ISSN 2355-3286

Pengaplikasian *Face Recognition* 3 Dimensi untuk Keamanan

Jason Adrian Mahalim[1], Muhamad Aliefian R[2], Muhamad Rizky Febrianto[3], Nabila Husna Shabrina[4]
[1, 2, 3, 4] Teknik Komputer, Universitas Multimedia Nusantara, Tangerang, Indonesia
jason.mahalim@student.umn.ac.id
muhamad3@student.umn.ac.id
muhamad.febrianto@student.umn.ac.id
nabila.husna@umn.ac.id

Diterima 20 Mei 2020
Disetujui 16 Juni 2020

***Abstract*—Face recognition is one of the biometric categories which uses face as the identifier. Currently, there are two versions of face recognition, 2 dimensional and 3 dimensional. This research uses 3 dimensional face recognition, and the goal for this research is for comparing the accuracy between 2 dimensional and 3 dimensional face recognition, analyze the performance of 3 dimensional face recognition, and applying 3 dimensional face recognition for security measure, namely for automatic door lock using face recognition. Face Alignment Network used as the method for this 3 dimensional face recognition. This research prove that 3 dimensional face recognition have better accuracy than its predecessor, however some weakness is also found in this research, i.e. image resolution, lighting of the photo, angle of the face when the photo taken will govern the accuracy of the 3 dimensional face recognition and 3 dimensional face recognition can't differentiate between twins brother faces.**

***Index Terms*—Accuracy, Face Recognition**

I. PENDAHULUAN

Keamanan merupakan salah satu hal yang penting bagi kehidupan manusia. Tanpa adanya keamanan terdapat banyak kekayaan dan data yang bisa dibobol oleh oknum yang tidak bertanggung jawab. Untuk mencegah hal tersebut, maka langkah keamanan mulai diaplikasikan ke banyak kasus, contohnya adalah penggunaan PIN (Personal Identification Number) pada ATM dan penggunaan password pada komputer personal. Namun langkah keamanan tersebut dinilai kurang aman, karena berdasarkan penelitian [1], sebanyak 30 password dari 95 anggota grup kontrol bisa dibobol dengan menggunakan *dictionary attack*, permutasi dari kata & angka dan *user information attack*.

Terdapat pengembangan dari langkah keamanan password dan PIN, yaitu dengan menggunakan *biometric* sebagai kunci dari langkah keamanan yang digunakan. *Biometric* adalah sebuah algoritma pengenalan otomatis yang mengambil karakteristik anggota tubuh yang dimiliki oleh seseorang. Terdapat beberapa contoh anggota tubuh yang bisa digunakan sebagai *biometric*, yaitu DNA, telinga, wajah, sidik jari dan retina mata [2], pada penelitian ini, *biometric* yang akan digunakan adalah wajah, spesifiknya akan digunakan sebagai *face recognition*.

Terdapat dua versi dari *face recognition*, yaitu 2 dimensi dan 3 dimensi. Dalam beberapa waktu belakangan ini, *face recognition* 3 dimensi mulai banyak dipakai dibandingkan dengan *face recognition* 2 dimensi, karena *face recognition 3* dimensi memiliki tingkat akurasi yang lebih baik dibandingkan dengan *face recognition* 2 dimensi, karena jika adanya penutupan wajah karena objek seperti masker, kacamata dan tangan, maka *face recognition* 2 dimensi tidak bisa membaca wajah tersebut dengan sempurna, karena terdapat informasi yang hilang akibat penutupan wajah tersebut [3].

Metode yang dipakai dalam penelitian ini adalah *Face Alignment Network* (FAN) yang dibuat oleh Adrian Bulat [4,5]. Alasan dipilihnya metode tersebut karena FAN bisa secara akurat memetakan bentuk wajah seseorang ke dalam 3 dimensi, meskipun terdapat beberapa gangguan, seperti wajah terhalang objek dan wajah yang terdapat di dalam foto miring. Cara kerja dari metode tersebut adalah dengan melihat fitur-fitur wajah dan kontur wajah pengguna dengan menggunakan beberapa stacked hourglass network untuk membuat heatmap dari masing-masing fitur wajah , sehingga penutupan wajah dengan objek masih bisa diperkirakan oleh algoritma *face recognition* 3 dimensi.

