

Implementasi Servo Lock System yang Terintegrasi Pengenalan Wajah untuk Keamanan Rak Senjata Otomatis

Yossy Tamara Putra¹⁾, Elga Aris Prasetyo²⁾, Ananda Herdi Akbar³⁾*

^{1), 2), 3)} Prodi Teknik Telekomunikasi Militer, Politeknik Angkatan Darat, Jl. Raya Anggrek No.1 Junrejo, Batu, Indonesia

E-mail: yossytamara2118@gmail.com¹⁾, elgaarisprastyo@office-teknolab.biz.id²⁾, aherdiakbar@gmail.com³⁾

Implementation of a Servo Lock System Integrated with Facial Recognition for the Security of Automatic Weapons Racks

Abstract: Military armories require strict monitoring of their security systems to prevent unauthorized use. The purpose of this research is to implement and evaluate a prototype of an automated weapon rack locking system based on face recognition. A quantitative descriptive method with an experimental approach was used. The HIKVISION DS-K1T343MFX terminal serves as the authentication device, the ESP32 microcontroller as the main controller, and the MG996R servo motor as the actuator. Parameters including False Acceptance Rate (FAR), False Rejection Rate (FRR), response time, as well as distance and light intensity variations, were used to evaluate system performance. The test results show that the prototype has a high level of accuracy with a FAR of 0% and an FRR of 0%, and it is capable of rejecting unauthorized access attempts using facial photos (spoofing). The average system response time from the scanning process to unlocking is 2.20 seconds. The system operates validly within a successful operating range of 30 cm to 150 cm, achieving the fastest response time at a distance of 100 cm, and successfully performed authentication across the three tested lighting conditions (morning at 67 lux, daylight at 857 lux, and night at 0 lux) with 10 repetitions per condition. In conclusion, this face recognition-based servo lock prototype has been successfully implemented and has the potential to be an efficient alternative for supporting the management of defense equipment protection in military units.

Keywords: Face Recognition, ESP32, Servo Lock, Weapon Rack, FAR, FRR

Abstrak: Gudang senjata militer membutuhkan pengawasan yang ketat untuk sistem keamanannya agar tidak dapat disalahgunakan. Tujuan dari penelitian ini adalah untuk menerapkan dan mengevaluasi prototipe sistem penguncian rak senjata otomatis berbasis pengenalan wajah. Metode kuantitatif deskriptif yang digunakan adalah eksperimental. Terminal HIKVISION DS-K1T343MFX berfungsi sebagai perangkat autentikasi, mikrokontroler ESP32 berfungsi sebagai pusat kendali, dan motor servo MG996R berfungsi sebagai aktuator. Parameter False Acceptance Rate (FAR), False Rejection Rate (FRR), waktu respons, serta variasi jarak dan intensitas cahaya digunakan untuk mengevaluasi kinerja sistem. Hasil pengujian pada skenario yang ditetapkan menunjukkan nilai observasi FAR sebesar 0% dan FRR sebesar 0%, serta sistem mampu menolak upaya akses ilegal menggunakan skenario foto wajah (photo-based spoofing). Rata-rata waktu respons sistem dari proses pemindaian hingga terbukanya kunci adalah 2,20 detik. Sistem beroperasi secara valid pada rentang jarak keberhasilan operasi

(successful operating range) 30 cm hingga 150 cm dengan titik waktu respons tercepat pada jarak 100 cm, dan berhasil melakukan autentikasi pada tiga kondisi pencahayaan yang diuji (pagi 67 lux, siang 857 lux, dan malam 0 lux) dengan masing-masing 10 kali pengulangan. Kesimpulannya, prototipe servo lock berbasis pengenalan wajah ini berhasil diimplementasikan dan berpotensi menjadi alternatif untuk mendukung tata kelola perlindungan alutsista pada satuan militer. Kata kunci: ESP32, Face Recognition, FAR, FRR, Rak Senjata, Servo Lock.

