

**SKRIPSI**

**PROTOTYPE SISTEM KEAMANAN AKSES MASUK RUANGAN BERBASIS  
*FINGERPRINT RECOGNITION* MENGGUNAKAN  
*ALGORITMA DEEP LEARNING***



**Disusun Untuk Memenuhi Syarat Mendapatkan Gelar Sarjana Teknik pada  
Jurusan Teknik Elektro Fakultas Teknik  
Universitas Sriwijaya**

**Oleh:**

**MUHAMMAD FATCHAN**

**03041281924029**

**JURUSAN TEKNIK ELEKTRO  
FAKULTAS TEKNIK  
UNIVERSITAS SRIWIJAYA**

**2023**

**LEMBAR PENGESAHAN**  
**PROTOTIPE SISTEM KEAMANAN AKSES MASUK RUANGAN BERBASIS**  
**FINGERPRINT RECOGNITION MENGGUNAKAN**  
**ALGORITMA DEEP LEARNING**



**SKRIPSI**

**Disusun untuk Memenuhi Syarat Mendapatkan Gelar Sarjana Teknik pada**  
**Jurusan Teknik Elektro Fakultas Teknik**

**Universitas Sriwijaya**

**Oleh:**

**MUHAMMAD FATCHAN**

**03041281924029**

**Indralaya, 7 Juli 2023**

**Menyetujui,**  
**Pembimbing Utama**

**Mengetahui,**  
**Dekan Jurusan Teknik Elektro**



**Muhammad Abu Bakar Sidik, S.T., M.Eng., Ph.D**  
**NIP. 197108141999031005**



**Dr. Eng. Ir. Suci Dwijayanti, S.T., M.S., IPM**  
**NIP. 198407302008122001**

## HALAMAN PERNYATAAN INTEGRITAS

Yang bertanda tangan di bawah ini :

Nama : Muhammad Fatchan  
NIM : 03041281924029  
Fakultas : Teknik  
Jurusan Prodi : Teknik Elektro  
Univeristas : Universitas Sriwijaya

Hasil Pengecekan *software iThenticate/Turnitin* : 8%

Menyatakan bahwa tugas akhir saya yang berjudul “Prototipe Sistem Keamanan Akses Masuk Ruangan Berbasis *Fingerprint Recognition* Menggunakan Algoritma *Deep Learning*” merupakan hasil karya sendiri dan benar keasliannya. Apabila ternyata dikemudian hari ditemukan unsur penjiplakan/plagiat dalam karya ilmiah ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya sesuai dengan ketentuan yang berlaku.


Demikian pernyataan ini saya buat dengan sebenarnya dan tanpa paksaan.

Palembang, 7 Juli 2023



Muhammad Fatchan  
NIM. 03041281924029

Saya sebagai Pembimbing dengan ini menyatakan bahwa saya telah membaca dan menyetujui skripsi ini dan dalam pandangan saya ruang lingkup dan kualitas skripsi ini mencukupi sebagai skripsi mahasiswa sarjana strata satu (S1).

Tanda Tangan :  \_\_\_\_\_

Pembimbing Utama : Dr. Eng. Ir. Suci Dwijayanti, S.T., M.S., IPM

Tanggal : 7 / Juli / 2023

**PERYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK  
KEPENTINGAN AKADEMIS**

Sebagai civitas akademik Universitas Sriwijaya, saya yang bertanda tangan di bawah ini:

Nama : Muhammad Fatchan

NIM : 03041281924029

Jurusan/Prodi : Teknik Elektro

Fakultas : Teknik

Jenis Karya : Skripsi

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Sriwijaya **Hak Bebas Royalti Noneksklusif (*Non-exclusive Royalty-Free Right*)** atas karya ilmiah saya yang berjudul:

**PROTOTYPE SISTEM KEAMANAN AKSES MASUK RUANGAN BERBASIS  
FINGERPRINT RECOGNITION MENGGUNAKAN ALGORITMA DEEP  
LEARNING**

beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Noneksklusif ini Universitas Sriwijaya berhak menyimpan, mengalih media /formatkan, mengelola dalam bentuk pangkalan data (database), merawat, dan mempublikasikan tulisan saya tanpa meminta izin dari saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta. Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di Palembang

Pada tanggal : 7 Juli 2023

Yang menyatakan



Muhammad Fatchan

NIM. 03041281924029

## KATA PENGANTAR

Segala puji dan syukur penulis ke hadirat Allah SWT, yang telah melimpahkan segala rahmat dan karunia-Nya sehingga Laporan Tugas Akhir (skripsi) ini dapat diselesaikan dengan baik dan tepat waktu. Laporan ini disusun untuk memenuhi syarat mendapatkan gelar Sarjana Teknik pada Jurusan Teknik Elektro Fakultas Teknik Universitas Sriwijaya, juga sebagian bentuk pertanggungjawaban penulis terhadap penelitian dalam rangka Tugas Akhir yang dilakukan sebelumnya. Laporan Tugas Akhir (skripsi) ini merupakan laporan tertulis hasil penelitian dalam pengimplementasian *convolutional neural network* (cnn) sebagai prototipe sistem keamanan berbasis sidik jari pada Laboratorium Teknik Kendali Robotika. Secara garis besar laporan ini disusun menjadi lima bab, yaitu bab pendahuluan, bab tinjauan pustaka, bab metode penelitian, bab hasil dan pembahasan, serta bab kesimpulan dan saran.

