Terakreditasi SINTA Peringkat 2
Surat Keputusan Dirjen Pendidikan Tinggi, Riset dan Teknologi No. 158/E/KPT/2021
masa berlaku mulai Vol. 5 No. 2 tahun 2021 s.d Vol. 10 No.1 tahun 2026

Terbit online pada laman web jurnal: **http://jurnal.iaii.or.id**

JURNAL RESTI
(Rekayasa Sistem dan Teknologi Informasi)
Vol. 5 No. 6 (2021) 1099 – 1105 ISSN Media Elektronik: 2580-0760

Implementasi Metode *Unsupervised Learning* Pada Sistem Keamanan Dengan Optimalisasi Penyimpanan Kamera IP

Desta Yolanda[1], Mohammad Hafiz Hersyah[2], Eno Marozi[3]
[1,2,3] Jurusan Teknik Komputer, Fakultas Teknologi Informasi, Universitas Andalas
[1]destayola@it.unand.ac.id, [2]mhafiz@it.unand.ac.id, [3]marozieno0@gmail.com

Abstract

Security monitoring systems using face recognition can be applied to CCTV or IP cameras. This is intended to improve the security system and make it easier for users to track criminals is theft. The experiment was carried out by detecting human faces for 24 hours using different cameras, namely an HD camera that was active during the day and a Night Vision camera that was active at night. The application of Unsupervised Learning method with the concept of an image cluster, aims to distinguish the faces of known or unknown people according to the dataset built in the Raspberry Pi 4. The user interface media of this system is a web-based application built with Python Flask and Python MySQL. This application can be accessed using the domain provided by the IP Forwarding device which can be accessed anywhere. According to the test results on optimization of storage, the system is able to save files only when a face is detected with an average file size of ± 2.28 MB for 1x24 hours of streaming. So that this storage process becomes more efficient and economical compared to the storage process for CCTV or IP cameras in general.

Keywords: Face Recognition, Unsupervised Learning, IP Camera, Datasets, IP Forwarding

Abstrak

Sistem monitoring keamanan menggunakan face recognition dapat diterapkan pada CCTV atau Kamera IP. Hal ini ditujukan untuk meningkatan sistem keamanan dan mempermudah pengguna juga dalam melacak pelaku aksi kriminal pencurian. Percobaan dilakukan dengan mendeteksi wajah manusia selama 24 jam menggunakan kamera yang berbeda, yaitu kamera HD yang aktif pada siang hari dan kamera Night Vision yang aktif pada malam hari. Penerapan metode Unsupervised Learning dengan konsep image cluster bertujuan untuk membedakan wajah orang yang dikenal atau tidak dikenal sesuai dataset yang dibangun dalam Raspberry Pi 4. Media antarmuka pengguna dari sistem ini berupa aplikasi berbasis web yang dibangun dengan Python Flask dan Python MySQL. Aplikasi ini dapat diakses menggunakan domain yang disediakan oleh perangkat IP Forwarding yang dapat diakses di mana saja. Berdasarkan hasil pengujian pada optimalisasi penyimpanan storage, sistem mampu menyimpan file hanya ketika ada wajah terdeteksi dengan rata-rata ukuran file ± 2,28 MB selama 1x24 jam streaming. Sehingga proses penyimpanan ini menjadi lebih efiisen dan ekonomis dibandingkan dengan proses penyimpanan CCTV atau kamera IP pada umumnya.

Kata kunci: Face Recognition, Unsupervised Learning, Kamera IP, Dataset, IP Forwarding

1. Pendahuluan

Kasus pencurian pada sekarang ini sangatlah banyak, dan pada umunya dari beberapa kasus pencurian tersebut kebanyakan kasus yang tidak teridentifikasi atau tidak diketahui siapa pelaku dari pencurian tersebut. Hal ini dikarenakan banyaknya masyarakat yang tidak mempedulikan faktor keamanan pada linkungan sekitar rumah yang tidak aman dan tidak diawasi. Ada beberapa hal yang memicu terjadinya pencurian baik itu yang terjadi langsung di dalam atau di luar rumah, contohnya yang di dalam rumah yaitu letak aset berharga kita yang mudah dijangkau oleh pencuri dan juga karena aset tersebut tidak disimpan pada penyimpanan yang tidak aman, seperti tempat penyimpanan yang tidak dikunci atau tidak tertutup. Kemudian untuk di luar rumah terkait pengawasan di perkarangan rumah yang cenderung pemilik rumah tersebut mengabaikan keadaan luar rumah dan jarang terpantau oleh pemilik rumah sehingga dapat memberikan kesempatan bagi pelaku pencurian ini untuk beraksi seperti pencurian sepeda motor, helm dan lainnya.

