Implementasi Metode Local Binary Pattern Histogram Dan Facial Landmark Pada Keamanan Akses Login

Implementation of Local Binary Pattern Histogram and Facial Landmark Methods in Login Access Security

Frindi Mangimbulude*[1], Pinrolinvic D.K. Manembu[2], Feisy Diane Kambey[3]
[1,2] Program Studi Teknik Informatika, Universitas Sam Ratulangi, Manado, [3] Program Studi Teknik Elektro, Universitas Sam Ratulangi, Manado
e-mail: *[1]**18021106090@student.unsrat.ac.id**, [2]pmanembu@unsrat.ac.id, [3]feisykambey@unsrat.ac.id

Abstrak

Teknologi pengenalan wajah banyak digunakan sebagai sebagai salah teknologi untuk melakukan autentifikasi seseorang. Namun pada beberapa perangkat belum memiliki komponen pengenalan wajah yang mampu mengenali orang asli yang sudah dikenali atau hanya foto saja karena hanya menyematkan sistem pengenalan wajah 2D terutama pada perangkat dengan perangkat lawas atau perangkat berspesifikasi rendah, Maka pada penelitian ini dibuatlah sistem login dengan pengenalan wajah dan pendeteksi kedipan mata. Sistem yang dibangun mampu beroperasi dengan baik pada perangkat yang sudah lama atau perangkat berspesifikasi rendah menggunakan metode pengenalan wajah yaitu Local Binary Pattern Histogram (LBPH) dan metode pendeteksi kedipan mata Facial Landmark dari library dlib. Pada perangkat lawas atau berspesifikasi rendah sistem dapat mengenali wajah dengan baik pada jarak maksimal 150cm, sistem dapat mendeteksi kedipan mata dengan minimal lama waktu berkedip 0,5 detik pada jarak 20cm sampai 120 cm, waktu yang dibutuhkan untuk pengambilan citra acuan rata-rata adalah 57 detik, waktu untuk melatih model rata-rata adalah 3,7 detik, akurasi pengenalan wajah 85%, dan waktu untuk melakukan proses login rata-rata adalah 6,7 detik. Dari hasil tersebut, terlihat bahwa sistem dapat beroperasi dengan baik. Berdasarkan hasil percobaan yang telah dilakukan, dapat ditarik kesimpulan bahwa metode yang digunakan untuk mengenalih wajah dan mendeteksi kedipan mata berhasil diimplementasikan.

***Kata Kunci**:* Deteksi Wajah; Pengenalan Wajah; Pendeteksi kedipan wajah, LBPH, Facial Landmark

Abstract

Facial recognition technology is widely used as one of the authentication technologies to identify a person. However, some devices do not have facial recognition components that can recognize the genuine person already known or only a photo because they only embed 2D facial recognition systems, especially on older or low-spec devices. Therefore, this research created a login system using facial recognition and blink detection. The system was built to work well on older or low-spec devices using the Local Binary Pattern Histogram (LBPH) facial recognition method and the blink detection method Facial Landmark from the dlib library. On older or low-spec devices, the system can recognize faces well at a maximum distance of 150cm, detect blinks with a minimum blink time of 0.5 seconds at a distance of 20cm to 120cm, the time required to capture reference images is an average of 57 seconds, the time to train the model is an average of 3.7 seconds, the facial recognition accuracy is 85%, and the time to complete the login process is an average of 6.7 seconds. From these results, it can be seen that the system can work well.

Based on the experimental results, it can be concluded that the methods used for facial recognition and blink detection have been successfully implemented.

Keywords: Face Detection; Face Recognition; Facial blink detection, LBPH, Facial Landmark

1. PENDAHULUAN

Menjaga keamanan menjadi hal yang paling penting dalam melindungi data, benda, atau rahasia seseorang [1], Oleh karena itu, terdapat banyak metode autentikasi atau validasi yang tersedia untuk menentukan apakah seseorang dapat mengakses data, benda, atau rahasia yang memiliki keamanan. [2]. Keamanan sebuah akun juga sangat penting[3]. Biasanya, untuk mengamankan sebuah akun, diberikan username dan password kepada pengguna, atau menggunakan keamanan biometik seperti pengenalan wajah untuk menakses atau menmanfaatkan akun tersebut. Username adalah kombinasi unik dari beberapa huruf yang digunakan sebagai identitas pengguna. [4], Password digunakan sebagai lapisan keamanan yang dibuat untuk melindungi profil atau data pribadi pengguna dari akses yang tidak sah oleh pihak yang tidak bertanggung jawab, password harus dijaga kerahasiaannya dan tidak boleh diberikan kepada pihak yang tidak diizinkan untuk mengaksesnya.[5]. Sehingga dengan mengetahui password tersebut maka pengguna tersebut atau pengguna lain dapat menggunakan akses untuk masuk ke sistem, ini tentunya tidak aman[6].