Dalam penyusunan Laporan Tugas Akhir (skripsi) maupun selama pelaksanaan penelitian di lapangan, penulis banyak mendapatkan bantuan dan dukungan dari berbagai pihak, oleh karena itu penulis menyampaikan ucapan terima kasih kepada:

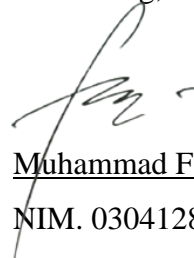
1. **Bapak Muhammad Abu Bakar Sidik, S.T., M.Eng., Ph.D., IPU.** Selaku Ketua Jurusan Teknik Elektro Fakultas Teknik Universitas Sriwijaya.
2. **Ibu Hera Hikmarika, S.T., M.Eng.** Selaku dosen Pembimbing Akademik yang selalu memberi dukungan dan semangat tak henti-hentinya.
3. **Ibu Dr. Eng. Ir. Suci Dwijayanti, S.T., M.S., IPM.** Selaku Dosen Pembimbing Tugas Akhir, atas kesediaannya membimbing, mengajarkan, dan megarahkan penulis selama penelitian dan penyusunan Laporan Tugas Akhir ini.
4. Kedua orang tua **Papa Mama (H. Akhirun dan Hj. Eta), Kakak Saya Madania S.T., Kakak Ipar Ari Yudha Baskoro S.T.,** serta seluruh keluarga besar yang telah banyak mendoakan dan selalu memberikan dukungan tak ternilai baik secara moriil maupun materiil sehingga bisa menyelesaikan perkuliahan ini dengan baik dan tepat waktu, saya ucapakan terima kasih yang sebesar-besarnya.

5. **Seluruh dosen di lingkungan Teknik Elektro Universitas Sriwijaya**, yang selama empat tahun membekali penulis dengan ilmu yang bermanfaat.
6. **Kak Selamat, Kak Ryan, Kak Rusman, Bu Diah** selaku Staf Adm Jurusan Teknik Elektro Universitas Sriwijaya, yang telah banyak membantu selama ini.
7. **Muhammad Irsyad Razan, Roni Wijaya, Alya Apriani, Rahman Hafidzin, Muhammad Deni Fajri, M. Azmi Tegar Putra Nova**, dan semua teman-teman Teknik Elektro yang namanya tidak bisa saya sebutkan satu persatu terkhusus angkatan 2019 yang telah memberikan bantuan selama penyusunan Laporan Tugas Akhir ini.
8. **Kak Rendika Perlyanza S. Kom.** selaku guru saya selama pengerjaan Laporan Tugas Akhir ini.
9. **Semua mahasiswa/i Teknik Elektro angkatan 2022** yang rela menjadi responden dalam penelitian agar Laporan Tugas Akhir ini dapat diselesaikan.
10. Semua pihak yang tidak dapat disebutkan satu persatu, penulis ucapkan terima kasih.

Ibarat pepatah “tak ada gading yang tak retak”, penulis menyadari bahwa masih banyak kekurangan didalam penyusunan Laporan Tugas Akhir ini, oleh karena itu kritik dan saran yang konstruktif dari bapak/ibu dosen serta teman-teman sekalian sangatlah diharapkan sebagai masukan dikemudian hari.

Akhir kata semoga Laporan Tugas Akhir ini dapat memberikan manfaat positif bagi peningkatan ilmu pengetahuan dan berguna bagi semua kalangan yang membutuhkan khususnya mahasiswa/I Teknik Elektro Universitas Sriwijaya.

Palembang, Juni 2023



Muhammad Fatchan

NIM. 03041281924029

**ABSTRAK**  
**PROTOTIPE SISTEM KEAMANAN AKSES MASUK RUANGAN**  
**BERBASIS *FINGERPRINT RECOGNITION* MENGGUNAKAN**  
**ALGORITMA *DEEP LEARNING***

(Muhammad Fatchan, 03041281924029, 2023, 61 halaman)

Kata sandi merupakan sistem keamanan tertua yang masih dipakai hingga sekarang. Namun, sistem keamanan tersebut rentan terhadap serangan *cyber* terutama *brute force*. Sistem keamanan biometrik merupakan salah satu solusi untuk meningkatkan sistem keamanan saat ini. Sidik jari merupakan salah satu biometrik yang sering digunakan pada saat ini. Pada penelitian ini, sistem pengenalan sidik jari diimplementasikan dalam bentuk prototipe dengan pengenalan menggunakan arsitektur *deep learning* dari *convolutional neural network* (CNN). Hasil pelatihan menunjukkan ResNet50 tidak mengalami *overfitting* secara signifikan daripada dua arsitektur lainnya dengan *loss value* 0,9935 dan akurasi 100%. Pada pengujian offline menggunakan data test pada ResNet50 pada variabel “terbuka atas nama yang bersangkutan” mendapatkan nilai 95,58% sedangkan pada EfficientNetV2M dan VGG16 mendapatkan nilai 93,13% dan 86,76%. Sehingga pada prototipe digunakan ResNet50 sebagai sistem pengenalan sidik jari. Namun, pada pengujian *online* ResNet50 masih belum mampu menggeneralisasi data baru terutama pada kondisi sidik jari rusak.