Diterima Redaksi: 11-10-2021 | Selesai Revisi: 22-12-2021 | Diterbitkan Online: 30-12-2021

CCTV (*Close Circuit Television*) merupakan alat perekaman yang menggunakan satu atau lebih kamera video yang nantinya akan menghasilkan data video maupun audio [1] . CCTV ini juga merupakan kamera video digital yang digunakan untuk mengirim sinyal gambar dari suatu ruangan atau penyiaran yang nantinya tertuju kepada ruang lingkup tertentu dan dapat dipantau melalui perangkat monitor [2]. Sehingga CCTV ini cukup banyak digunakan sebagai alat pengawasan suatu objek pada lingkungan rumah ataupun ruangan yang memiliki aset penting dan berharga. Namun masih banyak keterbatasan dan kekurangan dari kamera CCTV yang pada umumnya seperti tidak dapat mengenali atau mendeteksi siapa saja orang yang sudah masuk atau keluar rumah, tidak bisa mengenali wajah pemilik rumah, dan sangat boros akan media penyimpanan karena CCTV selalu menyimpan setiap detik dari rekamannya ke media penyimpanan. Oleh karena itu, penggunanya pun sangat malas melihat hasil dari tangkapan CCTV-nya sehari-hari karena terlalu lamanya rekaman CCTV. Kemudian CCTV juga bisa diakses secara publik yang memungkinkan penggunanya bisa memantaunya dari manapun. Dari hal tersebut banyak juga orang lain bahkan juga pencuri yang dapat mengakses CCTV tersebut dan mengetahui dengan mudah bagaimana keamanan dirumah dari sisi mana saja yang tidak terpantau oleh CCTV. Oleh Karena itu perlu adanya penambahan fitur pengaksesan CCTV publik tersebut menjadi *private*. Selain itu, pemantauan kamera yang kurang maksimal seperti tidak bisa mengeluarkan peringatan dalam aksi yang mencurigakan sesuai jam yang sudah ditentukan.

Sebelumnya telah terdapat beberapa penelitian terkait tentang CCTV dan Kamera IP baik itu menggunakan deteksi wajah ataupun tidak. Penelitian pertama yaitu dari Huang Zhiwu dkk [3] yang menerapkan pengenalan wajah dengan 3 skenario yaitu V2S, S2V dan V2V. Penelitian ini bertujuan untuk membandingkan proses pengenalan wajah berbasis video yang berbeda guna sebagai basis data tolak ukur yang baik untuk evaluasi. Penelitian kedua yaitu dari Sofyan Almer dkk [4] yang menerapkan IP Kamera sebagai sistem pemantauan keamanan dengan metode *deblurring* untuk mengantisipasi gambar yang rusak akibat oleh adanya gerakan (blur). Penelitian ketiga juga ada dilakukan oleh R.Venkatesan dkk [5] yang mengembangkan sistem pengawasan *autonomous video surveillance* yang bertujuan untuk melacak objek bergerak dilingkungan sekitar kamera IP. Pada pnelitian in sistem divalidasi untuk mengidentifikasi kendaraan pengguna yang di autentikasi yang dilengkapi dengan stiker unik serta nomor registrasi kendaraan. Pada penelitian keempat yaitu dari Cletus O. Ohaneme [6] mengimplementasikan sistem keamanan pengawasan berbasis *Internet Protocol* (IP). Pada penelitian ini menggabungkan tampilan jarak jauh dan penyimpanan video secara *real time* melalui kamera dan dipantau menggunakan *Personal Computer* (PC). Terakhir pada penelitian Hubarat D. Patriko dkk [7] membangun aplikasi *human tracking* dengan GPS (*Global Position System*) untuk mendapatkan posisi pengguna secara *real time* pada area terbuka. Pada penelitian ini menggunakan RFID untuk melakukan pelacakan pada area tertutup dan Kamera IP sebagai bagian dari sistem yang akan mengirim gambar visualisasi didalam ruangan. Hasil dari penelitian-penelitian tersebut masih memiliki keterbatasan dalam hal pendeteksian dan pengenalan wajah yang dapat izinkan dan tidak diizinkan. Selain itu, pada sistem tersebut belum terdapat proses optimalisasi mediapenyimpanan sebagai parameter yang harus dipertimbangkan dalam membangun sistem keamanan yang lebih ekonomis dan efisien.