PENDAHULUAN

Gudang senjata merupakan fasilitas strategis di lingkungan militer yang menyimpan aset alutsista penting, yang membutuhkan sistem keamanan dan pengawasan yang sangat baik. Praktiknya, di Poltekad pengamanan rak senjata masih mengandalkan metode konvensional seperti kunci mekanik, rantai, atau gembok. Metode ini memiliki kelemahan termasuk risiko duplikasi kunci yang tinggi, bergantung pada kelalaian manusia, dan tidak adanya pencatatan riwayat akses otomatis. Kelemahan ini menyebabkan sistem konvensional memiliki keterbatasan dalam menerapkan pembatasan akses secara individual berdasarkan hak akses personel terhadap senjata tertentu. Ini berpotensi menyebabkan kesalahan distribusi dan penyalahgunaan senjata.

Dibutuhkan sistem keamanan yang modern untuk melakukan autentikasi, memberikan atau menolak akses, mengontrol mekanisme pengunci, dan secara otomatis mencatat aktivitas. Sistem tertanam menawarkan mekanisme pengendalian akses elektronik yang tepat, salah satunya adalah sistem penguncian menggunakan

motor servo yang dikelola oleh mikrokontroler. Motor servo dipilih karena memiliki keunggulan dalam pengaturan posisi sudut yang presisi dan torsi yang memadai untuk menggerakkan mekanisme tuas pengunci. Sistem ini perlu diintegrasikan dengan metode autentikasi biometrik. Teknologi pengenalan wajah (face recognition) berbasis deep learning [1] dipilih karena sifatnya yang contactless (tanpa sentuhan), lebih higienis, dan tidak rentan terhadap keausan fisik dibandingkan sensor sidik jari (fingerprint), PIN, atau kartu RFID. Selain akurasi identifikasi, sistem biometrik modern juga menuntut ketahanan terhadap serangan pemalsuan presentasi (presentation attack atau spoofing) melalui fitur deteksi keaslian wajah (liveness detection) [2]. Selain akurasi identifikasi, sistem biometrik modern juga menuntut ketahanan terhadap serangan pemalsuan presentasi (presentation attack atau spoofing) melalui fitur deteksi keaslian wajah (liveness detection). Dalam penelitian ini, algoritma pengenalan wajah dan fitur deteksi keaslian (liveness detection) tidak dikembangkan dari awal, melainkan memanfaatkan kemampuan fitur bawaan dari

terminal biometrik komersial HIKVISION DS-K1T343MFX.

Beberapa penelitian sebelumnya telah menerapkan teknologi keamanan serupa, di antaranya pemanfaatan sensor sidik jari dan citra wajah berbasis Raspberry Pi untuk pengamanan senjata elektrik [3], serta penggunaan sistem biometrik fingerprint untuk rak penyimpanan senjata laras pendek elektronik [4]. Penelitian lainnya membahas pengamanan pusat data dan sistem loker pintar menggunakan mikrokontroler ESP32 dan aktuator motor servo untuk kontrol akses otomatis [5]. Namun, kajian state of the art menunjukkan bahwa sebagian besar prototipe terdahulu umumnya hanya mengendalikan satu aktuator tunggal atau belum mengintegrasikan manajemen hak akses spesifik per kompartemen dengan protokol perpesanan ringan (lightweight messaging) untuk rak senjata laras panjang. Oleh karena itu, kebaruan (novelty) dari penelitian ini terletak pada arsitektur integrasinya, yaitu perancangan alur sistem mulai dari autentikasi biometrik pada terminal HIKVISION, validasi hak akses per rak melalui API, pengiriman instruksi via protokol MQTT yang andal untuk komunikasi mesin-ke-mesin (M2M) [6], hingga eksekusi multi-aktuator servo lock (11 slot rak) oleh satu unit mikrokontroler ESP32. Perangkat autentikasi wajah, mikrokontroler ESP32, dan motor

servo digunakan dalam penerapan serta evaluasi prototipe sistem pengunci otomatis pada rak senjata laras panjang. Kinerja sistem dievaluasi menggunakan parameter observasi False Acceptance Rate (FAR), False Rejection Rate (FRR), dan waktu respons sejak pemindaian wajah hingga aktuator terbuka. Target desain pada penelitian ini menetapkan batas toleransi operasional nilai $FAR \leq 5\%$, $FRR \leq 5\%$, dan waktu respons maksimal 3 detik. Diharapkan prototipe ini dapat menjadi salah satu alternatif pengembangan tata kelola pengamanan rak senjata yang berpotensi mempermudah akses dan pencatatan dibandingkan mekanisme kunci mekanik konvensional.