**Kata Kunci:** **Pengenalan Sidik Jari, *Deep Learning*, Sistem Keamanan, *Convolutional Neural Network* (CNN)**

Indralaya, 24 Juni 2023

Menyetujui,

Pembimbing Utama

Dr. Eng. Ir. Suci Dwijayanti, S.T., M.S., IPM

NIP. 198407302008122001



Mengetahui,

Ketua Jurusan Teknik Elektro

Muhammad Abu Bakar Sidik., S.T., M.Eng., Ph.D

NIP.197108141999031005



**ABSTRACT**  
**PROTOTYPE OF ROOM ENTRY SECURITY SYSTEM BASED**  
**FINGERPRINT RECOGNITION USING DEEP LEARNING**  
**ALGORITHM**

(Muhammad Fatchan, 03041281924029, 2023, 61 pages)

---

The password is the oldest security system that is still used today. However, the security system is vulnerable to cyber attacks, especially brute force. The biometric security system is one of the solutions to improve the current security system. Fingerprints are one of the most frequently used biometrics today. In this study, the fingerprint recognition system is implemented in the form of a prototype with recognition using deep learning architecture from convolutional neural network (CNN). The training results show that ResNet50 does not experience significant overfitting compared to the other two architectures with loss value 0,9935% and accuracy 100%. Offline testing uses test data on ResNet50 with variable "open for the right person" getting a value of 95.58% while EfficientNetV2M and VGG16 get a value of 93.13% and 86.76%. So that the prototype used ResNet50 as a fingerprint recognition system. However, online testing on ResNet50 still not able to generalize new data especially in the condition of damaged fingerprints..

**Keywords: Fingerprint Recognition, Deep Learning, Security System, Convolutional Neural Network (CNN)**


Indralaya, 24 Juni 2023

Menyetujui,  
Pembimbing Utama

Mengetahui,  
Ketua Jurusan Teknik Elektro



**Muhammad Abu Bakar Sidik., S.T., M.Eng., Ph.D**  
NIP.197108141999031005



**Dr. Eng. Ir. Suci Dwijayanti, S.T., M.S., IPM**  
NIP. 198407302008122001

## DAFTAR ISI

<b>LEMBAR PENGESAHAN.....</b>	<b>i</b>
<b>HALAMAN PERNYATAAN INTEGRITAS.....</b>	<b>ii</b>
<b>PERYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS.....</b>	<b>iv</b>
<b>KATA PENGANTAR.....</b>	<b>v</b>
<b>ABSTRAK.....</b>	<b>vii</b>
<b>ABSTRACT.....</b>	<b>viii</b>
<b>DAFTAR ISI.....</b>	<b>ix</b>
<b>DAFTAR GAMBAR.....</b>	<b>xii</b>
<b>DAFTAR TABEL.....</b>	<b>xiv</b>
<b>DAFTAR RUMUS.....</b>	<b>xv</b>
<b>DAFTAR LAMPIRAN.....</b>	<b>xvi</b>
<b>BAB I PENDAHULUAN.....</b>	<b>1</b>
1.1 Latar Belakang.....	1
1.2 Perumusan Masalah.....	3
1.3 Tujuan Penelitian.....	3
1.4 Batasan Masalah.....	3
1.5 Keaslian Penelitian.....	4
<b>BAB II TINJAUAN PUSTAKA.....</b>	<b>7</b>
2.1 <i>State of The Art</i> .....	6
2.2 Teori Pendukung.....	12
2.2.1 <i>Fingerprint Recognition</i> .....	11
2.2.2 Identifikasi Sidik Jari.....	13
2.2.3 Pencocokan Sidik Jari.....	14
2.2.4 <i>Convolutional Neural Network (CNN)</i> .....	15
<b>BAB III METODE PENELITIAN.....</b>	<b>21</b>
3.1 Studi Literatur.....	22
3.2 Perancangan Prototype Security System Akses Ruang.....	22
3.2.1 <i>Fingerprint Reader ZKTECO ZK9500</i> .....	23