Pada publikasi ini dibangun sistem kemanan fisik yang juga merupakan kamera CCTV atau spesifiknya Kamera IP untuk pengawasan yang hemat akan media penyimpanan dan deteksi wajah untuk mengetahui siapa saja orang yang sudah keluar masuk rumah menggunakan metode *unsupervised machine learning* atau pembelajaran tanpa pengawasan. Algoritma *unsupervised learning* adalah salah satu tipe algoritma *machine learning* yang digunakan untuk menarik kesimpulan dari *dataset*. Metode ini hanya akan mempelajari suatu data berdasarkan kedekatannya saja atau yang biasa disebut dengan *clustering* [8]. Pada proses pengenalan wajah menggunakan *image cluster* untuk membedakan wajah orang yang dikenal atau tidak dikenal. *Image cluster* merupakan konsep dari *unsupervised machine learning* yaitu merupakan teknik mengumpulkan wajah yang akan di-*cluster* untuk membedakan gambar satu dengan gambar lainnya [9]. Fitur CCTV juga dapat diakses sesuai cakupan *public* dan WAN (*Wide Area Network*) secara *private* menggunakan IP *Static* yang alamatnya tidak berubah-ubah atau bersifat tetap melalui *webserver* [10].

IP Forwarding adalah metode untuk meneruskan paket (*tunneling*) data dari sebuah jaringan ke jaringan lain walaupun berbeda kelas jaringannya, sehingga kedua *host* tersebut dapat berkomunikasi [11]. *IP forwarding* biasanya diaplikasikan di sebuah perangkat keras router baik itu *manage* atau *unmanage* [11]. Dengan memanfaatkan fitur *Port Forwarding* ini pada router rumahan dapat memberikan notifikasi ke pengguna jika ada orang tidak dikenali terdeteksi oleh Kamera IP melalui Telegram.

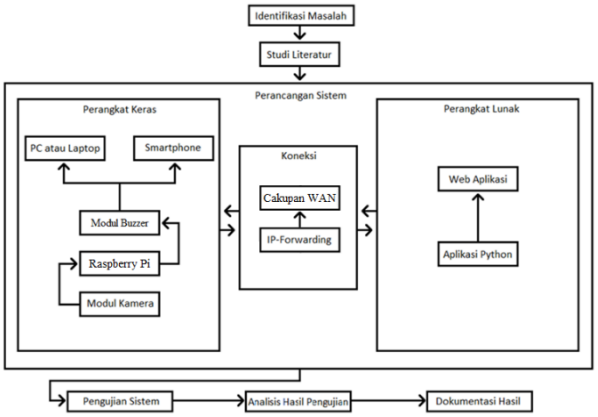
2. Metode Penelitian

Pada publikasi ini menggunakan metode penelitian eksperimental (*experimental research*). Penelitian eksperimental ini menggunakan percobaan yang dirancang secara khusus untuk membangkitkan data yang diperlukan guna menjawab pertanyaan dari penelitian [12]. Penelitian ini dilakukan dengan menghubungkan komponen dan alat-alat yang berbeda

DOI: https://doi.org/10.29207/resti.v5i6.3552

karakteristik. Komponen dan alat-alat tersebut antara lain adalah kamera IP, Raspberry Pi dan Smartphone. Kemudian komponen-komponen tersebut akan diuji apakah masukan yang diberikan sesuai dengan keluaran yang diinginkan.

Rancangan penelitian berisi tahapan yang akan dilakukan selama penelitian, dimulai dari identifikasi masalah, studi literatur, perancangan perangkat keras, perancangan perangkat lunak, implementasi, pengujian, analisis, hingga dokumentasi penelitian. Tahapan lebih rinci dalam penelitian ini dapat dilihat pada gambar 1 dibawah.



