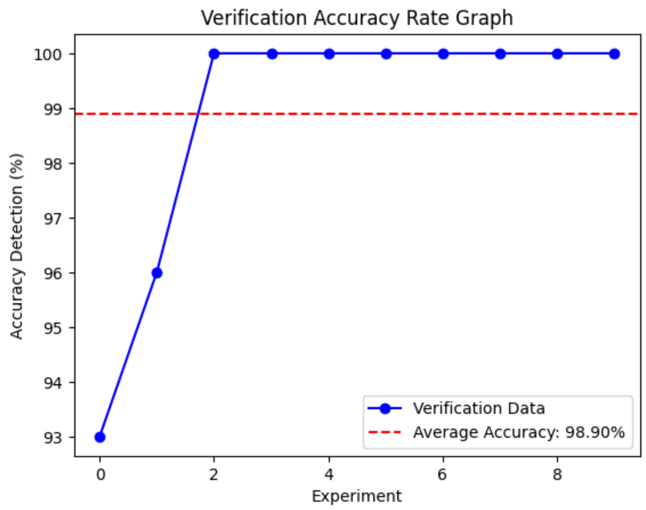

Figure 12. The Accuracy Rate of Face Recognition-Based Attendance Technology

Equipped with anti-spoofing technology, the facial recognition system can distinguish genuine faces from images that are not direct captures. The system registers the user's presence when an actual face is detected. However, the system identifies the user as "unknown" if facial recognition utilizes images from devices like smartphones.

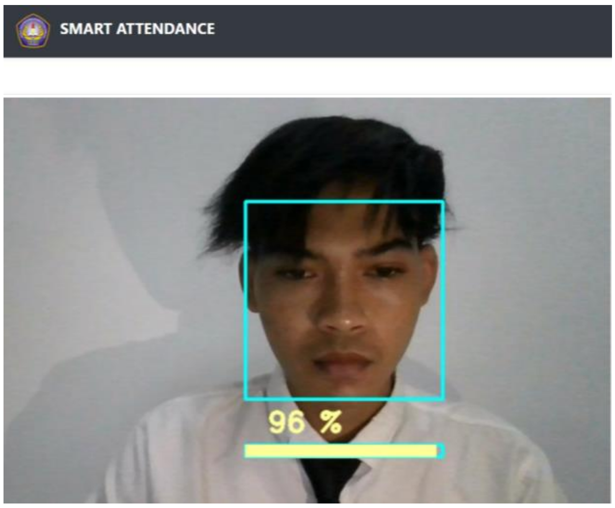

Figure 13. Face recognition using original images

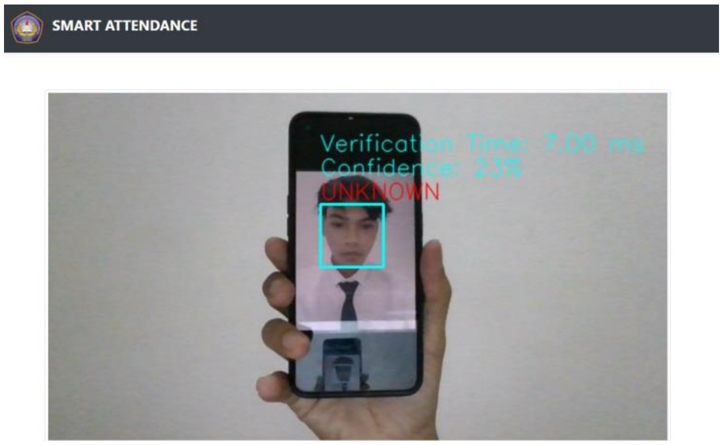

Figure 14. Face recognition using photos on a mobile phone

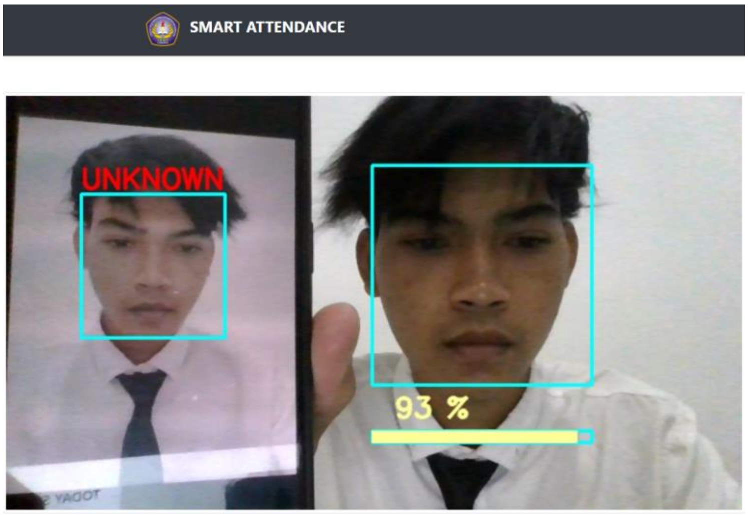

Figure 15. Facial recognition in multiple-image scenarios

When recognition is successful, attendance information will be stored in the database as attendance data. The stored data can be retrieved, displaying comprehensive details such as the identity of educational staff and the time of attendance.

