Volume 16 Nomor 2 (2021) 31-39
E – Link P-ISSN 1858-2109 E-ISSN 2656-5676
Jurnal Teknik Elektro dan Informatika

Penerapan *Liveness* Sebagai *Anti-Spoofing* Citra Digital Pada Sistem Keamanan Akses Kontrol Ruang Server Berbasis Raspberry Pi

Galeh Rizkya Safri [1)] , Denny Irawan [2)], Rini Puji Astutik [3)]
Teknik Elektro, Fakultas Teknik, Universitas Muhammadiyah Gresik, Sumatera 101 GKB Gresik.
Galeh0510@gmail.com, *[2]den2mas@umg.ac.id*, *[3]rini puji astutik@umg.ac.id*

ABSTRAK

Ruang server merupakan ruang yang menyimpan aset-aset dan data-data penting dari suatu perusahaan sehingga keamanan untuk akses keluar masuk ruang server perlu diperhatikan agar menghindari kejadian yang tidak diinginkan. Pada saat ini sudah banyak dikembangkan sistem keamanan hingga kunci konvensional, RFID, serta sistem keamanan menggunakan teknologi biometrik seperti sidik jari, iris, dan juga wajah yang memiliki karakteristik berbeda setiap wajahnya sehingga diharapkan bisa menjadi sistem keamanan yang handal. Seiring berkembangnya teknologi membuat seseorang semakin mudah mengakses internet untuk mendapatkan data-data biometrik seperti wajah yang dapat di gunakan untuk pemalsuan atau spoofing untuk mendapatkan akses ilegal ke suatu ruangan. Penelitian sistem keamanan ini menggunakan pegenalan wajah (*face recognition*) dan *liveness* sebagai anti-spoofing dan metode *Local Binary Pattern* dan *Convolution Neural Network* untuk meningkatkan sistem keamanan agar terhindar dari pemalsuan wajah. Hasil penelitian ini mendapatkan keakuratan pendeteksian wajah asli atau palsu sebesar 90% dan akurasi sistem dalam mengenali wajah sebesar 93.3%. Kesalahan proses pengenalan wajah terjadi 5 kali dan kesalahan saat proses pengenalan wajah dan 2 kali saat pengenalan wajah asli, dari 4 skenario dengan 40 kali uji coba. Sistem keamanan pada penelitian ini 95% bekerja dengan baik dan sesuai dengan perencanaan

Kata Kunci : Convolution Neural Network, Face Recognition, Liveness, Metode Local Binary, Ruang Server, dan Teknologi Biometrik.

ABSTRACK

The server room is a room that stores important assets and data from a company so that security for access in and out of the server room needs to be considered in order to avoid unwanted events. Currently, many security systems have been developed to conventional locks, RFID, and security systems using biometric technology such as fingerprints, irises, and faces that have different characteristics for each face so that it is expected to be a reliable security system. As technology develops, it becomes easier for someone to access the internet to get biometric data such as faces that can be used for forgery or spoofing to gain illegal access to a room. This security system research uses face recognition and liveness as anti-spoofing and Local Binary Pattern and Convolution Neural Network methods to improve the security system to avoid facial forgery. The results of this study get the accuracy of detecting real or fake faces by 90% and the accuracy of the system in recognizing faces by 93.3%. Errors in the face recognition process occurred 5 times and errors during the face recognition process and 2 times during the original face recognition, from 4 scenarios with 40 trials. The security system in this study is 95% working well and in accordance with the planning.

Keywords: *Convolution Neural Network, Face Recognition, Liveness, Local Binary Method, RuangServer, and Biometric Technology.*

Diterima Redaksi : 03-12-2021 | Selesai Revisi : 14-12-2021 | Diterbitkan Online : 31-12-2021

PENDAHULUAN

Dalam perkembangan teknologi sekarang ini, sistem keamanan ruangan dituntut ketingkat yanglebih tinggi, terutama pada ruangan server yang menyimpan data ataupun aset penting dalam sebuah perusahaan ataupun instansi yang sekarang masih menggunakan pengaman ruangan konvensional, dimana masih banyak celah untuk masuknya orang yang tidak bertanggung jawab. Telah banyak dikembangkan sebuah sistem pengamanan akses masuk ke sebuah ruangan dengan beberapa verifikasi identitas seperti dengan menggunakan kunci, kartu, *password*, dan lain sebagainya. Namun, karena keterbatasan manusia dalam mengingat benda dan kombinasi angka maka metode ini dirasa kurang efektif. Pengembangan teknologi biometrik yang memanfaatkan karakteristik khususmanusia dalam mengidentifikasi atau memverifikasi dianggap lebih handal [1].