3.2.2	<i>Kit Intel® NUC 11 Performance - NUC11PAHi7</i> .....	24
3.2.3	Board Arduino UNO R3 ATmega328 ATmega16U2.....	25
3.2.4	<i>Solenoid</i> .....	26
3.2.5	LCD 16x2 i2C IIC Module Solder Uno R3.....	26
3.3	Perancangan Sistem Akses Ruangan.....	27
3.3.1	Perancangan Sistem Pengenalan.....	27
3.3.2	Implementasi Sistem Keamanan Ruangan.....	29
3.4	Evaluasi.....	30
3.4.1	Pengujian Sistem Pengenal Sidik Jari.....	30
3.4.2	Pengujian Sistem Keamanan Berbasis Sidik Jari.....	31
<b>BAB IV HASIL DAN PEMBAHASAN</b> .....		32
4.1	Pengambilan Data.....	32
4.2	Proses Pengolahan Data.....	34
4.2.1	Pembagian Data.....	34
4.2.2	Augmentasi Data.....	35
4.2.3	<i>Resize</i> .....	36
4.3	Proses Pelatihan Data.....	36
4.3.1	Pelatihan Data Menggunakan ResNet50.....	37
4.3.2	Pelatihan Data Menggunakan EfficientNetV2M.....	39
4.3.3	Pelatihan Data Menggunakan VGG16.....	42
4.3.4	Analisis Ketiga Arsitekur.....	43
4.4	Pengujian Pengenalan Sidik Jari.....	46
4.4.1	Pengujian <i>Offline</i> Pada ResNet50.....	46
4.4.2	Pengujian <i>Offline</i> Pada EfficientNetV2M.....	47
4.4.3	Pengujian <i>Offline</i> Pada VGG16.....	49
4.5	Implementasi Pada Prototipe.....	50
4.5.1	Penghubungan Seluruh Komponen Utama Prototipe.....	50
4.5.2	Pemasangan Solenoid Pada Arduino UNO.....	54
4.5.3	Pemasangan LCD 16x2 i2C Module Solder Pada Arduino UNO.....	54
4.5.4	Hasil Seluruh Pemasangan Rangkaian Prototipe.....	55

4.7	Pengujian <i>Real</i> Pada Prototipe.....	57
4.7.1	Pengujian <i>Delay</i> Pada Prototipe.....	57
4.7.2	Pengujian <i>Online</i> Pada Prototipe.....	58
<b>BAB V KESIMPULAN DAN SARAN.....</b>		<b>60</b>
5.1	Kesimpulan.....	60
5.2	Saran.....	60
<b>DAFTAR PUSTAKA.....</b>		<b>62</b>
<b>LAMPIRAN.....</b>		

## DAFTAR GAMBAR

Gambar 2.1.	a-d Kurva ROC untuk percobaan pertama, kedua, ketiga, dan empat.....	7
Gambar 2.2	(a) Rata-rata tingkat kecocokan dan FRR (b) Hasil FRR menurut perubahan kriteria.....	10
Gambar 2.3	Bentuk pola dari <i>minutiae</i> sidik jari.....	13
Gambar 2.4	Jenis-jenis bentuk sidik jari.....	13
Gambar 2.5	Ilustrasi arsitektur CNN.....	15
Gambar 2.6	Ilustrasi operasi <i>convolution</i> .....	17
Gambar 2.7	Ilustrasi operasi <i>convolution</i> dalam 3D.....	18
Gambar 2.8	<i>Pooling layer</i> .....	18
Gambar 3.1	<i>Flowchart</i> penelitian.....	21
Gambar 3.2	Perancangan <i>prototype security system</i> akses ruangan.....	22
Gambar 3.3	Fingerprint reader ZKTECO ZK9500.....	23
Gambar 3.4	Mini PC.....	24
Gambar 3.5	Arduino UNO RE Atmega328 Atmega16U2.....	25
Gambar 3.6	Solenoid.....	26
Gambar 3.7	LCD 16x2 I2C.....	26
Gambar 3.8	Perancangan sistem akses ruangan.....	27
Gambar 3.9	<i>Flowchart</i> sistem akses masuk ruangan.....	28
Gambar 3.10	Implementasi sistem keamanan ruangan.....	29
Gambar 4.1	Proses pengambilan data sidik jari.....	33
Gambar 4.2	Posisi pengambilan data sidik jari.....	33
Gambar 4.3	(a) Sidik jari Anisa Dinda Septianan (b) Sidik jari Fery Hasan (c) Sidik jari Nadila Devita Ariani.....	33
Gambar 4.4	Hasil Augmentasi Data.....	35
Gambar 4.5	Hasil dari <i>preprocessing resize</i> sidik jari.....	36
Gambar 4.6	(a) Grafik akurasi pelatihan dan validasi (b) Grafik loss pelatihan dan validasi.....	39
Gambar 4.7	(a) Grafik akurasi pelatihan dan validasi (b) Grafik loss pelatihan dan validasi.....	41

Gambar 4.8	(a) Grafik akurasi pelatihan dan validasi (b) Grafik loss pelatihan dan validasi.....	43
Gambar 4.9	Hasil pelatihan tiga arsitektur pengenalan sidik jari.....	44
Gambar 4.10	Hasil <i>loss</i> pelatihan tiga arsitektur pengenalan sidik jari.....	44
Gambar 4.11	Hasil validasi tiga arsitektur pengenalan sidik jari.....	44
Gambar 4.12	Hasil <i>loss</i> validasi tiga arsitektur pengenalan sidik jari.....	44
Gambar 4.13	Komponen utama prototipe.....	50
Gambar 4.14	Contoh hasil UI demo dari bahasa C#.....	51
Gambar 4.15	odingan untuk memanggil file <i>testing deep learning</i> pada Microsoft Visual Studio.....	52
Gambar 4.16	Kodingan penghubung arduino uno.....	52
Gambar 4.17	(a) Penyesuaian alamat pada Microsoft Visual Studio, (b) Penyesuaian alamat pada Arduino IDE.....	53
Gambar 4.18	Hasil <i>custom</i> UI.....	53
Gambar 4.19	Perancangan solenoid.....	54
Gambar 4.20	Perancangan LCD 16x2 i2C.....	55
Gambar 4.20	Panel box prototipe.....	56
Gambar 4.21	Rangkaian kabel prototipe dalam ruangan.....	56
Gambar 4.22	Pengujian <i>real</i> pada prototipe.....	56
Gambar 4.23	Pengujian <i>online</i> pada prototipe.....	57
Gambar 4.24	(a) Sidik jari Muhammad Fatchan dari pengujian <i>online</i> (b) Sidik jari Mohammad Wahyu Anugrah Pratama dari data pelatihan.....	59