Pada penelitian ini, kami mengupayakan poin-poin yang menjadi hal utama dalam pembuatannya, poin-poin tersebut adalah:

1. Keamanan
   Penelitian ini akan diaplikasikan ke sebuah langkah keamanan, yang diharapkan akan memperkuat tingkat keamanan dari langkah keamanan tersebut.
2. Akurasi
   Penelitian bertujuan untuk membandingkan

akurasi dari *biometric face recognition* 2 dimensi dengan menggunakan *face recognition* 3 dimensi.

II. TINJAUAN PUSTAKA

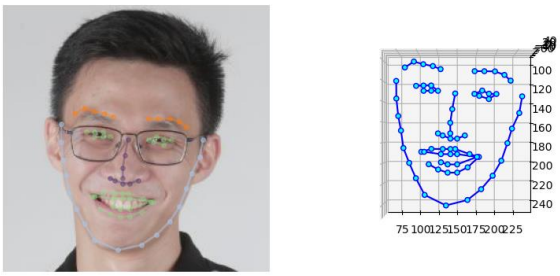
A. *Face Alignment Network*

Penelitian ini untuk memetakan wajah menggunakan salah satu algoritma, yaitu *face alignment network*. *Face alignment network* sendiri dibuat dengan menggunakan beberapa buah *hourglass network* yang awalnya dibuat untuk memperkirakan pose dari manusia [4,5]. Berdasarkan [5] untuk mendeteksi pose yang dimiliki oleh subjek yang terdapat di dalam foto, maka algoritma akan mengambil beberapa *heatmap* dari beberapa bagian tubuh manusia seperti leher, pergelangan tangan dan lutut. Setelah mendapatkan *heatmap* tersebut, nantinya pose bisa diperkirakan dengan cara menarik garis antar *heatmap* yang ada.

Sedikit berbeda dengan [5], [4] akan membuat *heatmap* dari wajah yang terdapat di dalam foto. Berdasarkan [6] untuk mendapatkan beberapa fitur dari wajah dan mendapatkan pose, ekspresi dan informasi bentuk. *Heatmap* juga berguna untuk memetakan *confidence* yang menyediakan konteks spasial dan hubungan antar bagian dan nantinya akan diterjemahkan ke dalam bentuk koordinat 3 dimensi. Tabel 1 menunjukkan hasil *mapping* dan gambar 1 menunjukkan visualisasi hasil *mapping* dari penggunaan algoritma Face Alignment Network.

Tabel 1. Koordinat hasil *mapping* FAN

Fitur Wajah	Nomor Koordinat
Rahang	1-17
Alis 1	18-22
Alis 2	23-27
Hidung	28-31
Lubang Hidung	32-36
Mata 1	37-42
Mata 2	43-48
Bibir	49-60
Gigi	61-68



Gambar 1. Visualisasi hasil *mapping* algoritma FAN

Implementasi dari algoritma tersebut untuk penelitian ini adalah untuk melakukan pemetaan foto *input* dan foto *dataset* ke dalam koordinat 3 dimensi, sehingga bisa dilakukan perhitungan kemiripan wajah dengan menggunakan *Euclidean Distance.*

III. METODOLOGI DAN IMPLEMENTASI

Pendekatan metodologi yang digunakan saat melakukan pengujian penelitian ini adalah secara kuantitatif, dimana hasil akan dinilai berdasarkan akurasi dan performa dari penelitian bila diberikan beberapa kasus. Terdapat 3 kasus untuk pengujian penelitian ini. Kasus pertama menggunakan dataset dengan beberapa kondisi, yaitu foto biasa, kedua mata tertutup oleh tangan, mata kiri tertutup oleh tangan, mata kanan tertutup oleh tangan, mulut ditutup oleh tangan, dan kondisi tiga foto yang relatif gelap. Kasus pertama memiliki tujuan untuk membandingkan tingkat akurasi *face recognition* 2 dimensi dan 3 dimensi apabila wajah tertutup oleh sebuah objek dan ketika pengambilan foto dilakukan di tempat yang relatif gelap.

