Infinity Engineering Journal
Vol. 2 No. 3, August (2026), pp. 134-141

ISSN 3090-5621 (online)
Published by Yayasan Cinta Negara Indonesia

A Comparative Literature Review of Facial and Fingerprint Authentication as Biometric Authentication Systems on Mobile Devices

Cindy Widya Lestari[1], Bayu Samudra[2], Roberto Kaban[3]
[1,2] Program Studi Sistem Informasi
[3] Program Studi Teknologi Informatika
[1,2,3] Institut Teknologi dan Bisnis Indonesia

A R T I C L E I N F O

Article history:

Received: Aug 5, 2026
Revised: Aug 20, 2026
Accepted: Aug 26, 2026

Keywords:

Biometrics
Facial Authentication
Face Recognition
Fingerprint
Security

ABSTRACT

This study aims to compare the effectiveness, advantages, disadvantages, security, and privacy of facial authentication (Face ID) and fingerprint authentication on mobile devices. The method used was a systematic literature review of scientific publications from Google Scholar, IEEE Xplore, and other reliable academic sources. The results of the study show that 3D-based Face ID offers a higher level of security against spoofing attacks, while fingerprint authentication excels in speed, accuracy under various environmental conditions, and user preference. Both methods store biometric data locally within a Trusted Execution Environment (TEE) or Secure Enclave to ensure the security of user data.

This is an open access article under the CC BY-NC license.

Corresponding Author:

Cindy Widya Lestari
Program Studi Sistem Informasi
Institut Teknologi dan Bisnis Indonesia
Jl. Binjai - Stabat No. Desa, Tandem Hilir, Sumatera Utara 20374. Indonesia
Email: cindywidialestari@gmail.com

1. INTRODUCTION

In today's modern world, mobile devices play a crucial role. Their role is so significant that they influence every aspect of people's daily lives. The need to ensure information security on mobile devices is becoming increasingly important and increasingly challenging. Certain human biometric features—such as fingerprints, facial features, hand geometry, voice, and iris patterns—are used to authenticate users in security systems to achieve a high level of security, replacing traditional password-based systems. This journal article presents the application of facial recognition algorithms on mobile devices (Sriyati et al., 2020).

Biometric authentication is a critical feature in today's smartphones, particularly for regulated industries and government agencies. Using unique biometric identifiers to authenticate users provides a high level of protection for sensitive data, while mobile users enjoy a convenient unlocking and login experience. It is literally security at your fingertips (Arridla & Hartati, 2025).

The term "biometrics" has become extremely important in the field of computer security. Human physical characteristics such as fingerprints, faces, palms, body geometry, voices, and irises are known as biometric data. These features are used to authenticate users in computer-based security systems to achieve a high level of security as an alternative to traditional password systems. Usernames and passwords can be replaced and/or used in conjunction with one of these biometric features to provide two-factor authentication. Facial recognition is the most suitable biometric method for authentication on mobile devices, as these devices typically have cameras (Jannah et al., 2024).

In today's digital age, the use of biometric authentication technology is becoming increasingly widespread, particularly on smartphones. Biometric authentication offers a more advanced security solution compared to traditional methods such as passwords or PINs. This system allows users to access devices or applications more quickly, conveniently, and securely, using unique characteristics such as fingerprints or facial recognition. These advantages have made biometric authentication the

top choice for app developers looking to enhance user convenience while reducing the risk of data theft (Yeovandi et al., 2025).

The implementation of a login system in smartphone apps is noted for providing a more secure authentication solution for users. In this context, this system is associated with a lower risk of data theft or unauthorized access, given that biometric authentication tends to be more difficult to forge compared to password-based methods. Furthermore, the use of biometrics allows users to access their accounts more quickly and conveniently—simply by using a fingerprint or facial scan—without having to remember various complex password combinations or patterns (Andini, 2025).

Face recognition uses the entire face, extracts facial features, and is capable of recognizing faces in real-time video (Natbais et al., 2024). Facial recognition technology has long been a subject of study in computer science, particularly in the field of biometric security. Since the early 1990s, geometry- and texture-based facial recognition methods have been used to distinguish individual identities (Nurhidayanti, 2025). Face ID is a facial recognition-based authentication system that uses cameras and sensors to map a user's facial features. There are two approaches: 3D systems such as Apple's TrueDepth, and 2D systems based on standard RGB cameras on Android devices (Ummu, 2024).