Gambar 1. Diagram Rancangan Penelitian

2.1. Rancangan Sistem

Secara umum rancangan sistem yang dibangun dalam publikasi ini dijelaskan dari gambar 2.

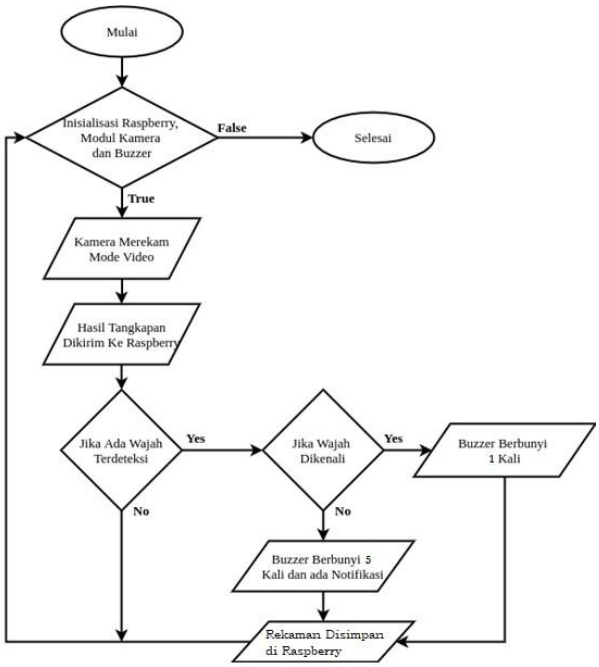
Berdasarkan gambar 2, CCTV ini terdapat komponen perangkat keras yang terdiri dari Modul Kamera sebagai pengambil citra dan Raspberry Pi sebagai komputer dan wadah pemroses citra yang diambil dan Buzzer sebagai keluaran sistem.

Gambar 2. Rancangan Umum Sistem

2.2. Rancangan Proses

Pada perancangan proses ini dilakukan dengan menspesifikasikan fungsionalitas sistem. Secara sistematis, alur fungsi sistem secara umum dapat dilihat pada Gambar 3.

Berdasarkan Gambar 3, alur program yang berjalan pada perangkat lunak mikrokontroler dimulai dengan inisialisasi Raspberry Pi, Modul Kamera dan Buzzer. Jika bernilai *False* maka Program selesai. Selanjutnya, hasil tangkapan dikirim ke Raspberry Pi. Jika ada wajah terdeteksi dan wajah tersebut dikenali maka Buzzer akan berbunyi sebanyak 1 kali. Jika wajah tidak dikenali maka Buzzer akan berbunyi sebanyak 5 kali, dan mengirim notifikasi ke pemilik Kamera IP melalui Telegram. Kemudian hasil rekaman disimpan ketika hanya wajah yang terdeteksi.



Gambar 3. *Flowchart* Proses Sistem

Kemudian untuk tahapan pemrosesan citra dapat dilihat pada gambar 4.

Berdasarkan gambar 4, alur dari pemrosesan citra dimulai dengan tangkapan kamera dalam mendeteksi wajah pada *frame* atau rekaman. Kemudian kamera memperbesar cakupannya (*Zoom in*) pada deteksi wajah. Selanjutnya pada pendeteksian area wajah akan terjadi proses pemotongan gambar dan warna pada gambar diganti ke *mode grayscale*.

Lalu untuk tahapan dari metode *Unsupervised Machine learning* yang ditanamkan pada sistem tertanam ini dapat dilihat pada gambar 5.

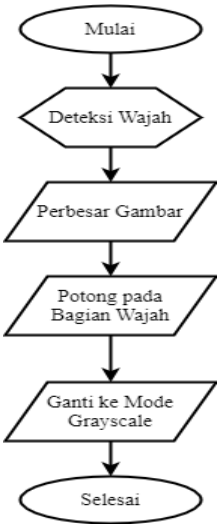
Berdasarkan gambar 5, terlihat bahwa alur dari metode *unsupervised learning* ini dimulai dengan melakukan inisialisasi data input dan kamera. Selanjutnya pencetakan data input dan wajah yang terdeteksi oleh kamera. Jika *Encoding* data input sama dengan wajah artinya wajah tersebut dikenali dan dilabeli dengan nama sesuai basis data. Jika tidak sesuai maka wajah akan dilabeli dengan orang tidak dikenali.