Teknologi pengenalan wajah sering digunakan sebagai salah satu metode untuk melakukan autentikasi individu.[7]. Dalam penggunaannya, sistem pengenalan wajah menjadi lebih sulit untuk ditembus, karena metode identifikasinya menggunakan identifikasi geometri wajah yang unik. [8]. Namun pada beberapa perangkat belum memiliki komponen pengenalan wajah yang mampu mengenali orang asli yang sudah dikenali atau hanya foto saja karena hanya menyematkan sistem pengenalan wajah 2D yang kurang aman[9], terutama pada perangkat dengan spesifikasi rendah dan perangkat lawas, dan masih banyak orang pada saat ini yang masih menggunakan perangkat seperti itu tapi mereka juga membutuhkan keamanan[10], dan pada beberapa sistem pengenalan wajah saat ini juga masih terdapat kekurangan yaitu sistem tersebut masih bisa dibobol oleh citra beresolusi tinggi[11]. Pada saat ini terdapat aplikasi dompet digital DANA yang memberikan perlindungan keamanan login dengan pengenalan wajah dengan kedipan mata dengan hanya sekali berkedip yang masih kurang aman.

Dalam menghadapi potensi pembobolan akun tersebut, penulis tertarik untuk mengusulkan solusi dengan menambahkan langkah-langkah keamanan tambahan yaitu, keamanan pada sistem pengenalan wajah yaitu pendeteksi kedipan mata pada saat melakukan login dalam sebuah akun, sehingga pada saat akan login maka sebelum sistem memproses data wajah, sistem akan meminta user untuk berkedip sebanyak yang akan di tentukan oleh sistem untuk memastikan wajah yang akan diproses adalah asli.

Beberapa penelitian telah membahas metode yang dapat dijalankan dengan baik pada perangkat lawas adalah metode Local Binary Pattern Histogram untuk mengenali wajah[12] dan metode Face landmark untuk mendeteksi kedipan mata dengan baik[13]. Dengan menggunakan metode Local Binary Pattern Histogram untuk mengenali wajah yang akan mengakses sistem apakah terdaftar atau tidak[14] dan untuk pendeteksi kedipan mata digunakan metode facial landmark[15] maka sistem ini dapat berjalan pada perangkat lawas atau berspesifikasi rendah. Diharapkan bahwa pembuatan sistem ini akan meningkatkan tingkat keamanan akun sehingga menjadi lebih sulit bagi pihak yang tidak bertanggung jawab untuk melakukan pembajakan.

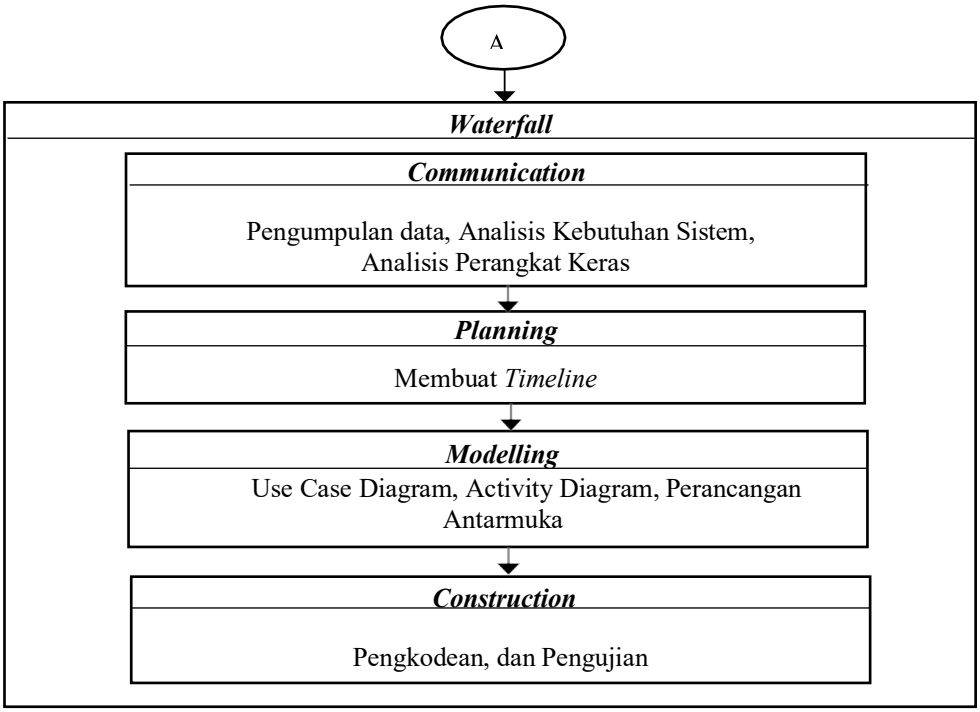
Rumusan masalah dalam penelitian ini mencakup hal-hal berikut ini, bagaimana merancang sistem keamanan dengan pengenalan wajah dan mengimplementasikan pendeteksi kedipan mata pada keamanan akses login ke suatu sistem pada perangkat berspesifikasi rendah. Dan tujuan penelitian ini adalah agar perangkat berspesifikasi rendah dapat menjalankan keamanan pengenalan wajah dan pendeteksi kedipan mata sebagai keamanan akses.