Although facial recognition technology has been around for a long time, significant challenges remain in its implementation. Variations in lighting, changes in viewing angles, differences in facial expressions, and image quality often reduce the system's accuracy. Conventional approaches based on traditional feature extraction have proven inadequate at delivering optimal results when the system is confronted with dynamic real-world conditions. This has led to the emergence of deep learning methods, particularly Convolutional Neural Networks (CNNs), which have proven to be more adaptive and possess better generalization capabilities in recognizing complex patterns in facial images (Nurhidayanti, 2025).

Fingerprint recognition is a biometric technology that has been in use for a long time and has proven to have a high level of accuracy. This system reads the unique patterns on a fingerprint—such as lines and dots (minutiae)—which are never identical, even among identical twins. The authentication process is carried out by placing a finger on the sensor. The sensor then scans and matches the pattern with stored data. The main advantages of fingerprint recognition are its high reliability and accuracy, making it a highly dependable choice for stricter security requirements (Mu'min, 2025).

Modern sensor technology also comes equipped with liveness detection capabilities, which can distinguish between live tissue and fake replicas. This makes it difficult for others to forge fingerprints, which is why we often see this technology in high-security areas such as server rooms, laboratories, or safes. However, fingerprint recognition has limitations under certain conditions. Sensor performance can decline if a finger is wet, dirty, injured, or has a change in texture. Additionally, because it requires physical contact, this technology also falls short in terms of hygiene, especially when there are many users taking turns using the device (Falasifah et al., 2022).

Fingerprint authentication works in three stages: image capture, minutiae feature extraction, and matching against a stored template. There are three types of sensors: capacitive, optical, and ultrasonic, with ultrasonic being the most accurate. Ultrasonic sensors offer a FAR below 0.001%, but they remain vulnerable to BrutePrint attacks that exploit CAMF and MAL vulnerabilities (Munandar, n.d.).

2. METHOD

This study employs a literature review design with a descriptive-comparative qualitative approach. This method was chosen because the primary objective of the study is to explore, evaluate, and compare two existing biometric authentication technologies—face recognition and fingerprint scanning—specifically within the mobile device ecosystem (Meldyantono, 2025).

This study did not conduct direct laboratory testing of hardware or develop new program code. Instead of using primary data, this study relied on secondary data obtained from reputable scientific journal articles, conference proceedings, and relevant official technical reports (Maskandi et al., 2025).

A comparative analysis was conducted systematically by comparing empirical data from various previous studies. The parameters compared focused on three main aspects: system accuracy (False Acceptance Rate and False Rejection Rate), vulnerability to cyberattacks (spoofing attacks), and user convenience (usability). Through this design, the study is expected to provide an

objective and comprehensive synthesis of the strengths and weaknesses of each biometric authentication system currently used on mobile devices (Jannah et al., 2024).

References

The literature search was conducted using several reputable academic databases, namely:

A. Google Scholar
B. Journal of Information Technology and Multimedia (JTIM)
C. NIST (National Institute of Standards and Technology) technical reports
D. ISO/IEC 19795 standard publication on biometric testing.

Research Process

To provide a systematic overview of the research stages, this literature review was conducted in several interrelated phases. The research process begins with determining the research topic, establishing the research objectives, searching for literature in various scientific sources, selecting relevant literature, conducting a comparative analysis of facial recognition and fingerprint authentication technologies, and finally, drawing research conclusions. This research flowchart is presented in Figure 1.