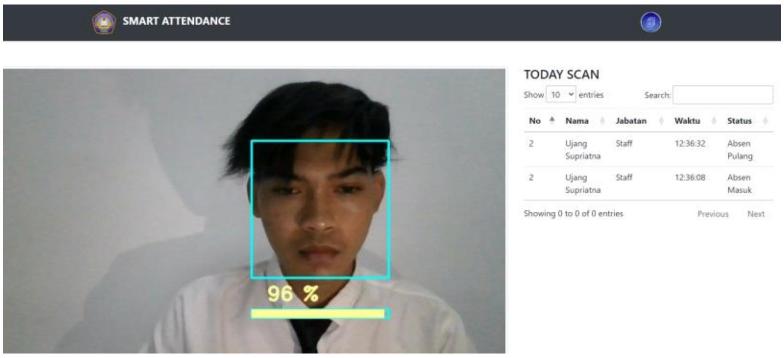

Figure 16. Smart daily attendance recording

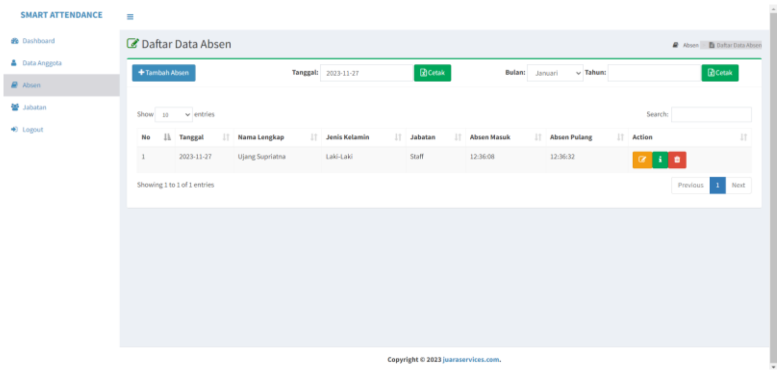

Figure 17. List of educational staff attendance data

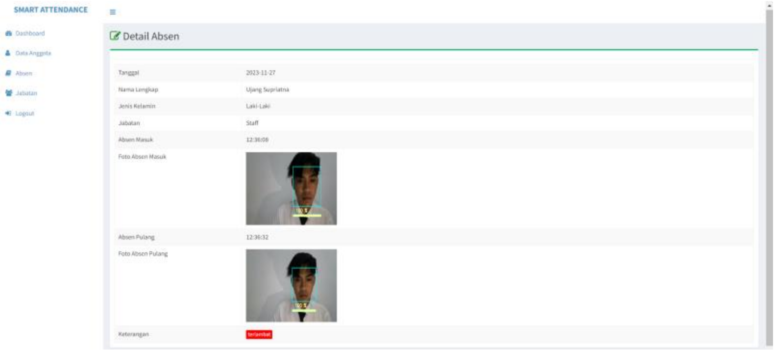

Figure 18. Details of educational staff attendance based on ID

5. DISCUSSION

The innovative attendance system developed in this research incorporates several key innovations that distinguish it from previous studies. By integrating anti-spoofing technology with the Haar Cascade Classifier, this system addresses a critical challenge in face recognition—preventing fraudulent attempts using static images or videos. This feature enhances the system's security and reliability, especially in environments where attendance data is sensitive, such as educational institutions.

Moreover, combining the Haar Cascade Classifier with the Adaboost algorithm resulted in an average accuracy rate of 98.90%, with a confidence threshold of 80%. This significantly improved over previous methods that struggled with lighting conditions and facial accessories. This research demonstrates that the system is robust across varying environments, making it suitable for real-world applications in educational staff attendance management, a niche not commonly addressed by previous studies that primarily focused on student attendance.

Another notable aspect is the system’s potential scalability. Future developments could integrate IoT technology and CCTV cameras, enabling seamless monitoring across multiple rooms or campuses. This versatility makes the system well-suited for larger institutions requiring efficient and automated attendance management.

6. CONCLUSION

This research has successfully developed an intelligent attendance system using face recognition and anti-spoofing technology, achieving an average accuracy of 98.90%. The system effectively addresses critical challenges such as ensuring accuracy, enhancing security, and improving efficiency in tracking educational staff attendance. Integrating the Haar Cascade Classifier with the Adaboost algorithm contributes to the system's high accuracy and reliability.