2. METODE PENELITIAN

Penelitian ini menggunakan metode pengembangan SDLC (Sistem Development Life Cycle) dengan pendekatan Model Waterfall yang dijelaskan oleh Pressman pada tahun 2015. [16][17]. Terdapat lima tahap dalam pengembangan, namun dalam penelitian ini terbatas pada tahap keempat, yaitu Communication, Planning, modeling, Construction[18].

2.1 Prosedur Penelitan

Tahap-tahap yang digunakan pada penelitian dapat dlihat pada gambar 1 berikut ini:



Gambar 1 Tahap-tahap penelitian

2. 2 Sumber dan jenis data

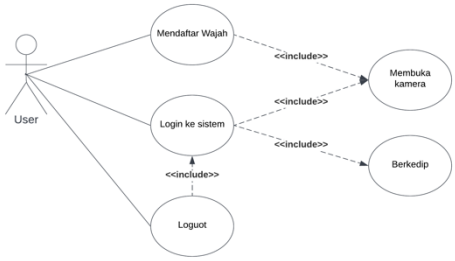
Data yang digunakan dalam penelitian ini merupakan hasil pengambilan gambar wajah dari pengguna akun. Data tersebut diperoleh melalui proses pengujian setelah sistem selesai dikembangkan. Eksperimen dilakukan dengan melakukan pengambilan gambar wajah pengguna dan menyimpannya. Data dari formulir pengambilan wajah pengguna kemudian diarsipkan dalam database sebagai referensi atau template yang akan digunakan oleh sistem saat mencocokkan wajah saat pengguna melakukan login.

2. 3 Permodelan Sistem

Pada tahap ini, dilakukan perancangan aplikasi yang meliputi pembuatan diagram dan antarmuka aplikasi yang akan dibangun.

2.3.1 Use Case Diagram

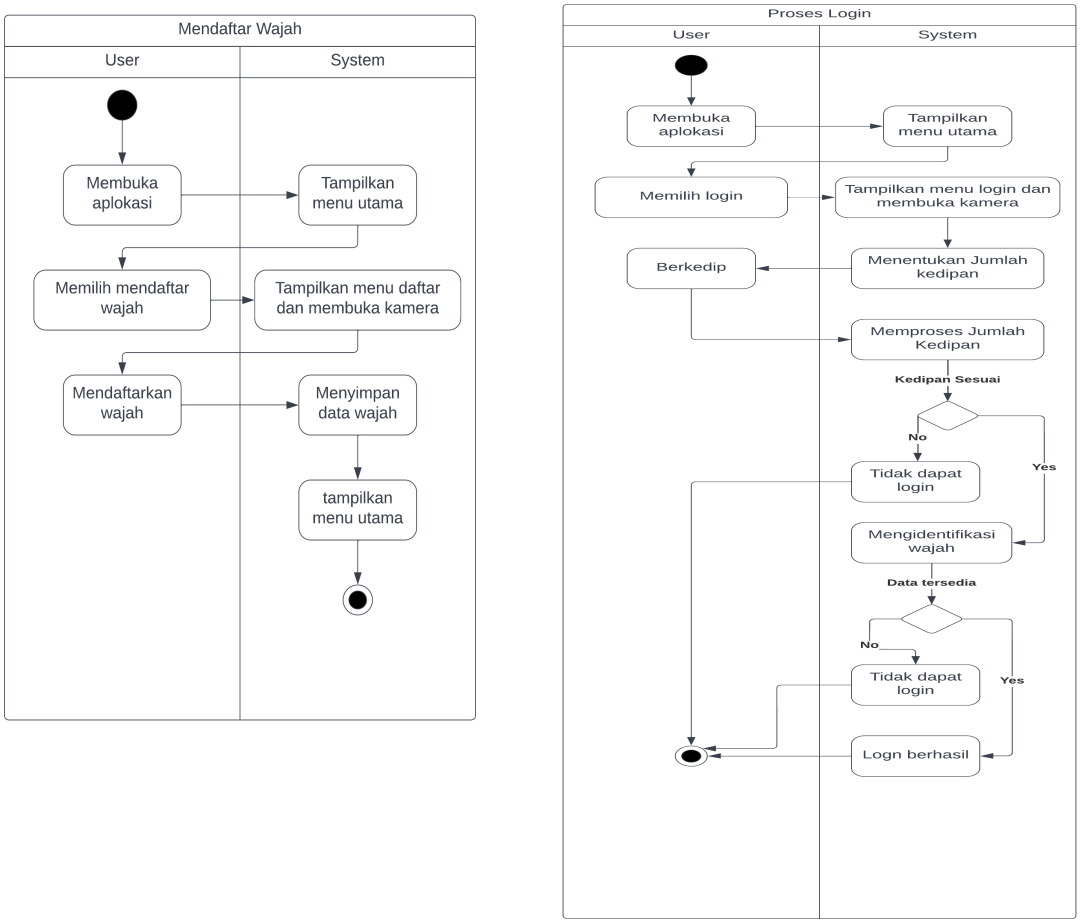
Use Case menggambarkan interaksi antara satu atau lebih aktor dengan sistem yang sedang dikembangkan. [19]. Use Case diagram digunakan untuk mengidentifikasi fungsi-fungsi yang ada dalam sistem informasi dan menunjukkan hak-hak pengguna dalam menggunakan fungsi-fungsi tersebut. Berikut Use Case diagram untuk aplikasi yang yang akan dirancang, ditunjukkan pada Gambar 2