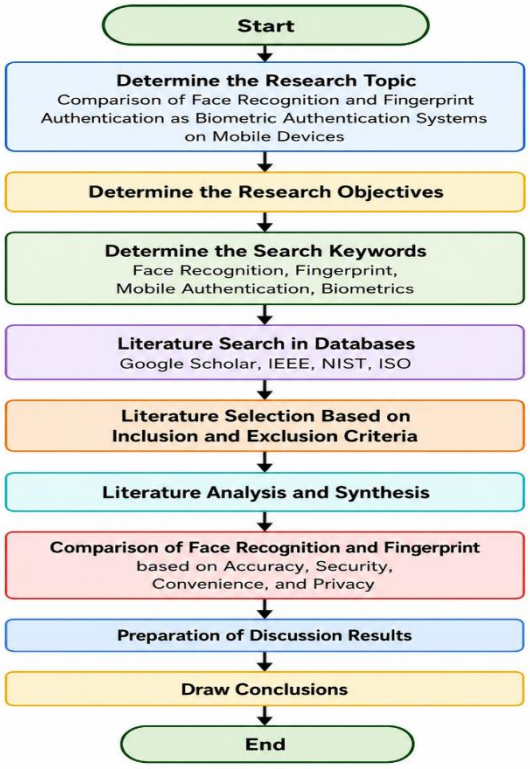


Figure 1. Research Methodology FlowchartResearch Methodology Flowchart

Based on Figure 1, the study began by defining the topic: a comparison of facial and fingerprint authentication as biometric authentication systems on mobile devices. Next, the research objective was established to identify the advantages, disadvantages, security levels, and performance of these two authentication technologies. The next step was to conduct a literature review using various relevant scientific sources, such as Google Scholar, IEEE Xplore, publications from the National Institute of Standards and Technology (NIST), and the ISO/IEC 19795 standard. The literature was then studied and analyzed comparatively by comparing aspects of security, accuracy, ease of use, and implementation on mobile devices. The results of this analysis are then compiled into a comprehensive discussion to serve as the basis for drawing research conclusions (Hidayat et al., 2025).

3. RESULTS AND DISCISSION

Comparison of Face ID and Fingerprint Recognition

The following table compares Face ID and fingerprint recognition as biometric authentication technologies on mobile devices, examining aspects such as technology, accuracy, security, convenience, environmental conditions, data storage, vulnerabilities, security standards, and their implementation on various devices.

Table 1. Comparison of Face Recognition and Fingerprint Authentication on Mobile Devices

Parameter	Face Recognition	Fingerprint
Technology	3D TrueDepth camera and 2D RGB camera	Ultrasonic, capacitive, and optical sensors
Identification Method	Facial feature mapping	Fingerprint minutiae pattern matching
False Acceptance Rate (FAR)	Approximately 1 in 1,000,000 for 3D systems	Less than 0.001% or approximately 1 in 50,000
Resistance to Spoofing Attacks	Very high in 3D systems, but lower in 2D systems	High when using ultrasonic sensors, although still vulnerable to fingerprint replicas
User Convenience	Contactless authentication	Touch-based authentication
Environmental Influence	Affected by lighting conditions, facial position, and the use of face masks	Affected by finger conditions such as moisture, dirt, or physical injuries
Biometric Data Storage	Trusted Execution Environment (TEE) or Secure Enclave	Trusted Execution Environment (TEE) or Secure Enclave
Primary Security Threats	Presentation attacks, deepfakes, and face spoofing	BrutePrint attacks, CAMF attacks, MAL attacks, and fingerprint replicas
Implementation	Commonly deployed on iOS devices and selected premium Android smartphones	Widely implemented on Android and iOS devices
Advantages	High security level and contactless authentication	Fast, practical, and reliable authentication process
Limitations	Sensitive to lighting conditions and facial occlusions	Sensitive to finger conditions and sensor cleanliness

Source: Compiled by the author based on Apple (2024), Samsung (2019), Chen & He (2023), ISO/IEC 19795 (2021), and the National Institute of Standards and Technology (2023).

Based on Table 1, face recognition and fingerprint technologies have different characteristics in supporting biometric authentication systems on mobile devices. These differences are evident in the technologies used, security levels, accuracy, ease of use, and factors that influence authentication performance. Each technology was developed to meet digital security needs using different approaches; therefore, the choice of technology depends heavily on user needs and the implementation environment.

From a technological standpoint, Face Recognition uses cameras and facial recognition algorithms to identify each individual's unique characteristics. On modern devices, particularly those using TrueDepth Camera technology, the authentication process is carried out through three-dimensional facial mapping, resulting in more accurate identification that is more resistant to identity spoofing attempts. In contrast, Fingerprint works by reading fingerprint patterns using optical, capacitive, or ultrasonic sensors, which are then compared to biometric data stored on the device (PRATAMA, 2020).