2.3. Rancangan Basis Data

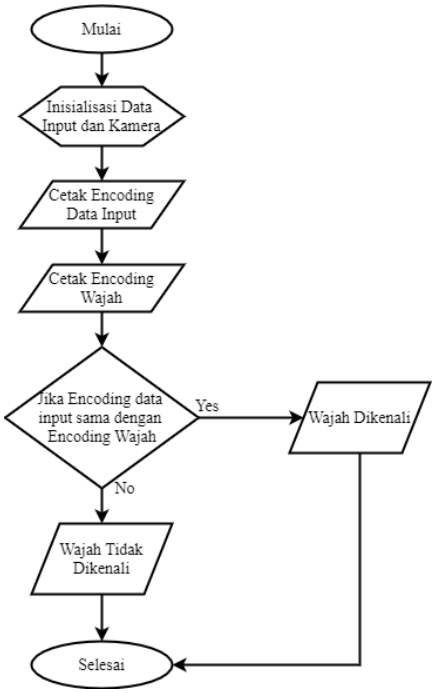
Perangkat lunak yang dibangun bertujuan untuk mengolah data yang disimpan kedalam basis data. Data yang disimpan berupa data untuk login pengguna dan

DOI: https://doi.org/10.29207/resti.v5i6.3552

data input. Rancangan pada *database* MySQL dapat dilihat dari tabel 1 dan 2.



Gambar 4. Flowchart Pemrosesan Citra



Gambar 5. Flowchart *Unsupervised Learning*

Tabel 1. Tabel Login Pengguna

No	Field	Type	Lenght	Null
1	Username	Varchar	10	No
2	Password	Varchar	10	No

Tabel 2. Tabel Inforrmasi Data Input

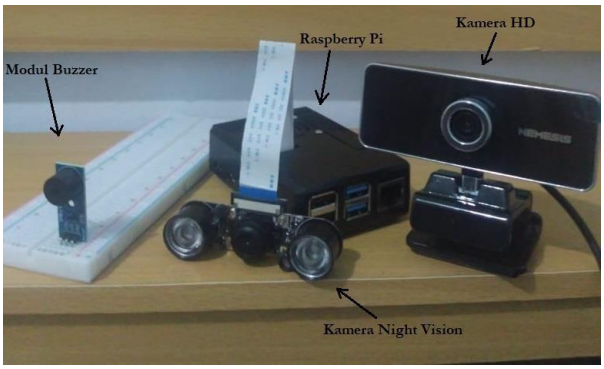
No	Field	Type	Lenght	Null
1	Nama	Varchar	15	No
2	Terakhir Terlihat	Timestamp	-	No
3	Info	Varchar	30	Yes

3. Hasil dan Pembahasan

Pada implementasi kamera IP sebagai pendeteksi wajah dengan metode *Unsupervised Learning* ini menggabungkan implementasi dari perangkat lunak dan perangkat keras secara keseluruhan untuk memenuhi seluruh fungsi dari alat.

3.1. Implementasi Perangkat Keras

Pada perangkat keras akan dilakukan implementasi berupa Modul kamera Night Vision, Modul Kamera HD dan Buzzer.



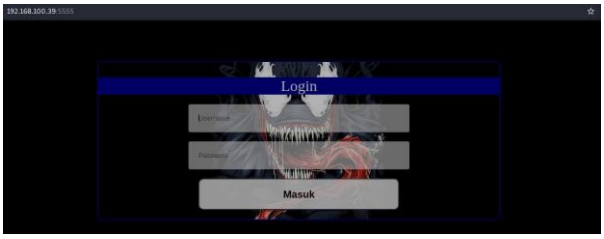
Gambar 6. Perangkat Sistem Monitoring

Berdasarkan gambar 6, komponen dari perangat keras yang digunakan pada sistem monitoring keamanan ini meliputi :

a) Raspberry Pi untuk mendapatkan waktu pemrosesan yang singkat dalam menjalankan program hingga mendapatkan hasil klasifikasi
b) Modul kamera Night Vision sebagai pendeteksi wajah dengan bantuan Library pada malam hari
c) Modul Kamera HD Sebagai pendeteksi wajah dengan bantuan Library pada siang hari
d) Modul Buzzer Passive Memberi notifikasi ke pengguna apakah objek tersebut dikenal atau tidak dikenal.