## DAFTAR TABEL

Tabel 2.1	Performa pengenalan percobaan keempat.....	8
Tabel 2.2	Hasil klasifikasi <i>dataset</i> NIST-DB4.....	9
Tabel 2.3	Hasil pengujian kecocokan sidik jari dengan berbagai kondisi.	11
Tabel 2.4	Hasil percobaan pada Samsung Galaxy S3 dengan tambahan pembaca sidik jari.....	12
Tabel 2.5	Hasil percobaan pada Samsung S5.....	12
Tabel 3.1	Spesifikasi fingerprint reader ZKTECO ZK9500.....	23
Tabel 3.2	Arduino UNO R3 Atmega328 Atmega16U2.....	25
Tabel 3.3	<i>Confusion matrix</i> .....	30
Tabel 4.1	Empat sampel dari pendataan kondisi sidik jari responden....	34
Tabel 4.2	Parameter augmentasi data.....	35
Tabel 4.3	Versi modul untuk pelatihan.....	37
Tabel 4.4	<i>Full connection</i> arsitektur ResNet50.....	38
Tabel 4.5	Parameter <i>training</i> ResNet50.....	38
Tabel 4.6	<i>Full Connection</i> Arsitektur EfficientNetV2M.....	40
Tabel 4.7	Parameter <i>training</i> EfficientNetV2M.....	41
Tabel 4.8	<i>Full Connection</i> Arsitektur VGG16.....	42
Tabel 4.9	Parameter <i>training</i> VGG16.....	42
Tabel 4.10	Pengujian <i>offline</i> sepuluh sampel menggunakan arsitektur ResNet50.....	47
Tabel 4.11	Pengujian <i>offline</i> sepuluh sampel menggunakan arsitektur EfficientNetV2M.....	48
Tabel 4.12	Pengujian <i>offline</i> sepuluh sampel menggunakan arsitektur VGG16.....	49
Tabel 4.13	Pengujian <i>delay</i> pada prototipe.....	57

## DAFTAR RUMUS

Rumus 2.1	Rumus <i>feature map</i> .....	16
Rumus 2.2	Rumus operasi konvolusi.....	17
Rumus 2.3	Rumus aktivasi ReLU.....	17
Rumus 2.4	Rumus <i>hidden layer</i> .....	19
Rumus 2.5	Rumus <i>output layer</i> .....	19
Rumus 2.6	Rumus fungsi <i>softmax</i> .....	20
Rumus 3.1	<i>Confusion matrix</i> .....	30



## DAFTAR LAMPIRAN

- Lampiran 1** Pendataan Kondisi Sidik Jari Dari Seluruh Responden
- Lampiran 2** Hasil Pengujian *Offline* ResNet50
- Lampiran 3** Hasil Pengujian *Offline* EfficientNetV2M
- Lampiran 4** Hasil Pengujian *Offline* VGG16
- Lampiran 5** Hasil Pelatihan ResNet50
- Lampiran 6** Hasil Pelatihan EfficientNetV2M
- Lampiran 7** Hasil Pelatihan VGG16
- Lampiran 8** Hasil Pengujian *Online* ResNet50
- Lampiran 9** Hasil Pengujian *Online* EfficientNetV2M
- Lampiran 10** Hasil Pengujian *Online* VGG16
- Lampiran 11** Program Pelatihan Arsitektur ResNet50
- Lampiran 12** Program Pelatihan Arsitektur EfficientNetV2M
- Lampiran 13** Program Pelatihan Arsitektur VGG16
- Lampiran 14** Program Testing Deep Learning
- Lampiran 15** Program User Interface menggunakan Microsoft Visual Studio
- Lampiran 16** Program Generate Data
- Lampiran 17** Program Pada Arduino

# BAB I

## PENDAHULUAN

### 1.1. Latar Belakang

Sistem keamanan terus berkembang dari waktu ke waktu. Salah satu sistem keamanan tertua yang sering digunakan hingga sekarang adalah sistem keamanan berbasis kata sandi [1]. Akan tetapi, sistem keamanan ini rentan terhadap serangan *cyber*, seperti teknik *brute force* yang merupakan salah satu metode peretas untuk mencari kata sandi pada suatu sistem. Menurut *Data Breach Investigation Report* (DBIR) tahun 2022, serangan *cyber* seperti *credentials*, *phishing*, *exploiting vulnerabilities* dan *ransomware* meningkat 13% dalam lima tahun terakhir. Serangan tersebut berusaha mencari celah agar dapat mengakses suatu sistem dengan mencari kata sandi sebagai sarannya sehingga dapat digunakan untuk meretas sistem tersebut [2]. Sehingga, solusi untuk meningkatkan sistem keamanan mereka dengan otentikasi menggunakan komponen biometrik.