METODE PENELITIAN

Penelitian ini menggunakan metode kuantitatif deskriptif dengan pendekatan eksperimental untuk merancang, mengimplementasikan, dan menguji kinerja servo lock system pada rak senjata [7].

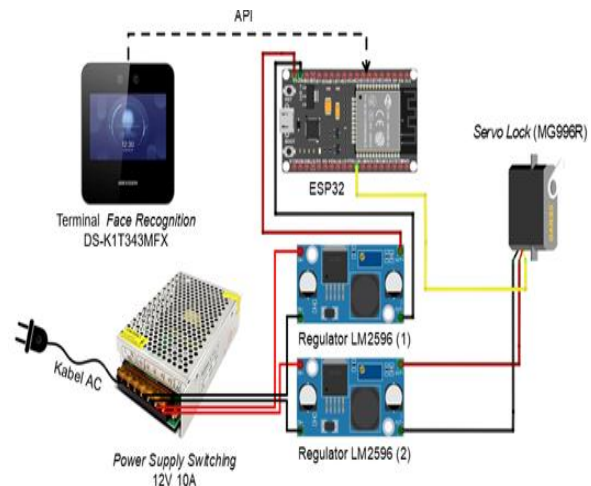
2.1 Perancangan Perangkat Keras dan Arsitektur Sistem

Sistem keamanan ini dibangun menggunakan tiga komponen utama: Terminal Face Recognition HIKVISION DS-K1T343MFX sebagai perangkat autentikasi biometrik, papan pengembang (development board) mikrokontroler ESP32 DOIT DevKit V1 (berbasis modul ESP-WROOM-32) sebagai pusat kendali dengan modul Wi-Fi

terintegrasi [8], dan motor servo MG996R sebagai aktuator pengunci mekanik [5]. Prototipe ini dirancang pada skala satu unit pengontrol sentral (ESP32) yang dikonfigurasi untuk mengendalikan 11 motor servo fisik yang mewakili 11 slot rak senjata individu. Masing-masing servo dihubungkan pada pin General Purpose Input/Output (GPIO) yang berbeda pada ESP32.

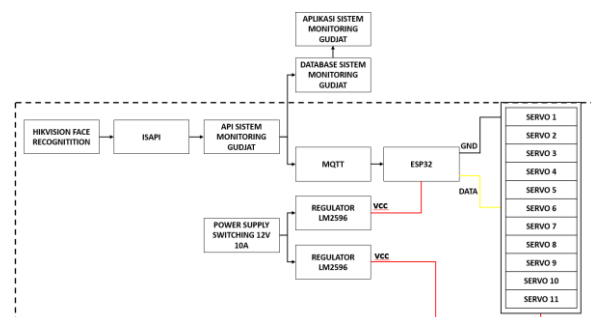
Untuk menjaga kestabilan daya dan mencegah noise akibat lonjakan arus dari 11 aktuator tersebut, sistem menggunakan power supply switching 12V 10A yang diturunkan tegangannya melalui dua buah regulator LM2596. Satu regulator (LM2596 1) dikonfigurasi pada tegangan keluaran 7,5 V khusus untuk menyuplai papan pengembang ESP32 DOIT DevKit V1 dengan menghubungkan jalur keluaran positifnya secara spesifik ke pin masukan VIN pada development board (bukan pin keluaran 3V3 maupun jalur 5V USB), sehingga tegangan tersebut diturunkan secara aman oleh regulator Low-Dropout (LDO) internal AMS1117 menjadi tegangan kerja logika 3,3 V. Sementara itu, regulator lainnya (LM2596 2) diatur pada tegangan 6,5 V secara terisolasi khusus untuk memberikan suplai daya utama ke seluruh 11 motor servo dengan jalur ground (GND) yang disatukan (common ground) terhadap ESP32. Mekanisme pengunci dirancang

menggunakan plat besi setebal 2 mm dan bersifat portable sehingga dapat dipasang pada dasar popor rak senjata tanpa merusak struktur aslinya.