3.2 Implementasi Perangkat Lunak

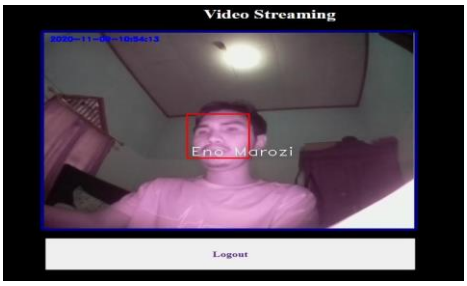
Berikut beberapa halaman sebagai antarmuka pengguna dengan sistem monitoring keamanan ini.



Gambar 7. Tampilan Antarmuka Halaman Utama

Pada gambar 7 ini merupakan halaman utama web atau berupa halaman login form untuk proses autentifikasi pengguna ke halaman kamera. Dimana untuk proses autentifikasi memerlukan *username* dan password yang telah tersimpan pada *database* MySQL.

DOI: https://doi.org/10.29207/resti.v5i6.3552



Gambar 8. Tampilan Antarmuka Halaman Kamera

Pada gambar 8 ini merupakan halaman kamera setelah proses autentifikasi berhasil. Halaman kamera ini berfungsi untuk menampilkan rekaman dan juga sekaligus melakukan pendeteksian wajah dan mengirim notifikasi melalui Telegram.

```
MariaDB [face_recognition]> select * from admin_login;
+----------+----------+
| username | password |
+----------+----------+
| admin    | password |
+----------+----------+
1 row in set (0.001 sec)

MariaDB [face_recognition]> select * from info_detection;
+------------+---------------------+-----------+
| Nama       | time                | info      |
+------------+---------------------+-----------+
| Eno Marozi | 2020-10-08 22:31:50 | Admin     |
| Edi Marion | 2020-10-08 22:36:08 | Orang tua |
| Rosmiyati  | 2020-10-08 22:37:15 | Orang tua |
| Taufik A   | 2020-10-08 22:37:58 | Teman     |
| Roni Fadli | 2020-10-08 22:34:36 | Teman     |
+------------+---------------------+-----------+
5 rows in set (0.001 sec)
```

Gambar 9. Tampilan Tabel pada *Database* MySQL

Dari gambar 9 ini merupakan semua informasi basis data untuk autentifikasi pengguna dan informasi dari setiap deteksi pengguna yang dikenal oleh sistem.

3.3 Hasil Pengujian Pendeteksian Wajah

Pada pengujian ini dilakukan pendeteksian wajah ketika memakai masker, kupluk dan tanpa memakai masker dan kupluk. Hasil pengujian ini dapat dilihat pada Tabel 3.

Berdasarkant Tabel 3 dapat dilihat bahwa wajah dapat terdeteksi ketika tanpa memakai masker atau kupluk dan saat memakai masker, karena pada saat memakai kupluk algoritma *facial recognition* tidak dapat memprediksi pola dari bentuk wajah atau fitur vektornya yang membuat wajah tidak dapat terdeteksi.

3.4 Hasil Pengujian Sistem

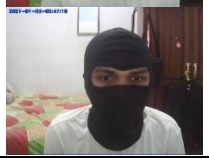
Pada pengujian keseluruhan sistem ini dilakukan pendeteksian wajah dikenali atau tidak dikenali sistem dan sekaligus melabeli target dengan nama yang terdapat pada basis data MySQL. Kemudian sistem memberikan notifikasi ke Telegram dan alarm pada modul buzzer. Buzzer akan berbunyi sebanyak 5 (lima) kali jika terdeteksi wajah tidak dikenali dan berbunyi 1 (satu) kali jika terdeteksi wajah yang dikenali oleh sistem. Semua hasil rekaman disimpan ke media penyimpanan. Hasil pengujian sistem dapat dilihat pada tabel 4.

Berdasarkan tabel 4 ini diperoleh rata – rata waktu proses yang dibutuhkan sistem yaitu 2.15 detik. Hal ini dipengaruhi dari performansi Raspberry Pi dalam mendeteksi jumlah wajah yang tertangkap oleh kamera IP. Kemudian berdasarkan percobaan dengan kamera IP yang digunakan pada siang hari dan malam hari diperoleh hasil bahwa kamera IP sangat baik mendeteksi pada siang hari (dapat lebih dari 5 meter) dan kurang baik pada malam hari (kurang dari 1 meter).