From a security perspective, 3D-based facial recognition offers a higher level of protection against spoofing attacks because it can recognize facial depth and detect the user's biological characteristics. Meanwhile, fingerprint authentication still offers a high level of security, particularly with ultrasonic sensors equipped with liveness detection technology. However, this system remains vulnerable to attacks using fingerprint replicas if the detection mechanism is not implemented optimally.

In terms of user convenience, both technologies offer different advantages. Face Recognition provides a contactless authentication experience, making it more practical in certain situations. On the other hand, Fingerprint offers a faster and more reliable authentication process because users simply need to place their finger on the sensor without having to adjust the device's position or lighting. These advantages make fingerprint authentication the primary choice on various smartphones, especially for everyday use (Jannah et al., 2024).

Overall, the comparison results show that no single technology is completely superior to the others. Face recognition is better suited for environments that require a high level of security, while fingerprint recognition is superior in terms of efficiency, speed, and ease of use. Therefore, current trends in mobile device development tend to integrate both technologies as complementary biometric authentication systems, thereby enhancing security while providing a better user experience.

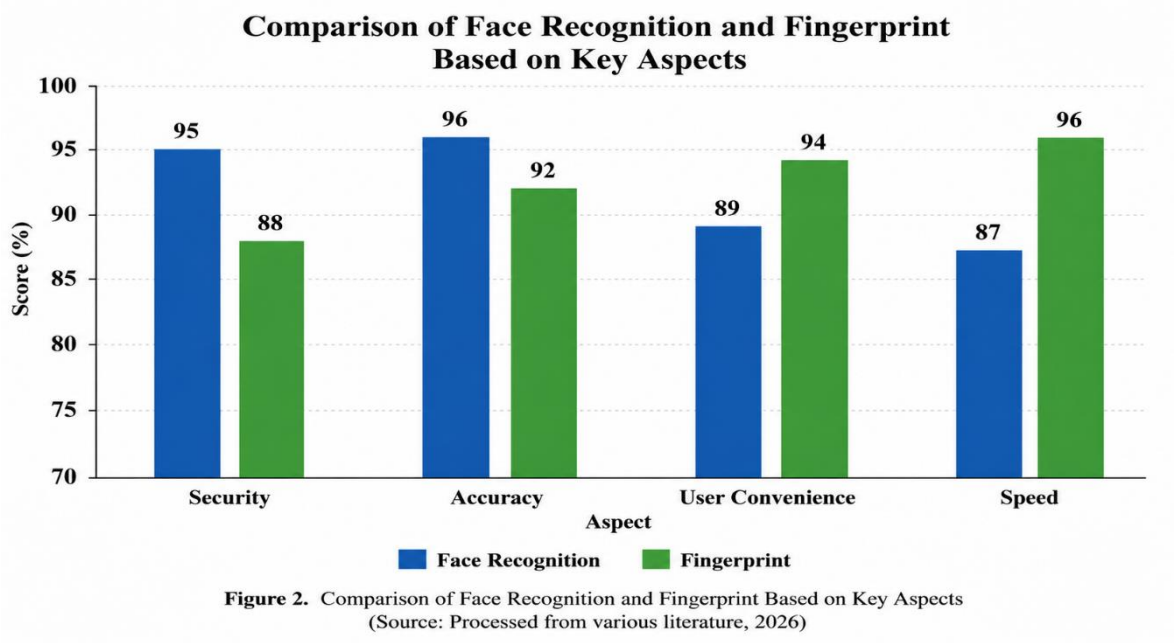


Figure 2. Comparison of Face Recognition and Fingerprint Based on Key Aspects
(Source: Processed from various literature, 2026)

Based on Figure 2, the two biometric technologies exhibit different characteristics across each analyzed aspect. Face Recognition demonstrates superiority in terms of security and accuracy because it utilizes three-dimensional (3D) face mapping, which reduces the risk of spoofing attacks. Additionally, this technology has an extremely low False Acceptance Rate (FAR), thereby providing a higher level of protection against unauthorized access.

On the other hand, fingerprint authentication is superior in terms of authentication speed and ease of use. The fingerprint verification process can be performed quickly without requiring the device to be in a specific position, making it more practical for everyday use. However, fingerprint authentication performance can be affected by the physical condition of the finger, such as if it is wet, dirty, or injured (Hakim et al., n.d.).