Kasus kedua menggunakan foto anak kembar, dimana tujuan digunakan foto anak kembar adalah untuk menguji apakah algoritma *face recognition* 3 dimensi bisa membedakan muka anak kembar. Kasus ketiga menggunakan dataset *Labeled Faces in the Wild* (LFW), tujuan pengujian kasus ini adalah untuk menghitung kecepatan dari algoritma *face recognition* 2 dimensi dan 3 dimensi jika terdapat banyak data yang akan dibandingkan di dalam *dataset*. Semua pengujian dilakukan pada komputer dengan CPU Intel Core i7 6700 dan *Graphic Card* NVIDIA GTX 960M.

Hasil pengujian akan diolah menggunakan *confusion matrix* untuk menghitung tingkat akurasi dari masing-masing kasus pengujian [7]. Rumus yang digunakan untuk mendapatkan akurasi pengujian pertama dan kedua terdapat pada (1).

Pada bagian ini akan dibahas tentang hasil perancangan dan pengujian telah dilakukan pada perangkat. Pengujian dilakukan untuk mengetahui apakah sistem yang telah dibangun telah berfungsi dengan benar atau tidak.

$$akurasi = \frac{TP + TN}{TP + TN + FP + FN} \quad (1)$$

Euclidean distance akan kami gunakan untuk menghitung kemiripan yang dimiliki oleh foto *input* dengan foto *dataset*. Alasan kami menggunakan *Euclidean distance* karena output yang dihasilkan berupa koordinat 3 dimensi, sehingga untuk menghitung jarak antar koordinat akan digunakan *Euclidean Distance.* Alasan lain dipilihnya *Euclidean Distance*, karena *Euclidean Distance* umum digunakan, mudah untuk dikomputasi, dan bekerja dengan baik dengan data yang padat atau memiliki cluster yang kecil [8]. Semakin kecil jarak yang dimiliki oleh foto input dengan foto *dataset*, maka akan semakin mirip wajah tersebut. Syarat yang digunakan untuk menentukan kemiripan antara foto input dengan foto *dataset* terdapat pada (2).

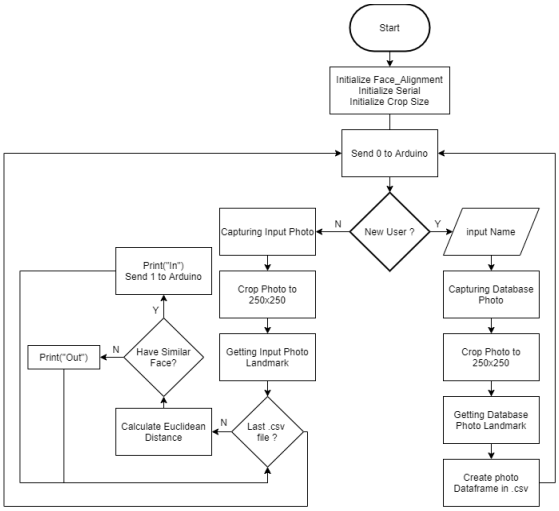
(jarak[x] < 120 and jarak [y] < 120 and jarak [z] < 120) or (jarak [x] < 120 and jarak [y] < 120) or (jarak [y] < 120 and jarak [z] < 120) or (jarak [x] < 120 and jarak [z] < 120) (2)

Alasan kami memilih banyak kombinasi koordinat yang dibandingkan, untuk membandingkan banyak fitur wajah yang dimiliki oleh orang tersebut, sehingga ketika salah satu fitur tertutup, masih terdapat fitur wajah lain yang bisa dibandingkan.

Penelitian ini menggunakan bahasa pemrograman python untuk melakukan *image processing* dan C untuk komunikasi bersama dengan Arduino. Penelitian kami menggunakan Arduino sebagai *prototype* jika penelitian ini digunakan ke dalam kasus nyata, yaitu digunakan sebagai kunci. Gambar 1 menunjukkan alur dari program yang kami buat untuk penelitiaan ini.

Proses yang terjadi selama penggunaan program adalah pengguna diberikan pilihan ketika pertama kali program dinyalakan, apakah pengguna merupakan pengguna baru atau lama. Jika pengguna merupakan pengguna baru, maka wajah pengguna tersebut akan difoto, dipetakan ke dalam koordinat 3 dimensi dan disimpan ke dalam sebuah *folder database* yang berisikan pengguna yang sudah mendaftar dengan format CSV.