Biometrik merupakan salah satu teknologi yang semakin sering digunakan sebagai pengenal pribadi otomatis berdasarkan karakteristik fisiologis dan perilaku. Kata biometrik berasal dari bahasa Yunani *bios* (hidup) dan *metrikos* (mengukur). Penggunaan biometrik sama seperti *password* atau *ID Card* yang hanya dimiliki oleh pengguna itu sendiri [3]. Salah satu teknologi biometrik yang telah berkembang dan semakin banyak digunakan di berbagai bidang kehidupan sehari-hari adalah *fingerprint recognition*. Penggunaan *fingerprint* ini telah digunakan pada *E-commerce*, pembayaran *online*, dan kontrol akses suatu sistem [4]. Teknologi *fingerprint recognition* lebih baik digunakan terutama untuk sistem keamanan yang tinggi dibandingkan dengan teknologi pengenal identitas berbasis biometrik lainnya seperti *face recognition*, *iris*, dan *voice recognition*.

Beberapa penelitian terdahulu telah dilakukan untuk mengenali sidik jari. Fanfeng Zeng, dkk [4] melakukan penelitian yang bertujuan mencari metode otentikasi yang kuat dan efektif pada citra meskipun salah satu informasi citra hilang. Metode yang digunakan adalah *residual network* untuk meningkatkan akurasi dari arsitektur *convolution neural network* (CNN). Namun, penelitian

tersebut hanya membuktikan bahwa algoritma yang dirancang lebih baik daripada algoritma pengenalan sidik jari parsial yang ada serta, belum ada implementasi lanjut untuk digunakan dalam bidang sistem keamanan. Selanjutnya, Mohammad Hafidz Hersyah, dkk [5] membuat sistem keamanan pintu pada laboratorium berbasis mikrokontroler Atmega328. Akan tetapi, sistem keamanan yang digunakan bergantung pada kecocokan data sidik jari yang direkam pada mikrokontroler dan tidak ada metode khusus untuk mengenali sidik jari yang terbaca. Pada penelitian lain, Michal Szczepanik, dkk [6] melakukan penelitian mengenali sidik jari yang digunakan pada perangkat seluler untuk membuka kunci atau mengonfirmasi tindakan pengguna. Penelitian dilakukan dengan menggunakan algoritma yang sering digunakan pada ponsel seluler seperti *minutiae adjacency graph* (MAG), *elastic minutiae matching* (EMM), dan lain-lain. Algoritma tersebut diuji pada dua perangkat seluler beserta dengan algoritma yang diusulkan. Akan tetapi, penelitian tersebut menunjukkan kekurangan pada salah satu *device* yang digunakan karena sistem pengenalan yang dimiliki *device* tersebut tidak dapat melakukan pengenalan sidik jari pada sidik jari dengan kondisi yang rusak. Kemudian penelitian yang dilakukan oleh Seungdo Jeong [7] mendesain pintu akses masuk ruangan dengan menggunakan kata sandi dan diikuti dengan pengenalan sidik jari yang bertujuan untuk mengurangi tingkat kriminal disana. Untuk pengenalan sidik jari digunakan algoritma *convolutional neural network* (CCN) dari *dataset Sokoto Coventry Fingerprint* (SOCOFing) yang berisi 6000 gambar sidik jari. Meskipun, nilai pengenalan sidik jari yang didapatkan berhasil mendapatkan nilai diatas 90% akan tetapi belum ada implementasi terkait desain tersebut. Bahkan tidak ada informasi apakah pengambilan data sidik jari menggunakan *webcam* yang dibatasi oleh tempered glass atau akrilik dapat dilakukan.

Pada penelitian-penelitian sebelumnya, masih belum banyak yang menggunakan sidik jari sebagai sistem keamanan untuk mengakses ruangan [4][6]. Selain itu, penelitian-penelitian tersebut hanya menggunakan data sekunder dan belum diimplementasikan sebagai alat sistem keamanan [4][7]. Sehingga, pada penelitian ini akan dikembangkan suatu *prototype security system* untuk membuka pintu masuk menggunakan sidik jari secara *real-time*. *Prototype* ini sendiri nantinya akan digunakan sebagai alat sistem keamanan di Laboratorium Sistem Kendali

sebagai sistem keamanan. Pengenalan sidik jari pada *prototype* ini menggunakan algoritma *deep learning* dari CNN untuk meningkatkan kualitas dalam pengenalan sidik jari dan terbukanya pintu masuk secara *real-time*. Algoritma ini telah menunjukkan performa yang baik dalam mengenali sidik jari [4].

## **1.2. Perumusan Masalah**

Sistem keamanan pengenalan sidik jari berbasis *deep learning* masih sebatas desain dan pengujian algoritma menggunakan data primer maupun data sekunder. Sistem keamanan pengenalan sidik jari yang sering dijumpai masih menggunakan algoritma sederhana yang bergantung pada kecocokan data sidik jari yang direkam pada *database*. Hal tersebut membuat sistem sulit mengenali sidik jari yang mengalami perubahan kondisi seperti lembab ataupun mengalami kerusakan akibat aktivitas harian. Maka, pada penelitian ini dikembangkan sebuah prototipe sistem keamanan berbasis sidik jari menggunakan algoritma *deep learning*. Sistem ini nantinya akan digunakan sebagai *security system* agar suatu individu dapat mengakses ruangan.