Gambar 1 Arsitektur Perangkat Keras Sistem

2.2 Alur Komunikasi dan Logika Akses

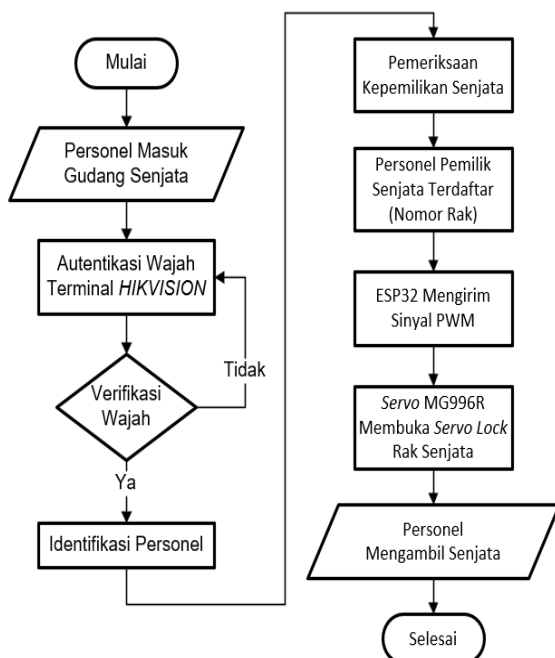


Gambar 2 Blok Diagram Sistem

Alur kerja sistem mengintegrasikan komunikasi jaringan dan kontrol perangkat keras. Proses dimulai saat wajah personel dipindai oleh terminal HIKVISION. Hasil verifikasi tersebut dikirimkan ke API Sistem Monitoring Gudang Senjata menggunakan antarmuka protokol ISAPI (Intelligent Security Application Programming Interface). Pada

tahap ini, API akan melakukan validasi hak akses personel terhadap nomor rak senjata tertentu.

Apabila identitas personel sah dan memiliki hak akses, server akan mengirimkan perintah pembukaan kunci melalui protokol MQTT yang dikenal ringan dan stabil untuk ekosistem IoT [9]. Payload data dari MQTT tersebut memuat informasi spesifik mengenai target nomor rak (misalnya identifikasi Rak 3). Mikrokontroler ESP32 yang mendengarkan (subscribe) topik MQTT tersebut kemudian mengekstraksi data nomor rak, lalu membangkitkan sinyal Pulse Width Modulation (PWM) secara spesifik pada pin GPIO yang terhubung dengan aktuator Servo 3, sehingga hanya kunci rak senjata tersebut yang terbuka.



Gambar 3 Algoritma Logika Akses

2.3 Skenario Pengujian

Untuk mengevaluasi keandalan operasional prototipe, pengujian sistem dibagi menjadi empat skenario utama. Hasil pada pengujian ini merepresentasikan observasi pada populasi uji dan kondisi lingkungan laboratorium yang digunakan.

Pengujian False Acceptance Rate (FAR): Melibatkan 11 subjek independen yang tidak terdaftar dengan masing-masing melakukan 10 kali percobaan pemindaian (total 110 percobaan). Pengulangan dilakukan dengan sedikit variasi pose (kemiringan sudut kepala) dan jarak. Nilai FAR dihitung menggunakan formula:

$$FAR = \left(\frac{\text{Jumlah Akses Ilegal yang Diterima}}{\text{Total Percobaan Akses Ilegal}} \right) \times 100\%$$

Pengujian False Rejection Rate (FRR): Melibatkan 11 personel terdaftar dengan masing-masing 10 kali pengulangan bervariasi pose untuk mengukur tingkat penolakan sistem terhadap akses yang sah (total 110 percobaan). Nilai FRR dihitung menggunakan formula:

$$FRR = \left(\frac{\text{Jumlah Akses Sah yang Ditolak}}{\text{Total Percobaan Akses Sah}} \right) \times 100\%$$

Pengujian Waktu Respons: Menghitung total waktu (dalam detik) sejak pemindaian wajah, pengiriman data komunikasi, pemrosesan ESP32, hingga aktuator servo bergerak membuka kunci.