Overall, the results of the literature review indicate that facial recognition is better suited for applications that prioritize a high level of security, while fingerprint recognition is better suited for users who prioritize speed and ease of access. Therefore, many modern mobile devices are beginning to integrate these two technologies as complementary biometric authentication systems (Wijaya et al., 2026).

Comparison of Security and Accuracy

Security and accuracy are two key indicators for evaluating the performance of biometric authentication systems on mobile devices. The security level reflects the system's ability to prevent access by unauthorized users, while accuracy describes the system's ability to correctly recognize a user's identity without producing authentication errors. Both aspects are critical factors in determining the effectiveness of biometric technology implementations on smartphones (Fauzi et al., 2025).

Based on a literature review, three-dimensional (3D) face recognition technology offers a very high level of security because it utilizes facial depth mapping, analysis of biological characteristics, and liveness detection mechanisms. This technology is capable of distinguishing real faces from photos, videos, or three-dimensional replicas, thereby minimizing the risk of presentation attacks or spoofing attacks. In addition, this system has an extremely low False Acceptance Rate (FAR)—approximately 1 in 1,000,000—making it highly unlikely that an unauthorized user will gain access to the device.

Conversely, fingerprint authentication also offers a high level of security, particularly on devices that use ultrasonic sensors. These sensors can read the structure of a fingerprint down to the skin layers, making them more difficult to forge than optical or capacitive sensors. Some devices

have also implemented liveness detection technology to ensure that the scanned fingerprint comes from living tissue. However, research by Chen and He (2023) shows that fingerprint authentication remains vulnerable to BrutePrint attacks that exploit weaknesses in the Cancel After Match Fail (CAMF) and Match After Lock (MAL) mechanisms, meaning that security aspects still require further development.

In terms of accuracy, both technologies perform very well in recognizing users' identities. Face recognition has a high accuracy rate as long as the scanning process is conducted under adequate lighting conditions and the user's face is not covered by a mask or other accessories. Meanwhile, fingerprint authentication tends to provide consistent results under various usage conditions, although its performance may decline if the finger is wet, dirty, injured, or has changes in skin texture (SUJIYANTO, 2025).

The analysis results show that Face Recognition is superior in terms of security because it is better equipped to handle various forms of identity spoofing attacks. On the other hand, Fingerprint remains a highly effective option because it offers a high level of accuracy, a fast authentication process, and wider implementation across various types of mobile devices. Therefore, the choice of biometric authentication technology should be tailored to user needs, the desired level of security, and the characteristics of the device's usage environment (Yeovandi et al., 2025).

Comparison of User Comfort

In addition to security and accuracy, usability is a key factor influencing the acceptance of biometric authentication technology by mobile device users. An authentication system that is secure but difficult to use tends to diminish the user experience, while a system that is easy to use but has a low level of security is also unable to provide optimal protection. Therefore, striking a balance between security and usability is one of the primary considerations in the development of biometric authentication technology (Nurhidayanti, 2025).

Based on the results of a literature review, face recognition offers a more practical authentication experience because the verification process is contactless. Users simply need to face the camera so that the authentication process can take place automatically without having to touch the device. This approach provides convenience, especially when the user's hands are carrying items, wearing gloves, or in situations that make it difficult to use a fingerprint sensor. However, this convenience may be reduced if lighting conditions are inadequate, the face is covered by a mask, certain accessories are worn, or the device's position does not align with the scanning angle required by the system (Pando T, 2022).

On the other hand, fingerprint authentication remains one of the most widely used methods on mobile devices because it offers a fast, simple authentication process that is easy for users to understand. Users simply need to place their finger on the sensor without having to face the camera. This technology can also be used effectively under various lighting conditions, providing a relatively stable authentication experience. However, fingerprint sensor performance may decline if the finger is wet, dirty, injured, or has changes in skin texture; under certain conditions, the authentication process may need to be repeated more than once (SAPUTRA, 2025).

From a user experience perspective, both technologies offer distinct advantages. Face recognition provides convenience through a contactless authentication process and more natural integration with the device's interface, while fingerprint recognition offers high authentication speed with consistent success rates in everyday use. Therefore, some modern smartphone manufacturers no longer rely solely on a single authentication method but have begun combining Face Recognition and Fingerprint as a multimodal biometric authentication system. This approach allows users to choose the authentication method best suited to their usage conditions, while also enhancing the device's flexibility and security (SAPUTRA, 2025).