Gambar 2 Use Case Diagram

2.3.2 Activity Diagram

Activity Diagram menunjukkan event-event dari setiap task yang ada, yang biasanya menggambarkan jalannya suatu program atau proses bisnis, bisa juga menggambarkan event-event dari menu yang sedang di gunakan. Activity Diagram berikut dari aplikasi yang dirancang dijelaskan pada Gambar 3.



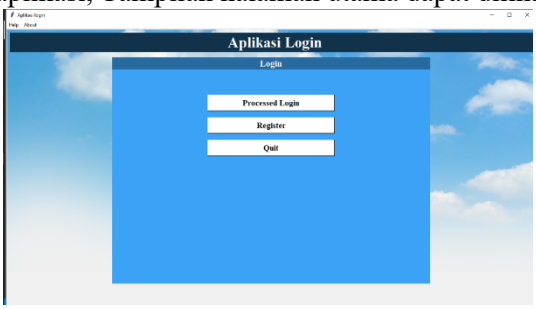
Gambar 3 Activity Diagram

3. HASIL DAN PEMBAHASAN

3.1 Implementasi Antarmuka

3.1.1 Halaman Utama

Pada halaman ini adalah halam yang petama kali ditampilkan saat pertama kali sistem dijalankan. Pada halaman ini terdapat tiga tombol pilihan yaitu tombol Processed login yaitu tombol pilihan untuk untuk melakukan login kedalam aplikasi,tombol register yaitu tombol pilihan untuk pergi ke halaman pendaftara pengguna aplikasi, dan tombol Quit yaitu tombol pilihan untuk keluar dari aplikasi, Tampilan halaman utama dapat dilihat pada Gambar 4



Gambar 4 Halaman Utama

3.1.2 Halaman Daftar

Pada halaman ini adalah halaman yang akan tampil saat tombol register pada halaman utama di klik. Halaman ini meupakan halaman yang digunakan pengguna untuk mendaftarkan kata sandi pada saat pertama kali mendaftar dan untuk mendaftarkan wajah yang dibutuhkan saat melakukan proses login. Pada halaman ini terdapat informasi total yang telah melakukan registrasi, kolom untuk memasukan id dan nama pengguna, tombol clear untuk membersikan imputan pada kolom sebelumnya, tombol kembali untuk kembali pada halaman utama, tombol ambil gambar untuk mulai mengambil gambar wajah dari pengguna untuk digunakan sebagai dataset, dan tombol simpan profil untuk menyimpan semua dataset wajah yang di ambil pada tahap sebelumnya kemudian dibuat kedalam model. Gambar 5 menampilkan tampilan halaman daftar yang dapat dilihat oleh pengguna.

Gambar 5 Halaman Daftar

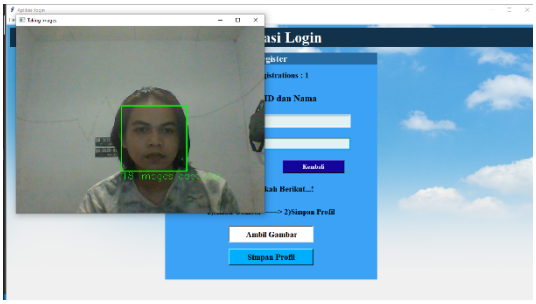
3.1.3 Halaman Dashboard

Pada halaman ini adalah halaman yang akan tampil ketika pengguna berhasil melakukan proses login. Pada halaman ini terdapat tombol logout untuk keluar dari halaman ini dan kembali ke halaman utama, dan tombol quit untuk keluar dari aplikasi. Tampilan halaman dashboard dapat dilihat pada Gambar 6.

Gambar 6 Halaman Dashboard

3.1.4 Halaman deteksi wajah

Terdapat dua halaman untuk mendeteksi dan mengenali wajah termasuk mendeteksi kedipan mata yaitu halaman deteksi wajah saat mendaftarkan wajah yang dapat dilihat pada Gambar 7, dan halaman deteksi wajah saat melakukan proses login yang dapat dilihat pada Gambar 8.



Gambar 7 Halaman deteksi wajah daftar

Gambar 8 Halaman deteksi wajah login

3.2 Implementasi Alur Program

3.2.1 Pendaftaran

Pengguna sistem diijinkan untuk login atau masuk kedalam sistem apabilah telah terdaftar dalam sistem. Oleh karena itu, pengguna perlu melakukan proses pendaftaran ke dalam sistem sebagai langkah pengenalan diri kepada sistem. Hal ini bertujuan agar sistem dapat mengenali pengguna ketika mereka menggunakan aplikasi di waktu-waktu selanjutnya.