3.5 Hasil Pengujian Media Penyimpanan

Pada pengujian ini dilakukan pemantauan selama kurun waktu 1x24 jam dengan kamera IP untuk memastikan berapa memori atau kapasitas yang digunakan dalam media penyimpanan. Pengujian ini dilakukan selama 5 (lima) hari. Hasil pengujian dapat dilihat pada Tabel 5.

Tabel 3. Hasil Pengujian Deteksi Wajah

No	Kondisi	Gambar	Hasil
1	Tanpa Memakai Masker dan Kupluk		Wajah Terdeteksi
2	Memakai Masker		Wajah Terdeteksi
3	Memakai Kupluk		Wajah Tidak Terdeteksi

DOI: https://doi.org/10.29207/resti.v5i6.3552

Tabel 4. Pengujian Sistem Monitoring Keamanan

No	Gambar	Wajah	Waktu Proses (detik)	Jarak Tangkap (meter)	Notifiksi Buzzer dan Telegram	Status Penyimpanan
1		Dikenali	2.25	4.2	Suara 1 kali dan Tidak ada Notifikasi	Rekaman Disimpan
2		Tidak Dikenali	0.52	0.5	Suara 5 kali dan Ada Notifikasi Telegram	Rekaman Disimpan
3		Dikenali	2.10	3.3	Suara 1 kali dan Tidak ada Notifikasi	Rekaman Disimpan
4		Tidak Dikenali	3.50	5.5	Suara 5 kali dan Ada Notifikasi Telegram	Rekaman Disimpan
5		Dikenali	2.10	3.5	Suara 1 kali dan Tidak ada Notifikasi	Rekaman Disimpan
6		Tidak Dikenali	1.81	2.3	Suara 5 kali dan Ada Notifikasi Telegram	Rekaman Disimpan
7		Dikenali	1.92	4.1	Suara 1 kali dan Tidak ada Notifikasi	Rekaman Disimpan
8		Tidak Dikenali	3.51	2.2	Suara 5 kali dan Ada Notifikasi Telegram	Rekaman Disimpan
9		Dikenali	2.0	3.6	Suara 1 kali dan Tidak ada Notifikasi	Rekaman Disimpan

DOI: https://doi.org/10.29207/resti.v5i6.3552

10		Tidak Dikenali	1.82	4.5	Suara 5 kali dan Ada Notifikasi Telegram	Rekaman Disimpan

Tabel 5. Hasil Pengujian Media Penyimpanan

No	Percobaan	Siang	Malam	Ukuran File
1	Percobaan Hari Ke-1	06.00 AM s/d 18.00 PM	18.01 PM s/d 05.59 AM	3.7 MB
2	Percobaan Hari Ke-2	06.00 AM s/d 18.00 PM	18.01 PM s/d 05.59 AM	5.1 MB
3	Percobaan Hari Ke-3	06.00 AM s/d 18.00 PM	18.01 PM s/d 05.59 AM	1.41 MB
4	Percobaan Hari Ke-4	06.00 AM s/d 18.00 PM	18.01 PM s/d 05.59 AM	0.5 MB
5	Percobaan Hari Ke-5	06.00 AM s/d 18.00 PM	18.01 PM s/d 05.59 AM	0.7 MB
	Rata- rata			2.28 MB

Dari Tabel 5 dapat dilihat bahwa rata-rata ukuran file yang tersimpan hanya sebesar 2,28 MB selama *streaming* 24 jam. Penyimpanan hanya dilakukan ketika ada wajah terdeteksi. Jika menyimpan seluruh *streaming* atau semua *frame* maka ukuran file menjadi 331 MB. Hal ini menunjukkan bahwa penyimpanan file hanya dilakukan ketika kondisi ada wajah terdeteksi dapat menghemat 99% media penyimpanan. Akan tetapi sebenarnya kapasitas tersebut tergantung dari banyaknya pengguna atau wajah yang terdeteksi oleh sistem dan disimpan ke media penyimpanan.