Overall, the results of the analysis show that no single technology is absolutely superior to others in terms of convenience. The choice of authentication method is heavily influenced by user needs, device usage habits, environmental conditions, and the desired level of security. Therefore, integrating both biometric technologies into mobile devices is the most effective solution for creating a secure, fast, and user-friendly authentication system (Johan et al., 2025).

4. CONCLUSION

Based on the results of the literature review and comparative analysis conducted, it can be concluded that 3D-based facial recognition and fingerprint scanning systems exhibit different performance characteristics and security levels on mobile devices. 3D face recognition technology (such as

Apple's TrueDepth) demonstrates significant advantages in terms of security, with a False Acceptance Rate (FAR) of 1:1,000,000 and high resistance to spoofing attacks using 2D photos or masks. However, the effectiveness of this system tends to decrease in environments with extreme lighting conditions or when users wear facial accessories such as masks. On the other hand, fingerprint authentication—particularly that using the latest ultrasonic sensors—offers high access speed and reliability in various environmental conditions, with a FAR below 0.001%. Nevertheless, fingerprint systems have critical vulnerabilities to BrutePrint-based cyberattacks that exploit zero-day vulnerabilities such as Cancel After Match Fail (CAMF) and Match After Lock (MAL), as well as functional limitations when the user's finger is wet or dirty. Both systems have met modern privacy standards by storing and processing biometric data locally within isolated areas such as a Trusted Execution Environment (TEE) or Secure Enclave. No single technology is absolutely superior, as the choice of system depends heavily on the user's priorities regarding security and convenience. As a recommendation for future research and development, the implementation of a multimodal (multi-biometric) authentication system that combines facial and fingerprint scanning is the most optimal solution for providing both a dual layer of security and flexibility on mobile devices.

REFERENCES

Andini, N. P. (2025). *Implementasi biometric online onboarding dalam upaya meningkatkan transaksi nasabah: studi kasus Bank Syariah Indonesia KCP Kisaran*. UIN Syekh Ali Hasan Ahmad Addary Padangsidimpuan.

Arridla, H. I., & Hartati, S. (2025). *Keamanan Informasi dan Data*. Penerbit NEM.

Falasifah, N., Umamah, R., & Harfuddin, Y. I. (2022). Penerapan Teknologi Tepat Guna Tempat Hand Sanitizer Sistem Pedal Pijak dalam Pencegahan Penyebaran Covid-19 di Sidoarjo: Application of Appropriate Technology for Touchless Pedal System Hand Sanitizer in Preventing the Spread of Covid-19 in Sidoarjo. *Amalee: Indonesian Journal of Community Research and Engagement*, *3*(1), 11–19.

Fauzi, A., Aprilla, I. N., Fauziyyah, N., & Bachtiar, N. F. (2025). Implementasi Multi-Faktor Authentication, Single Sign-on dan Role-Based Access Control dalam Keamanan Sistem Informasi (Studi Literature Review). *Fibonacci: Jurnal Ilmu Ekonomi, Manajemen Dan Keuangan*, *2*(1), 33–45.

Hakim, M. L., Syamsid, A. Q., & Ainul, M. M. (n.d.). *Analisis Perbandingan Efisiensi Mekanisme Otentikasi Password dan Biometrik Berbasis Penggunaan Harian pada Smartphone*.

Hidayat, R., Fitri, R. A., & Hermina, D. (2025). Langkah Penelitian Manajemen Pendidikan: Penemuan Masalah, Telaah Pustaka, Persiapan Penelitian, Pengumpulan Data, Analisis Data Dan Penyimpulan/Pemaknaan, Dan Pelaporan & Evaluasi Penelitian. *Jurnal Riset Multidisiplin Edukasi*, *2*(6), 509–523.

Jannah, M., Hidayat, M. F., Agustiyyani, M., Buana, P. W., & Purwani, F. (2024). Implementasi Autentikasi Biometrik untuk Meningkatkan Keamanan dan Privasi Pengguna Dompet Digital. *Journal of Scientech Research and Development*, *6*(2), 531–539.