3.2.2 Proses Login

Proses login adalah langkah untuk masuk ke dalam sistem komputer setelah pengguna telah melakukan registrasi akun. Halaman sebelumnya menunjukkan bahwa pengguna harus memenuhi 2 syarat untuk masuk ke sistem, Proses login melibatkan dua persyaratan utama, yaitu kata sandi yang benar dan cocoknya wajah dengan data yang terdaftar. Saat pengguna melakukan login, sistem akan memeriksa kesesuaian kata sandi yang dimasukkan dengan kata sandi yang

telah tersimpan dalam sistem saat pengguna mendaftar. Jika kata sandi benar, metode pencocokan akan dipanggil. Pada saat yang sama, Jika kata sandi yang dimasukkan tidak cocok dengan yang ada di sistem, pengguna tidak dapat masuk ke dalam sistem atau akan diminta untuk mengulangi proses login dari awal.

Dalam metode pencocokan diterapkan metode LBPH. Metode ini digunakan untuk mencocokkan gambar input dengan gambar referensi. Metode ini merupakan tahap terakhir dari program dan akan menentukan apakah pengguna dapat berhasil masuk ke dalam sistem atau tidak. Sistem tidak akan memperbolehkan login ketika citra masukan berbeda dengan citra acuan.

3.2.3 Proses ganti kata sandi

Pada menu help yang terdapat diatas sebelah kiri aplikasi terdapat pilihan untuk mengubah katasandi, Pengguna yang sudah pernah mengatur kata sandi untuk proses login dan proses mendaftar dapat mengubah kata sandi tersebut dengan cara memilih menu tersebut, setelah mengubah kata sandi maka proses mendaftar dan login selanjutnya akan di minta kata sandi sesuai dengan yang telah diubah. Syarat untuk mengubah katasandi adalah pengguna harus mengingat kata sandi sebelumnya.

3.2.4 Poses pengambilan dataset citra wajah

Sebelum mengambil gambar, kamera melakukan pencarian wajah untuk dideteksi menggunakan metode face detection. Pada pendeteksian objek, digunakan pendekatan haar cascade classifier yang melibatkan dua kali proses pengolahan sebelum menghasilkan output objek yang terdeteksi dalam citra. Dalam metode ini, proses pemrosesan yang digunakan adalah Grayscale dan Haar-Like Feature.

3.2.5 Latih Dataset

Dalam proses ini, algoritma Haar Cascade akan digunakan dari semua gambar yang diperoleh (kumpulan data) untuk penelitian, dan wajah pada setiap gambar akan dibedakan dengan Ekstraksi Informasi Ekspresi Wajah.
Mekanisme yang digunakan adalah membagi area gambar menjadi blok 8x8 terlebih dahulu. Setiap blok diubah menjadi ukuran thresholding 3x3 untuk mendapatkan nilai histogram. Selanjutnya, piksel perantara dari blok tersebut diambil sebagai pembanding.

3.2.6 Pengenalan wajah

Setelah gambar disimpan dalam format yml, data akan dibaca dan diberi nama sesuai dengan nomor id yang diberikan Hasil dari proses ini diolah dengan manfaatkan hasil pelatihan dari haar cascade, lalu menggunakan salah satu metode algoritma haar cascade yaitu Local Binary Pattern Histogram. Dengan menggunakan pendekatan ini, Citra pelatihan dibandingkan dengan deteksi yang diperoleh dari streaming kamera untuk mencocokkan hasil deteksi, yang kemudian dicocokkan dengan beberapa gambar di database. Pencocokan menghasilkan ya atau tidak dalam verifikasi, sedangkan pengenalan menghasilkan persentase akurasi tertentu dengan menggunakan nilai histogram yang diekstrak dari citra menggunakan metode Local Binary Pattern Histogram. Kesalahan saat melakukan proses pengenalan wajah, yaitu kamera menolak citra masukan saat mendeteksi wajah, Citra masukan yang seharusnya dapat dikenali (yang identitasnya ada di database) tidak dapat dikenali oleh sistem.

3.2.7 Pendeteksi kedipan mata

dlib library menyediakan metode untuk menghitung kedipan mata dengan menggunakan deteksi titik-titik landmark pada wajah dan analisis perbedaan dari posisi titik-titik tersebut dari frame ke frame dalam video. Metode ini menggunakan titik-titik landmark yang dideteksi pada mata kiri dan mata kanan, kemudian menghitung perbedaan posisi dari titik-titik tersebut dari frame ke frame untuk menentukan apakah mata tersebut sedang kedip atau tidak.

Pertama, algoritma ini menggunakan deteksi titik-titik landmark pada wajah untuk menemukan posisi mata kiri dan mata kanan. Kemudian, algoritma terus memantau posisi dari titik-titik ini dari frame ke frame dalam video. Jika ada perbedaan yang cukup besar dalam posisi titik-titik ini dari frame ke frame, algoritma menganggap bahwa mata tersebut sedang kedip.