Pengujian Kondisional & Spoofing: Menguji validitas pembacaan pada berbagai rentang jarak autentikasi, menguji keberhasilan autentikasi pada tiga kondisi intensitas pencahayaan yang diukur dengan digital lux meter yaitu pagi (67 lux), siang (857 lux), dan malam (0 lux) dengan masing-masing 10 kali pengulangan percobaan pada setiap kondisi pencahayaan (total 30 percobaan), serta menguji serangan manipulasi wajah (photo-based spoofing) sebanyak 20 kali percobaan.

Aspek Etika Penelitian dan Privasi Biometrik: Pelaksanaan pengujian yang melibatkan pengambilan data biometrik wajah dan dokumentasi visual personel telah mengikuti prosedur kepatuhan etika penelitian internal pada Program Studi Teknik Telekomunikasi Militer, Politeknik Angkatan Darat. Seluruh partisipan uji (11 personel terdaftar dan 11 subjek independen tidak terdaftar) telah diberikan penjelasan mengenai tujuan eksperimen dan menandatangani lembar persetujuan partisipan (informed consent), termasuk pemberian izin eksplisit atas publikasi dokumentasi foto pengujian pada Gambar 4 dan Gambar 5. Mengacu pada prinsip perlindungan privasi dan keamanan template biometrik [10], ekstraksi fitur wajah hanya disimpan secara lokal di dalam memori terenkripsi perangkat terminal HIKVISION selama pengujian berlangsung (tidak

diunggah ke server cloud publik), dan seluruh template biometrik partisipan dihapus secara permanen (purged) dari perangkat segera setelah rangkaian eksperimen selesai.

HASIL PENELITIAN

Berdasarkan pengujian sistem servo lock pada 11 rak senjata, evaluasi kinerja diukur menggunakan parameter False Acceptance Rate (FAR), False Rejection Rate (FRR), waktu respons, serta ketahanan terhadap variasi jarak dan cahaya. Hasil pengujian FAR yang melibatkan 11 personel tidak terdaftar independen (masing-masing 10 kali percobaan bervariasi pose, total 110 percobaan) menunjukkan nilai observasi FAR sebesar 0%. Sistem berhasil menolak 100% akses ilegal pada skenario uji ini. Pada pengujian FRR terhadap 11 personel terdaftar dengan kondisi serupa (total 110 percobaan), didapatkan nilai observasi FRR sebesar 0%, di mana sistem mengenali seluruh personel sah tanpa penolakan keliru.



Gambar 4 Indikator Keberhasilan Autentikasi Personel Terdaftar dipublikasikan atas persetujuan partisipan

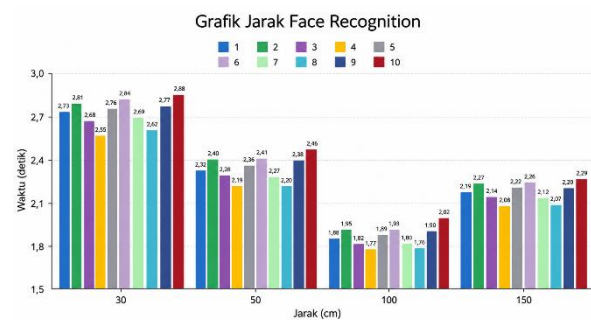
Lebih lanjut, pengujian keamanan terhadap manipulasi visual (photo-based spoofing) dilakukan menggunakan sampel foto cetak berwarna dan tampilan digital dari layar smartphone pada jarak 50 cm. Hasil pengujian (total 20 kali percobaan) menunjukkan bahwa fitur liveness detection bawaan terminal secara konsisten menolak seluruh upaya akses palsu tersebut. Kesimpulan ini mengonfirmasi keamanan sistem spesifik pada skenario photo-based spoofing.