The primary contribution of this research is integrating anti-spoofing technology, which ensures the system’s suitability for sensitive environments. Additionally, the system’s scalability potential—through incorporating IoT and CCTV technologies—opens opportunities for deployment in more extensive and more complex settings. Future work could explore these developments further, allowing for attendance monitoring across broader institutional environments.

.

ACKNOWLEDGEMENT

Thank you to the research directorate of STMIK IKMI Cirebon for granting permission for the research location.

REFERENCES

[1] D. Armiady, “Absensi Kehadiran Menggunakan Kamera Pengawas Berbasis Teknologi Computer Vision,” *J. Tika*, vol. 6, no. 02, pp. 140–146, 2021, doi: 10.51179/tika.v6i02.541.
[2] D. I. Mulyana, Y. Yanti, A. Saputry, A. Ramadan, and S. Saragih, “Penerapan Face Recognition Dengan Algoritma Haar Cascade Untuk Sistem Absensi Pada Yayasan Pusat,” *J. Cahaya Mandalika*, pp. 215–226, 2022.
[3] 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, p. 1008, 2021, doi: 10.30865/mib.v5i3.3008.
[4] 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.
[5] T. Susim and C. Darujati, “Pengolahan Citra untuk Pengenalan Wajah (Face Recognition) Menggunakan OpenCV,” *J. Heal. Sains*, vol. 2, no. 3, pp. 534–545, 2021, doi: 10.46799/jsa.v2i3.202.
[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] R. S. Prince, R. U. . S. Sherwin, and E. . N. Meicsy, "Aplikasi Pengenalan Wajah Untuk Sistem Absensi Kelas Berbasis Raspberry Pi," *J. Tek. Inform.*, vol. 15, no. 3, pp. 179–188, 2020.
[8] H. Habiburrahman, "Sistem Presensi Berbasis Face Recognition," *Electrices*, vol. 1, no. 1, pp. 15–21, 2019, doi: 10.32722/ees.v1i1.1911.
[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] 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.
[11] E. Indra, M. D. Batubara, M. Yasir, and S. Chau, "Desain dan Implementasi Sistem Absensi Mahasiswa Berdasarkan Fitur Pengenalan Wajah dengan Menggunakan Metode Haar-Like Feature," *J. Teknol. dan Ilmu Komput. Prima*, vol. 2, no. 2, p. 11, 2019, doi: 10.34012/jutikomp.v3i1.637.
[12] R. Kosasih, "Pengenalan Wajah Menggunakan PCA dengan Memperhatikan Jumlah Data Latih dan Vektor Eigen," *J. Inform. Univ. Pamulang*, vol. 6, no. 1, p. 1, 2021, doi: 10.32493/informatika.v6i1.7261.
[13] R. Rossi, M. A. Lazarini, and K. Hirama, "Systematic Literature Review on the Accuracy of Face Recognition Algorithms," *EAI Endorsed Trans. Internet Things*, vol. 8, no. 30, p. e5, 2022, doi: 10.4108/eetiot.v8i30.2346.
[14] D. H. Fudholi, *Presensi Kelas Berbasis Pola Wajah Dan Tersenyum Menggunakan Deep Learning*. dspace.uii.ac.id, 2023. [Online]. Available: https://dspace.uii.ac.id/handle/123456789/42509
[15] S. J, J. Joshi, P. M, and U. B, "Face Recognition Based Attendance System Using OpenCV Python," *Adv. Intell. Syst. Technol.*, vol. 7, no. 10, pp. 52–56, 2022, doi: 10.53759/aist/978-9914-9946-1-2_10.
[16] V. Dores, "Identifikasi Masker pada Face Detection dengan Menggunakan Metode Haar Cascade dan CNN," *J. Sistim Inf. dan Teknol.*, vol. 4, pp. 149–154, 2022, doi: 10.37034/jsisfotek.v4i4.154.
[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] S. Sugeng and A. Mulyana, "Sistem Absensi Menggunakan Pengenalan Wajah (Face Recognition) Berbasis Web LAN," *J. Sisfokom (Sistem Inf. dan Komputer)*, vol. 11, no. 1, pp. 127–135, 2022, doi: 10.32736/sisfokom.v11i1.1371.
[19] Jamal Rosid, "Face Recognition Dengan Metode Haar Cascade dan Facenet," *Indones. J. Data Sci.*, vol. 3, no. 1, pp. 30–34, 2022, doi: 10.56705/ijodas.v3i1.38.
[20] D. R. NURUZZULFA, *PERBANDINGAN ADABOOST C4. 5 DAN ADABOOST NAIVE BAYES PADA KLASIFIKASI KORBAN KECELAKAAN LALU LINTAS DI KABUPATEN PATI*. repository.unimus.ac.id, 2020. [Online]. Available: http://repository.unimus.ac.id/4554