Jika pengguna merupakan pengguna lama, maka pengguna tersebut bisa langsung memfoto wajahnya ke kamera yang tersedia. Setelah wajah pengguna di foto, maka foto tersebut akan dipetakan ke dalam koordinat 3 dimensi, kemudian akan dibandingkan dengan *file-file* CSV yang terdapat dalam *folder* database. Jika parameter kemiripan mengatakan bahwa pengguna tersebut memiliki kemiripan dengan salah satu *file* CSV di dalam *folder database*, maka pengguna tersebut bisa masuk dan program akan kembali ke kondisi awal, namun jika parameter kemiripan mengatakan tidak ada wajah yang mirip dalam *folder database*, maka pengguna tersebut tidak diijinkan untuk masuk.



Gambar 2. *Flowchart program*

IV. HASIL DAN ANALISIS

Kasus pengujian pertama dilakukan untuk membandingkan tingkat akurasi antara *face recognition* 2 dimensi dan 3 dimensi jika terdapat objek yang menutup wajah. Foto yang digunakan sebagai input terdapat pada Gambar 3 dan foto yang menjadi pembanding terdapat pada Gambar 4. Hasil yang didapatkan terdapat pada Tabel 2.

Gambar 3. Input pengujian pertama (dari kanan ke kiri: input 1, input 2, input 3)

Gambar 4. Gambar *dataset* pengujian kasus pertama

Tabel 2. Koordinat hasil *mapping* FAN

Klasifikasi	3 Dimensi Input			2 Dimensi Input		
	Inp 1	Inp 2	Inp 3	Inp 1	Inp 2	Inp 3
TP	5	7	4	2	3	2
TN	19	17	14	19	19	16
FP	5	3	6	8	7	8
FN	1	3	6	1	1	4
Akurasi	80%	80%	60%	70%	73%	60%
Rata-rata	73,34%			67,78%		

Berdasarkan hasil pengujian pertama, dapat disimpulkan bahwa *face recognition* 3 dimensi memiliki tingkat akurasi yang lebih baik dibandingkan dengan rekan imbangannya. Rata-rata akurasi dihitung dengan menjumlahkan semua hasil akurasi dan dibagi tiga. *Face recognition* 3 dimensi dan 2 dimensi bisa mendeteksi kemiripan wajah di tempat yang relatif gelap, namun tidak bisa membedakan wajah yang miring ke kiri dan ke kanan dengan foto input ketika di dalam kondisi tersebut.

Face recognition 3 dimensi akan lebih unggul jika terdapat kasus dimana wajah tertutup oleh objek dan wajah miring ke kiri atau ke kanan. Penyebab input 3 memiliki akurasi yang rendah dibandingkan dengan input lainnya adalah foto yang digunakan relatif gelap dibandingkan dengan foto lainnya, sehingga hasil *mapping* dari foto tersebut tidak akurat dan menyebabkan tingkat akurasi yang rendah.

Pengujian yang kedua, foto yang digunakan adalah foto anak kembar, pengujian ini dilakukan untuk mengetahui apakah *face recognition* 3 dimensi bisa membedakan muka anak kembar. Gambar 5 menunjukkan input dari pengujian kedua, dan Gambar 6 menunjukkan gambar pembanding. Hasil dari pengujian kedua terdapat pada Tabel 3.

Gambar 5. Input pengujian kedua

Gambar 6. Gambar *dataset* pengujian kasus kedua

Tabel 3. Hasil pengujian kedua

Klasifikasi	Hasil
True Positive	2
True Negative	0
False Positive	3
False Negative	0
Akurasi	40,00%

Berdasarkan Tabel 3 tersebut, bisa disimpulkan bahwa penelitian ini tidak bisa membedakan anak kembar, akurasi yang didapatkan dari pengujian tersebut adalah 40 persen. Penyebab didapatkan hasil tersebut adalah banyak kombinasi sumbu yang dibandingkan pada parameter kemiripan, sehingga ketika harus membedakan muka anak kembar, penelitian ini mengalami kesulitan.