Gambar 5 Pengujian Sistem Menolak Akses Manipulasi Foto (Spoofing) dipublikasikan atas persetujuan partisipan

Pengukuran waktu respons sistem mencatat rata-rata keseluruhan 2,20 detik sejak pemindaian wajah hingga aktuator servo terbuka. Pada pengujian variasi jarak, rentang operasi yang berhasil (successful operating range) berada pada jarak 30 cm hingga 150 cm. Titik dengan waktu respons terbaik dicapai pada jarak 100 cm dengan rata-rata 1,71 detik (rentang 1,68 – 1,74 detik). Sementara itu, pada batas jarak 30 cm

dan 150 cm, waktu respons sedikit meningkat namun tetap memenuhi target operasional maksimal ≤ 3 detik. Delay komunikasi MQTT dan pemrosesan ESP32 tercatat sangat rendah, sehingga durasi terlama dihabiskan oleh proses deteksi liveness kamera dan mekanik servo.



Gambar 6 Grafik Waktu Respon Sistem Terhadap Variasi Jarak

Selain itu, pengujian pada skenario pencahayaan (diukur menggunakan digital lux meter) yang meliputi kondisi pagi (67 lux), siang (857 lux), dan gelap total malam hari (0 lux) dilakukan dengan masing-masing 10 kali pengulangan autentikasi pada setiap kondisi (total 30 percobaan). Hasil pengujian menunjukkan bahwa sistem berhasil melakukan autentikasi sebesar 100% (10 dari 10 percobaan berhasil pada tiap kondisi) berkat dukungan iluminasi inframerah (infrared supplement light) bawaan terminal. Hal ini membuktikan keandalan fungsional terminal dalam beroperasi pada ketiga kondisi pencahayaan yang diuji tersebut, asalkan pengguna berada pada batas jarak operasional yang ditentukan.

PEMBAHASAN

Berdasarkan hasil observasi secara menyeluruh, integrasi face recognition, protokol MQTT, dan ESP32 untuk servo lock rak senjata menunjukkan potensi aplikasi yang baik dalam manajemen kontrol akses logistik militer. Nilai FAR sebesar 0% pada populasi uji mengindikasikan bahwa pembatasan akses sistem mampu beroperasi secara ketat untuk menolak subjek ilegal. Secara paralel, nilai FRR sebesar 0% membuktikan bahwa penerapan keamanan biometrik ini tidak menghambat akses personel yang sah. Tingkat konsistensi ini sejalan dengan standar keandalan pada instrumen smart locker modern berbasis IoT [11].

Selain itu, keberhasilan penolakan sistem terhadap skenario serangan manipulasi visual mengonfirmasi bahwa kemampuan liveness detection bawaan pada terminal HIKVISION dapat diandalkan untuk kasus photo-based spoofing [12]. Pemanfaatan kamera ganda (dual-lens RGB dan inframerah) pada terminal komersial terbukti efektif mendeteksi kedalaman tekstur wajah asli terhadap permukaan planar 2D tanpa membebani komputasi mikrokontroler ESP32, sementara pemisahan regulator daya pada pin VIN ESP32 (7,5 V) dan jalur beban 11 servo (6,5 V) menjaga kestabilan sistem dari kegagalan koneksi selama aktuator bekerja. Kecepatan aktuator dengan rata-rata

waktu respons 2,20 detik merepresentasikan bahwa arsitektur integrasi sistem ini berpotensi meningkatkan efisiensi proses pengambilan senjata, meskipun diperlukan pengujian perbandingan langsung secara statistik dengan waktu pembukaan kunci mekanik konvensional. Kapabilitas adaptasi perangkat yang tetap mampu melakukan autentikasi pada kondisi minim cahaya (0 lux) dan rentang operasi jarak 30–150 cm menegaskan bahwa rancangan arsitektur ini layak dikembangkan lebih lanjut untuk lingkungan gudang senjata militer [13].

PENUTUP

Arsitektur integrasi sistem keamanan rak senjata yang terdiri dari terminal Face Recognition komersial, komunikasi ISAPI–MQTT, mikrokontroler ESP32, dan aktuator servo lock telah berhasil diimplementasikan. Hasil pengujian pada kondisi eksperimental mencatat observasi nilai False Acceptance Rate (FAR) dan False Rejection Rate (FRR) sebesar 0%, serta kapabilitas fitur bawaan sistem dalam menolak manipulasi skenario photo-based spoofing. Waktu respons rata-rata sistem mencapai 2,20 detik dari pemindaian hingga terbukanya kunci mekanik. Sistem juga terbukti mampu menyelesaikan proses autentikasi pada rentang jarak keberhasilan operasional (successful operating range) 30 cm hingga 150 cm dan mencapai tingkat keberhasilan 100% pada tiga kondisi pencahayaan yang

diuji (67 lux, 857 lux, dan 0 lux dengan masing-masing 10 kali pengulangan). Untuk pengembangan penelitian selanjutnya, disarankan melakukan pengukuran baseline perbandingan waktu dengan kunci konvensional secara langsung, serta menambahkan integrasi catu daya cadangan (Uninterruptible Power Supply / UPS) guna mengantisipasi kegagalan operasional saat terjadi pemadaman listrik.