4. Kesimpulan

Berdasarkan hasil pengujian dan analisa yang dilakukan menghasilkan bahwa sistem dapat membedakan wajah orang yang dikenali dan orang yang tidak dikenali dengan metode *unsupervised machine learning* dalam pendeteksian wajah dengan konsep *image cluster*. Rata-rata waktu yang dibutuhkan sistem dalam pengolahan citra wajah hingga menghasilkan keluaran pada antarmuka pengguna yaitu sebesar ± 2,15 detik. Dari segi optimalisasi media penyimpanan pada kamera IP, sistem ini juga dapat menghemat media penyimpanan dengan rata-rata ukuran file saat disimpan sebesar ± 2,28 MB selama streaming 24 Jam. Hal ini menunjukan bahwa melakukan penyimpanan file hanya ketika kondisi wajah terdeteksi saja dapat menghemat 99% media penyimpanan. Sehingga, secara umum, dapat dikatakan sistem yang dibangun ini dapat bekerja dengan baik dan sesuai dengan hasil yang diharapkan.

Ucapan Terimakasih

Kajian ini merupakan bagian dari Program Dekan untuk mendukung Program Penelitian Prioritas Produktif Dosen Fakultas Teknologi Informasi Universitas Andalas Padang Sumatera Barat, Indonesia.

Daftar Rujukan

[1] Atmoko, E. H. (2012). Membuat Sendiri CCTV Berkelas Enterprise Dengan Biaya Murah. In *Yogyakarta: ANDI* (1st ed.). Andi Publisher.

[2] Azikin, A. (2005). Kamera Pengawas Berbasis Open Source. In *Elex Media Komputindo: Jakarta*.

[3] Huang, Z., Shan, S., Wang, R., Zhang, H., Lao, S., Kuerban, A., & Chen, X. (2015). A Benchmark and Comparative Study of Video-Based Face Recognition on COX Face Database. *IEEE Transactions on Image Processing*, *24*(12), 5967–5981. https://doi.org/10.1109/TIP.2015.2493448

[4] Sofyan, A., Wisaksono Sudiharto, D., & Wirawan Wijiutomo, C. (2018). Surveillance Embedded IP Camera with Integrated Cloud Storage and Image Deblurring Using Richardson-Lucy. *2018 International Seminar on Application for Technology of Information and Communication*, 388–393. https://doi.org/10.1109/ISEMANTIC.2018.8549775

[5] Venkatesan, R., Raja, P. D. A., & Ganesh, A. B. (2016). Unsupervised Learning Based Video Surveillance System Established with Networked Cameras. In *Advances in Signal Processing and Intelligent Recognition Systems* (pp. 603–614). Springer. https://doi.org/10.1007/978-3-319-28658-7_51

[6] Ohaneme, C. O., Eke, J., Azubogu, A. C. O., Ifeagwu, E. N., & Ohaneme, L. C. (2012). Design and Implementation of an IP-based Security Surveillance System. *International Journal of Computer Science Issues (IJCSI)*, *9*(5), 391.

[7] Hutabarat, D. P., Patria, D., Budijono, S., & Saleh, R. (2016). Human tracking application in a certain closed area using RFID sensors and IP camera. *2016 3rd International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE)*, 11–16. https://doi.org/10.1109/ICITACEE.2016.7892401

[8] Rezkia, S. M. (2020). *Kenali Algoritma Machine Learning* (Annissa Widya Davita (ed.); 14th ed.). DQLab.

[9] Noor, M. H., & Hariadi, M. (2009). Image Cluster Berdasarkan Warna untuk Identifikasi Kematangan Buah Tomat dengan Metode Valley Tracing. *Seminar Nasional Informatika (SEMNASIF)*, *1*(1).

[10] Space and Naval Warfare Systems Center Atlantic. (2013). *CCTV Technology Handbook*. U.S. Department of Homeland Security.

[11] Roughan, M., Griffin, T., Mao, M., Greenberg, A., & Freeman, B. (2004). Combining routing and traffic data for detection of IP forwarding anomalies. *ACM SIGMETRICS Performance Evaluation Review*, *32*(1), 416–417. https://doi.org/10.1145/1012888.1005745

[12] Ratminingsih, N. M. (2010). Penelitian Eksperimental dalam Pembelajaran Bahasa Kedua. *Prasi: Jurnal Bahasa, Seni, Dan Pengajarannya*, *6*(11), 31–40. https://doi.org/0.23887/prasi.v6i11.6816.g4

DOI: https://doi.org/10.29207/resti.v5i6.3552