Pengujian ketiga menggunakan *dataset Labeled Faces in The Wild* (LFW), terdapat hanya 13.233 foto dari LFW, dan input yang digunakan adalah wajah yang tidak terdapat di dalam dataset. Gambar 7 menunjukkan foto input yang digunakan, dan gambar 8 beberapa contoh foto yang terdapat di LFW. Hasil yang didapatkan dari pengujian ketiga terdapat pada Tabel 4. Pengujian akan dilakukan sebanyak 5 kali untuk masing-masing algoritma, dan waktu yang didapatkan akan dirata-rata.

Gambar 7. Input dari pengujian ketiga

Gambar 8. Beberapa gambar LFW

Tabel 4. Hasil pengujian ketiga

Algoritma	Percobaan Ke-	Hasil (S)	Rata-rata (S)
3d	1	26,9	27,12
	2	32,00	
	3	25,7	
	4	25,5	
	5	25,5	
2d	1	34,8	26,74
	2	26,7	
	3	23,9	
	4	24,4	
	5	23,9	

Berdasarkan pengujian tersebut, algoritma 3 dimensi dan 2 dimensi memiliki perbedaan waktu yang relatif sedikit, yaitu selama 0,38 detik. Metode yang digunakan untuk melakukan perhitungan waktu adalah dengan menggunakan library *time* dan menghitung selisih waktu mulai dan waktu berakhirnya program. Alasan terdapat 5 kali percobaan masing-masing algoritma dan hasil dirata-rata adalah karena terdapat perbedaan waktu setiap kali program dijalankan.

V. SIMPULAN

Keamanan dan akurasi merupakan poin yang ingin kami tegaskan pada penelitian ini. Hasil penelitian kami menunjukkan bahwa *face recognition* 3 dimensi akan memiliki akurasi yang lebih baik dan waktu proses yang tidak berbeda jauh jika dibandingkan dengan *face recognition* 2 dimensi, namun *face recognition* 3 dimensi masih belum bisa membedakan wajah anak kembar dan masih memiliki banyak syarat untuk mendapatkan tingkat akurasi yang optimal.

DAFTAR PUSTAKA

[1] J. Yan, A. Blackwell, R. Anderson and A. Grant, "Password memorability and security: empirical results," in *IEEE Security & Privacy*, vol. 2, no. 5, pp. 25-31, Sept.-Oct. 2004, doi: 10.1109/MSP.2004.81.

[2] A. K. Jain, A. Ross and S. Prabhakar, "An introduction to biometric recognition," in *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 4-20, Jan. 2004, doi: 10.1109/TCSVT.2003.818349.

[3] M. Chihaoui, A. Elkefi, W. Bellil, and C. B. Amar, "A Survey of 2D Face Recognition Techniques," *Computers*, vol. 5, no. 4, p. 21, 2016.

[4] A. Bulat and G. Tzimiropoulos, "How Far are We from Solving the 2D & 3D Face Alignment Problem? (and a Dataset of 230,000 3D Facial Landmarks)," *2017 IEEE International Conference on Computer Vision (ICCV)*, 2017.

[5] J. Yang, A. Bulat, and G. Tzimiropoulos, "FAN-Face: a Simple Orthogonal Improvement to Deep Face Recognition."

[6] A. Newell, K. Yang, and J. Deng, "Stacked Hourglass Networks for Human Pose Estimation," *Computer Vision – ECCV 2016 Lecture Notes in Computer Science*, pp. 483–499, 2016.

[7] K. S. Nugroho, "Confusion Matrix untuk Evaluasi Model pada Supervised Learning," Confusion Matrix untuk Evaluasi Model pada Supervised Learning, 13-Nov-2019. [Online]. Available: https://medium.com/@ksnugroho/confusion-matrix-untuk-evaluasi-model-pada-unsupervised-machine-learning-bc4b1ae9ae3f. [Accessed: 06-Apr-2020].

[8] A. S. Shirkhorshidi, S. Aghabozorgi, and T. Y. Wah, "A Comparison Study on Similarity and Dissimilarity Measures in Clustering Continuous Data," *Plos One*, vol. 10, no. 12, 2015.