DAFTAR PUSTAKA

- [1] M. Wang and W. Deng, "Deep face recognition: A survey," *Neurocomputing*, vol. 429, pp. 215–244, 2021, doi: 10.1016/j.neucom.2020.10.081.
- [2] Z. Yu, Y. Qin, X. Li, C. Zhao, Z. Lei, and G. Zhao, "Deep Learning for Face Anti-Spoofing: A Survey," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 45, no. 5, pp. 5609–5631, 2023, doi: 10.1109/TPAMI.2022.3215850.
- [3] J. Elkasista *et al.*, "Implementasi Sensor Fingerprint Dan Pengolahan Implementation of Fingerprint Sensor and Facial Image Processing on a Raspberry Pi Based Electric Weapon," vol. 3, pp. 1–10, 2022.
- [4] S. Prayogi, Dekki Widiatmoko, Mokhammad Syafaat, Dedi Pradigdo, Rafi Maulana Alfarizi, and Aguk Sridaryono, "Design of the pistol P1 weapon storage system shelf using fingerprint electronic system in the TNI-AD units," *TEKNOSAINS J. Sains, Teknol. dan Inform.*, vol. 11, no. 2, pp. 238–244, 2024, doi: 10.37373/tekno.v11i2.948.
- [5] M. Babiuch, P. Foltyniek, and P. Smutny, "Using the ESP32 microcontroller for data processing," *Proc. 2019 20th Int. Carpathian Control Conf. ICCC 2019*, 2019, doi: 10.1109/CarpathianCC.2019.8765944.
- [6] S. Hessien *et al.*, "Secrecy Analysis of Generalized Space-Shift Keying Aided Visible Light Communication," *IEEE Access*, vol. 7, no. 2, 2019.
- [7] K. Nandakumar, A. K. Jain, and A. Nagar, "Biometric template security," *EURASIP J. Adv. Signal Process.*, vol. 2008, 2008, doi: 10.1155/2008/579416.
- [8] D. Hercog, T. Lerher, M. Truntič, and O. Težak, "Design and Implementation of ESP32-Based IoT Devices," *Sensors*, vol. 23, no. 15, 2023, doi: 10.3390/s23156739.
- [9] OASIS, "MQTT Version 3.1.1," *OASIS Stand.*, no. October, p. 81, 2014, [Online]. Available: <http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/os/mqtt-v3.1.1-os.html>
- [10] P. Drozdowski, C. Rathgeb, A. Dantcheva, N. Damer, and C. Busch, "Demographic bias in biometrics: A survey on an emerging challenge," *IEEE Trans. Technol. Soc.*, vol. 1, no. 2, pp. 89–103, 2020, doi: 10.1109/TTS.2020.2992344.
- [11] R. Ahmad, A. Wagyaana, and P. D. Junianto, "Perancangan dan Implementasi Sistem Smart Locker dengan Face Recognition Berbasis Internet of Things," *Spektral*, vol. 5, no. 1, pp. 239–245, 2024, doi: 10.32722/spektral.v5i1.7117.
- [12] A. K. Jain, A. Ross, and S. Prabhakar, "An Introduction to Biometric Recognition," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 14, no. 1, pp. 4–20, 2004, doi: 10.1109/TCSVT.2003.818349.
- [13] A. Maier, A. Sharp, and Y. Vagapov, "Comparative analysis and practical implementation of the ESP32 microcontroller module for the internet of things," *2017 Internet Technol. Appl. ITA 2017 - Proc. 7th Int. Conf.*, pp. 143–148, 2017, doi: 10.1109/ITECHA.2017.8101926.