Johan, C. K., Abdullah, D., Wijaya, A., & Imanullah, M. (2025). IMPLEMENTASI SMART PADLOCK GUNA MENINGKATKAN SISTEM KEAMANAN PADA KENDARAAN RODA DUA BERBASIS SIDIK JARI DAN MIKROKONTROLER ESP32. *JATI (Jurnal Mahasiswa Teknik Informatika)*, *9*(6), 9758–9763.

Maskandi, L., Irwan, M. P. M., Murcahyanto, M. P. D. H., & Haritani, M. H. D. H. H. (2025). *PARADIGMA BARU PENELITIAN PENDIDIKAN Fondasi, Metode, Dan Inovasi Untuk Abad Ke-21*. Hamzanwadi Press.

Meldyantono, A. P. (2025). *Implementasi Sistem Absensi Berbasis Pengenalan Wajah Menggunakan Metode Cnn Dan Model Facenet*. Universitas Islam Sultan Agung Semarang.

Mu'min, M. A. (2025). Desain Sistem Keamanan Sepeda Motor Menggunakan Mikrokontroller Arduino dan Sensor Fingerprint ZFM-60 Berbasis Mobile. *Scientific: Journal of Computer Science and Informatics*, *2*(1), 40–47.

Munandar, L. K. (n.d.). *MENGENAL JENIS–JENIS SENSOR DAN PEMANFAATANNYA DI DUNIA INDUSTRI KNOWING THE TYPES OF SENSORS AND THEIR USE IN THE INDUSTRIAL WORLD*.

Nurhidayanti, M. (2025). Penerapan Deep Learning dalam Pengenalan Wajah untuk Sistem Keamanan. *Jurnal Informatika Indonesia*, *1*(1), 29–37.

Pando T, A. C. (2022). *FAKTOR YANG BERHUBUNGAN DENGAN KELUHAN KELELAHAN MATA (ASTENOPIA) PADA KARYAWAN DINAS KOMUNIKASI INFORMATIKA DAN*

PERSANDIAN KABUPATEN SINJAI= Factors Associated with Delaying Eye Fatigue (Asthenopia) in Employees of the Information Communications and Encoding Office of Sinjai Regency. Universitas Hasanuddin.

PRATAMA, T. A. (2020). *Rancang Bangun Akses Ruangan Dengan Teknologi (Biometrik) Sidik Jari Berbasis Web*. POLITEKNIK NEGERI SRIWIJAYA.

SAPUTRA, C. (2025). *SISTEM PENGAMAN PINTU RUMAH DENGAN TEKNOLOGI BIOMETRIK SIDIK JARI MENGGUNAKAN ESP32 DAN ANDROID BERBASIS IOT*. UNIVERSITAS ISLAM NEGERI SULTAN SYARIF KASIM RIAU.

Sriyati, S., Setyanto, A., & Luthfi, E. E. (2020). Literature Review: Pengenalan Wajah Menggunakan Algoritma Convolutional Neural Network. *Jurnal Teknologi Informasi Dan Komunikasi (TIKomSiN)*, *8*(2).

SUJIYANTO, D. A. D. I. (2025). *Penggunaan Sidik Jari Sebagai Otentikasi Identitas Penghadap Dalam Minuta Akta Notaris Berbasis Sistem Elektronik*. Universitas Islam Sultan Agung Semarang.

Ummu, Q. (2024). *MEDIA PEMBELAJARAN NETS OF 3D SHAPES BERBASIS ANDROID UNTUK SISWA SEKOLAH DASAR MENGGUNAKAN 3D OBJECT MARKER*.

Wijaya, T. K., Missyamsu Algusri, S. T., Wicaksono, A. W., Meku, R. N. D., & Roland, R. (2026). *Teknologi Smart Door Lock Berbasis Face Recognition: Konsep, Desain, dan Implementasi pada Sistem Keamanan Modern*. PT Penerbit Qriset Indonesia.

Yeovandi, F., Sabariman, S., & Prasetyo, S. E. (2025). Evaluasi Keamanan Sistem Autentikasi Biometrik pada Smartphone dan Rekomendasi Implementasi Optimal. *Jurnal Teknologi Informasi Dan Multimedia*, *7*(1), 133–148.