## **1.3. Tujuan Penelitian**

Adapun tujuan dilakukannya penelitian ini adalah menerapkan sistem pengenalan sidik jari menggunakan algoritma *deep learning* sebagai sistem keamanan akses masuk ruangan berupa prototipe. Penelitian ini juga bertujuan untuk menunjukkan performa dari algoritma *deep learning* dalam mengenali data sidik jari baru yang akan di pasang pada prototipe yang akan dibuat.

## **1.4. Batasan Masalah**

Adapun batasan masalah pada penelitian ini meliputi:

1. Sampel data sidik jari yang digunakan merupakan sidik jari para dosen teknik elektro, pegawai/staff jurusan, asisten laboratorium, dan para praktikan yang menggunakan Laboratorium Teknik Kendali dan Robotika.

2. Sampel data sidik jari diambil dari setiap responden dengan jumlah 22 gambar sidik jari. Yang terdiri dari sebelas gambar salah satu sidik jari tangan kanan dan sebelas gambar salah satu sidik jari tangan kiri. Setiap sidik jari akan diambil satu sample gambar sidik jari untuk dijadikan data test pada pengujian *offline*.
3. Program sistem pengenalan yang akan digunakan pada prototipe merupakan salah satu dari tiga arsitektur *deep learning* dari CNN, yaitu ResNet50, VGG16, dan EfficientNetV2M yang dipilih berdasarkan hasil pelatihan dan pengujian *offline* menggunakan data test.
4. Lokasi penelitian hanya sebatas di Laboratorium Teknik Kendali dan Robotika.

### 1.5. Keaslian Penelitian

Ada beberapa penelitian-penelitian sebelumnya yang telah dilakukan berkaitan dari *design smart door lock* maupun metode *fingerprint recognition*. Seungdo Jeong dalam penelitiannya mendesain *digital door lock* dengan menggunakan kata sandi dan sidik jari untuk dapat membuka pintu [7]. Setelah kata sandi yang dimasukkan benar, maka pengguna harus diperiksa sidik jarinya sesuai atau tidak. Pemeriksaan sidik jari dilakukan dengan menempelkannya pada kaca transparan yang akan didata menggunakan kamera. Dalam proses pengenalannya digunakan algoritma *convolutional neural network* (CCN) dari *dataset Sokoto Coventry Fingerprint* (SOCOFing). Penelitian tersebut menggunakan 100 sidik jari yang berbeda sebagai *dataset* uji yang kemudian dilakukan perbandingan gambar sidik jari asli dari setiap jari sebanyak 1000 kali dengan beberapa kondisi yang mungkin akan terjadi dilapangan. Nilai rata-rata akurasi yang didapatkan sebesar 95.93% dan nilai kesalahan dalam pengenalan sebesar 5.52%.

Pada penelitian yang dilakukan Mohammad Hafidz Hersyah, dkk dibuat *prototype* sistem keamanan berupa *smart door lock* menggunakan mikrokontroler [5]. Pintu akan terbuka pada saat pengenalan sidik jari dan kata sandi dari *keypad* yang dimasukkan benar. Data diinput menggunakan sensor fingerprint dan disimpan dalam bentuk *database* pada mikrokontroler. Namun, data sidik jari yang

tersimpan langsung berupa data ID untuk membedakan sidik jari yang teridentifikasi. Hal tersebut membuat proses pengenalan sidik jari kurang maksimal. Hasil uji coba data pengenalan pun hanya dilakukan sebanyak sepuluh kali dan tingkat keberhasilan sistem mengenal sidik jari langsung turun sebanyak 40% saat kondisi sidik jari yang diinput lembab.

Fanfeng Zeng, dkk melakukan penelitian pengenalan sidik jari berbasis algoritma CNN dan dilanjutkan dengan ResNet [4]. Dataset yang digunakan adalah *dataset* sidik jari parsial NCUT-FR dengan total citra sidik jari akhir sebanyak 5070 dan *dataset* publik NIST-DB4 yang berisi 2000 pasang gambar sidik jari. Pada dataset NCUT-FR dilakukan empat percobaan dengan hasil percobaan pertama didapatkan *false rejection rate* (FRR) sebesar 3.6% saat *false acceptance rate* (FAR) 0%. Pada percobaan kedua, FAR bernilai 0.0154% saat hasil FRR 20%, percobaan ketiga dengan FRR 12.3%, dan percobaan keempat dengan hasil FRR 0.036%. Sementara untuk NIST-DB4 dibagi menjadi dua subset dengan nama NIST-DB4-S dan NIST-DB4-F. Hasil nilai akurasi yang didapatkan dari NIST-DB4-S sebesar 93% dan NIST-DB4-F sebesar 91.80%.