3.3 Pengujian sistem

3.3.1 Pengujian tingkat akurasi deteksi

Pada pengujian tingkat akurasi deteksi wajah, tujuannya adalah untuk mengetahui apakah sistem deteksi wajah dengan baik dan akurat pada saat pengambilan data wajah pada beberapa kondisi. Pengujian dilakukan dengan dua kondisi yaitu berdasarkan jarak dan berdasarkan sudut miring citra wajah. Pengujian dapat dilihat pada Tabel 1

Tabel 1 Pengujian terhadap sudut dan jarak wajah

	Jarak Wajah (cm)				
Sudut wajah	30	50	100	150	200
15º ke kanan	✓	✓	✓	✓	-
45º ke kanan	✓	✓	✓	-	-
15º ke kiri	✓	✓	✓	✓	-
45º ke kiri	✓	✓	✓	-	-
30º ke atas	✓	✓	✓	-	-
30º ke bawah	✓	✓	✓	✓	-

3.3.2 Pengujian akurasi deteksi kedipan

Pengujian akurasi deteksi kedipan mata bertujuan untuk mengetahui apakah sistem dapat mengenali kedipan mata yang dilakukan oleh pengguna dan untuk mengukur akurasi dari pendeteksi kedipan mata pada kondisi tertentu. Pengujian dilakukan berdasarkan jumlah waktu untuk berkedip dan jarak wajah ke posisi kamera dan dilakukan lima kali kedipan pada setiap kondisi. Pengujian dapat dilihat pada Table 2 dan Table 3

Tabel 2 lama waktu untuk berkedip

Lama waktu kedipan dalam hitungan detik	Gagal	Terdeteksi
0,1	✓	
0,2	✓	
0,3	✓	
0,4	✓	
0,5		✓
1,0		✓
2,0		✓

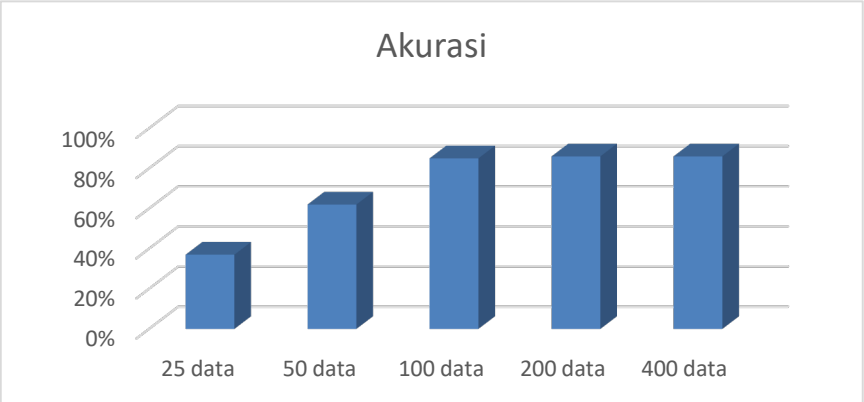
Tabel 3 Jarak untuk berkedip

Percobaan	Jarak	Gagal	Terdeteksi
1	20		✓
2	30		✓
3	40		✓
4	50		✓
5	60		✓
6	70		✓
7	80		✓
8	90		✓

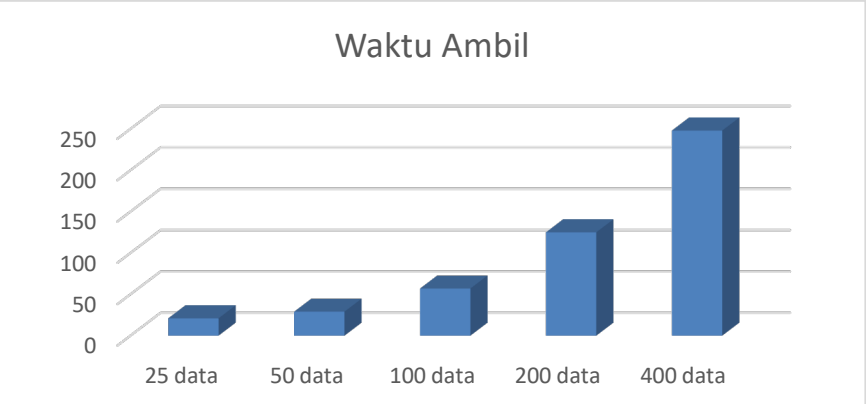
9	100		✓
10	120		✓
11	140	✓	
12	150	✓	

3.3.3 Pengujian Jumlah Dataset Citra Acuan

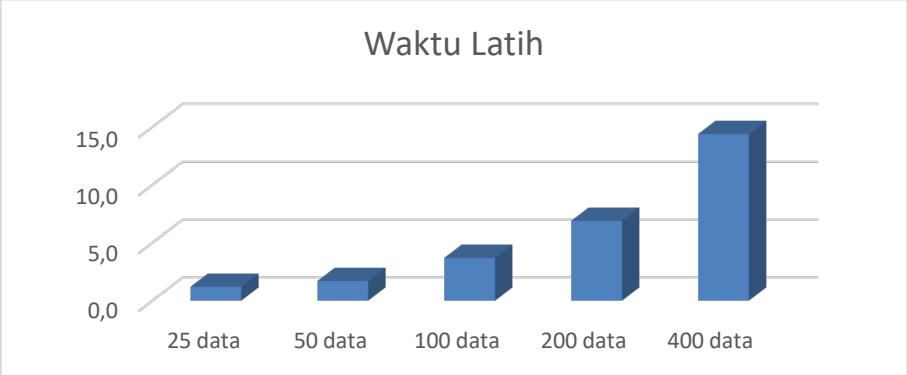
Pada pengujian ini bertujuan untuk mengetahui berapa banyak citra acuan yang paling oktimal untuk nantinya di jumlah itu digunakan untuk mengatur jumlah pengambilan citra wajah saat pendaftaran ke dalam sistem yang dilakukan oleh pengguna. Pengujian ini dilakukan dengan membandingkan waktu yang dibutuhkan untuk membuat sebuah model acuan dari masing-masing banyaknya citra acuan agar dapat berjalan dengan baik pada perangkat lawas, dan membandingkan akurasi mengenali wajah yang didapatkan dari setiap banyaknya jumlah citra acuan. Sehingga dari hasil waktu dan akurasi yang didapat akan disimpulkan berapa banyak jumlah dari dataset citra acuan yang paling optimal untuk digunakan dalam aplikasi. Tahapan pengujian ini adalah mengukur waktu pengambilan citra wajah, waktu untuk latih model, dan akurasi yang berdasarkan keberhasilan mengenali wajah terdaftar dibandingkan kesalahan mengenali wajah yang terdaftar dan kesalahan mengenali wajah yang tidak terdaftar. Pengujian dan hasilnya dapat dilihat pada Gambar 9, Gambar 10, dan Gambar 11.



Gambar 9 Pengujian Pada Akurasi



Gambar 10 Pengujian waktu ambil dataset



Gambar 11 Pengujian waktu latih dataset

Dari percobaan diatas berdasarkan waktu pengambilan citra wajah, waktu untuk melatih model dan akurasi yang didapatkan maka penulis menyimpulkan jumlah data citra wajah yang paling ideal adalah 100 citra.

3.3.5 Pengujian waktu saat proses login

Pengujian ini bertujuan untuk mengetahui waktu yang diperlukan untuk menyelesaikan proses login. dengan melakukan pengukuran pada waktu yang dibutuhkan sistem untuk mendeteksi 5kali kedipan dan waktu yang dibutuhkan sistem untuk mengenali wajah yang telah dilatih. Pengujian dilakukan terhadap 14 orang berbeda dan juga dengan kondisi pencahayaan yang berbeda yaitu redup, terang dan normal. Pengujian dapat dilihat pada Tabel 5.

Tabel 5 Waktu Proses login

Kondisi pencahayaan	Kedipan	Kenal wajah
Terang	6,3 detik	0,2 detik
Redup	7,4 detik	0,6 detik
Normal	6,9 detik	0,1 detik

3.5.6 Pengujian pada beberapa berangkat

Pengujian ini bertujuan untuk mengevaluasi apakah aplikasi yang dibuat dapat berjalan dengan baik pada beberapa perangkat lawas dan perangkat berspesifikasi rendah, pengujian dilakukan dengan menjalankan fitur-fitur pada aplikasi yaitu mendaftarkan wajah, dan melakukan login kedalam aplikasi. Pengujian dapat dilihat pada Tabel 6.

Tabel 6 Pengujian pada beberapa perangkat

Nama perangkat	Fitur aplikasi	Dapat dijalankan	
		Ya	Tidak
ASUS X453SA	Mendaftar	✓	
	Login	✓	
Vaio C15	Mendaftar	✓	
	Login	✓	
HP AM514TU	Mendaftar	✓	
	Login	✓	

4. KESIMPULAN

Berdasarkan hasil analisis, perancangan, pengujian, dan implementasi program yang telah dilakukan terhadap pengembangan aplikasi login menggunakan pengenalan wajah dan kedipan mata, maka dapat ditarik kesimpulan bahwa sistem login dengan menggunakan pengenalan wajah dan pendeteksian kedipan mata telah berhasil dibangun dan dapat dijalankan dengan baik pada perangkat lawas atau perangkat dengan spesifikasi rendah.

5. SARAN

Saran yang dapat dipertimbangkan dan dijadikan bahan referensi untuk penelitian selanjutnya adalah Sistem dapat dikembangkan untuk perangkat dengan spesifikasi tinggi dengan menggunakan algoritma deeplearning agar dapat mengenali wajah dan mendeteksi kedipan mata dengan lebih baik, Mengimplementasikan di sistem keamanan selain akses login, menambahkan pendeteksi ekspresi wajah yang lain, dan penggunaan kamera dengan resolusi yang lebih tinggi.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Tuhan Yang Maha Kuasa atas berkat dan rahmat-Nya yang telah membantu penulis menyelesaikan penelitian ini. Penulis juga menyadari bahwa banyak pihak yang memberikan bantuan dan bimbingan selama proses penelitian ini. Oleh karena itu, penulis ingin memberikan penghargaan yang setinggi-tingginya dengan ucapan terima kasih kepada dosen pembimbing, orang tua, keluarga besar penulis, rekan-rekan penulis, serta redaksi Cogito Smart Journal yang telah mempublikasikan hasil penelitian ini.