Selanjutnya, Michal Szczepanik, dkk melakukan penelitian pengenalan sidik jari pada perangkat seluler yang memiliki kondisi perubahan struktur tidak normal akibat kerusakan [6]. Penelitian dilakukan dengan membandingkan algoritma yang ada dengan algoritma mereka. Algoritma tersebut terdiri dari *minutiae adjacency graph* (MAG), *elastic minutiae matching* (EMM), *pattern-based templates algorithm* (PBTA), *minutia group matching* (MGM), dan *minutia group matching selective attention phase* (MGMSA). Algoritma-algoritma tersebut diuji pada dua perangkat yaitu Samsung Galaxy S3 dengan tambahan *fingerprint reader* dan Samsung S5. Data yang digunakan berupa 12 sidik jari yang berbeda dan memiliki 10 sampel. Tetapi sistem pengenalan sidik jari yang sudah dimiliki Samsung S5 sendiri (*embedded*) tidak dapat melakukan pengenalan pada sidik jari dengan FRR 8.10%.

Dari penelitian-penelitian diatas, maka pada penelitian ini akan dibuat *prototype security system* berupa *smart door lock* berbasis *fingerprint recognition* yang menggunakan algoritma *deep learning* dari CNN. Salah satu algoritma itu

adalah ResNet yang memiliki tingkat akurasi yang baik karena memiliki *residual block* yang berfungsi untuk mencegah *vanishing gradient problem* yang mengakibatkan nilai *gradient* menjadi kecil.

## DAFTAR PUSTAKA

- [1] N. Riaz, A. Riaz, and S. A. Khan, "Biometric template security: an overview," *Sens. Rev.*, vol. 38, no. 1, pp. 120–127, Jan. 2018, [Online]. Available: <https://www.emerald.com/insight/content/doi/10.1108/SR-07-2017-0131/full/html>. [Accessed Jan.12, 2023].
- [2] D. Breach and I. Report, "DBIR 2022 Data Breach Investigations Report Small Business snapshot," 2022.
- [3] Anil K. Jain, Salil Prabhakar, Sharath Pankanti, "Biometric Recognition: Security and Privacy Concerns," *Michigan State Univ.*, pp. 33–42, 2003.
- [4] F. Zeng, S. Hu, and K. Xiao, "Research on partial fingerprint recognition algorithm based on deep learning," *Neural Comput. Appl.*, vol. 31, no. 9, pp. 4789–4798, 2019.
- [5] M. H. Hersyah, D. Yolanda, and H. Sitohang, "Multiple laboratory authentication system design using fingerprints sensor and keypad based on microcontroller," in *2020 International Conference on Information Technology Systems and Innovation, ICITSI 2020 - Proceedings*, pp. 14–19, 2020.
- [6] M. Szczepanik, J. J. Ireneusz, and T. Jamka, "Security Lock System for Mobile Devices Based on Fingerprint Recognition Algorithm," *Information Systems Architecture and Technology: Proceedings of 36<sup>th</sup> International Conference on Information System Architecture and Technology-ISAT 2015-Part III*, pp. 25–35, 2016.
- [7] S. Jeong, "Design on Novel Door Lock Using Minimizing Physical Exposure and Fingerprint Recognition Technology," *Int. J. Informatics Vis.*, vol. 6, no. 1, pp. 103–108, 2022.
- [8] A. Riyadi, D. Handoko, A. S. Nugroho, M. Gunawan, and J. M. H. T. No, "Pengembangan Antarmuka Grais Automated Fingerprint Identification System Berbasis Open Source," *Seminar Nasional Teknologi Infromasi.*, 2010.
- [9] A. Zafrullah, "Mengenal Minutiae pada sidik jari," *ugm.ac.id*, 2017. [Online]. Available: <https://zafmti15.web.ugm.ac.id/fingerprint/mengenal-minutiae-pada-sidik-jari/>. [Accessed Jan. 13, 2023].
- [10] Lourde, Mary, and Dushyant Khosla. "Fingerprint identification in biometric security systems." *International Journal of Computer and Electrical Engineering 2.*, no. 5, p.852, 2010.
- [11] S. R. Suartika E. P, I Wayan, Wijaya Arya Yudhi, "Klasifikasi Citra Menggunakan Convolutional Neural Network (Cnn) Pada Caltech 101," *J. Tek. ITS*, vol. 5, no. 1, p. 76, 2016.
- [12] E. A. Oktaviari, "Bab II Landasan Teori," *J. Chem. Inf. Model.*, vol. 53, no.



- 9, p. 1689, 2019, [Online]. Available: <https://repository.bsi.ac.id/index.php/unduh/item/257726/File-10-BAB-II.pdf>. [Accessed Jan. 13, 2023].
- [13] Hibatullah, Alwan. "Penerapan Metode Convolutional Neural Network Pada Pengenalan Pola Citra Sandi Rumpot." *Diss. Universitas Komputer Indonesia.*, 2019.
- [14] Trivusi, "Pengertian dan Cara Kerja Algoritma Convolutional Neural Network (CNN)," *Trivusi*, 2022. [Online]. Available: <https://www.trivusi.web.id/2022/04/algoritma-cnn.html>. [Accessed Jan. 13, 2023].
- [15] Rim, Beanbonyka, Junseob Kim, and Min Hong. "Fingerprint classification using deep learning approach." *Multimedia Tools and Applications* 80., pp 35809-35825, 2021.
- [16] Huang, Mei-Ling, and Yu-Chieh Liao. "Stacking Ensemble and ECA-EfficientNetV2 Convolutional Neural Networks on Classification of Multiple Chest Diseases Including COVID-19." *Academic Radiology.*, 2022.