DAFTAR PUSTAKA

[1] B. A. Malin, MS, and MPhil, “An Evaluation of the Current State of Genomic Data Privacy Protection Technology and a Roadmap for the Future”, *Journal of the American Medical Informatics Association,* vol. 12, no. 1, pp. 28-34, 2005, doi: 10.1197/jamia.M1603.

[2] P. W. Dowd, and J. T. McHenry, “Network Security: It’s Time To Take It Seriously”*, IEEE Computer*, vol 31, no. 9, pp. 24-28, 1998, doi: 10.1109/2.708446.

[3] Dyna Marisa Khairina, “Analisis Keamanan Sistem Login”, *Jurnal Informatika Mulawarman*, vol. 6, no. 2, pp. 64-67, 2011.

[4] V. Beal, “What is username”, 1998. https://www.webopedia.com/definitions/username/ (accessed Feb. 5, 2023)

[5] Azhar Azhar, Wais Alkarni, Atthariq Atthariq, “Sistem Keamanan Pada Halaman Login Menggunakan One Time Password”, *Journal Of Embedded System And Intelligent System,* vol. 1, no. 2, hal 107-113, 2020.

[6] Y. Han, and J. Kim, “An Analysis of Security Threats and Countermeasures for Passwords”, *Security and Communication Networks*, vol. 10, no. 7, pp. 1067-1082, 2017.

[7] S. Z. Li, and A. K. Jain, "A Survey of Face Recognition Technologies", *Pattern Recognition*, vol. 40, no. 3, pp. 1106-1122, 2007.

[8] Arnold Nasir, "Perancangan Aplikasi Pengenalan Wajah Sebagai Media Akses Kontrol Pada Organisasi XYZ", *Jurnal Edukasi Dan Penelitian Informatika*, vol. 2, no. 1, pp. 71-77, 2016, doi: 10.26418/jp.v2i1.14767.

[9] Shilpi Singha ,S.V.A.V.Prasad, "Techniques and Challenges of Face Recognition: A Critical Review", *Procedia Computer Science,* vol. 143, pp. 536–543, 2018, doi: 10.1016/j.procs.2018.10.427.

[10] R. C. Seacord, Daniel Plakosh, G. A. Lewis, *Modernizing Legacy Systems: Software Technologies, Engineering Processes, and Business Practices,* Addison-Wesley Professional, Lake Ave Glenview, 2003.

[11] Reyvan Maulid, "Penerapan Algoritma Machine Learning Pada Face Recognition", 2021, https://www.dqlab.id/penerapan-algoritma-machine-learning-pada-face-recognition , (accessed Des. 20, 2022).

[12] A. Nene, H. Jain, K. Gaikar, S. Bohra, and N. Mahajan, "Facial Recognition System Using LBPH Algorithm and Raspberry Pi", *IRJET,* vol. 08, no. 6, pp. 4411-4415, 2021.

[13] A. Arora, A. Sinha, K. Bhansali, R. Goel, I. Sharma, and A. Jayal, "SVM and Logistic Regression for Facial Palsy Detection Utilizing Facial Landmark Features", *Association for Computing Machinery (ACM),* pp. 43-48, 2022.

[14] R. Kosasih, & C. Daomara, "Pengenalan Wajah dengan Menggunakan Metode Local Binary Patterns Histograms (LBPH)", *JURNAL MEDIA INFORMATIKA BUDIDARMA*, vol. 5, no. 4, pp. 1258-1264, 2021, doi: 10.30865/mib.v5i4.3171.

[15] Nggiku, C. K, "Deteksi Kantuk Pada Pengemudi Mobil Menggunakan Eye Aspect Ratio Dengan Metode Facial Landmark", *SinarFe7*, vol. 5, no. 1, pp. 72-78, 2022.

[16] A. Moenir, & F. Yuliyanto, "Perancangan Sistem Informasi Penggajian Berbasis Web dengan Metode Waterfall pada PT. Sinar Metrindo Perkasa (Simetri)", *Jurnal Informatika Universitas Pamulang*, vol. 3, no. 2, pp. 127-137, 2017, doi: 10.32493/informatika.v2i3.1237.

[17] P. Nurmala, W. Gazali, & W. Budiharto, "Sistem Kontrol Akses Berbasis Real Time Face Recognition dan Gender Information", *ComTech: Computer, Mathematics and Engineering Applications*, vol. 6, no. 2, pp. 198-207, 2015.

[18] Bintang Anugrah, *Uji Keakurasian Metode Eigenface Dalam Face Recognition*, Sekolah Tinggi Manajemen Informatika & Komputer Indonesia Mandiri, Bandung, 2019.

[19] A. Cockburn, *Writing effective use cases*, Pearson Education India, Uttar Pradesh, 2001.

[20] M. Fowler, *UML distilled: a brief guide to the standard object modeling language*, Addison-Wesley Professional, Glenview, 2004.