Penggunaan teknologi biometrik sangat cocokuntuk diimplementasikan pada sistem identifikasi yang membutuhkan keamanan yang tinggi. Teknologi biometrik merupakan teknologi yang memanfaatkan karakteristik fisik atau perilaku tertentu dari seseorang manusia, seperti menggunakan identifikasi sidik jari, pola wajah dan suara. Semua teknologi ini juga sudah banyak dikembangkan dalam berbagai aplikasi seperti absensi dan sistem keamanan. Dalam penelitian ini penulis menggunakan wajah sebagai teknologi *face recognition* karena wajah merupakan bagian tubuh yang susah di duplikat maupun di manipulasi [2].

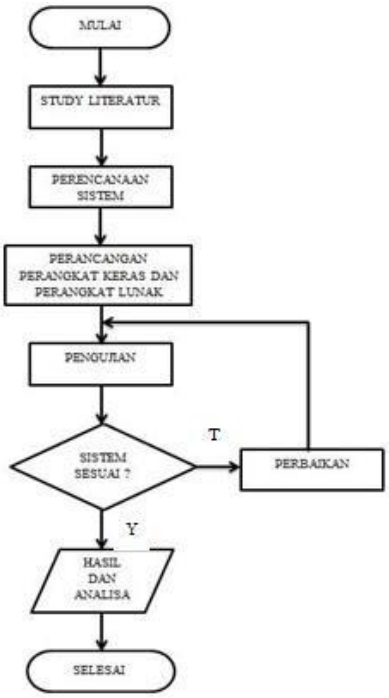
Sudah banyak dikembangkan sistem keamanan yang mengimplementasikan identifikasi menggunakan citra wajah, namun dengan berkembangnya teknologi internet mempermudahseseorang untuk mendapatkan foto atau video orang lain yang dapat digunakan untuk pemalsuan wajah atau *spoofing* dengan tujuan mendapatkan akses ilegal ke suatu ruangan yang membuat sistem keamanan *face recognition* masih memiliki kerentanan terhadap penyusup atau orang yang tidak bertanggung jawab [3].

Berdasarkan hasil penelitian ini, penulis mengusulkan penerapan teknologi biometrik anti-*spoofing* wajah untuk meningkatkan sistem kemanan pada ruang *server*.

METODE PENELITIAN

Metode dan prosedur penyelesaian masalah yang digunakan dalam penelitian ini sebagaimana ditunjukkan pada bagan alir berikut:

Diterima Redaksi : 03-12-2021 | Selesai Revisi : 14-12-2021 | Diterbitkan Online : 31-12-2021



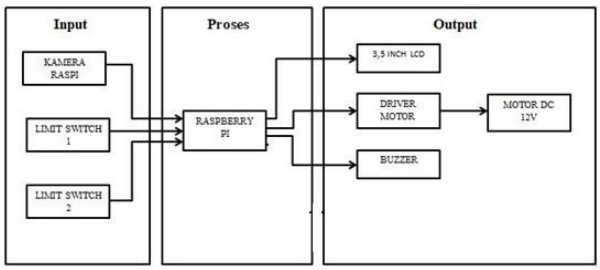
Gambar 2.1 *Flowchart* Penelitian

2.1 Studi Literatur

Sebagai bahan acuan dan pertimbangan pada perancangan alat ini, maka dilakukan proses pengumpulan referensi dan teori yang bersumber dari diskusi atau konsultasi dengan dosen, jurnal, internet, buku, dan penelitian-penelitian terdahulu yang relevan.

2.2 Perancangan Sistem

Desain rancangan sistem keamanan ruang server menggunakan *face recognition* digambarkan pada gambar berikut :



Gambar 2.2 Blok Diagram Sistem

Dari blok diagram di atas, perencanaan dan perancangan *prototype* sistem ini dibagi menjadi beberapa bagian utama:

1. Bagian Input

   Pada bagian ini terdapat sebuah kamera sebagai sensor utama untuk mengambil citra wajah. Terdapat juga dua buah *limit sitch* yang diletakkan pada bagian ujung kanan dan kiri pintu sebagai penanda bahwa pintu sudah tertutup atau sudah terbuka.

2. Bagian Proses

   Pada bagian proses menggunakan mini komputer raspberry pi dan program *phyton* agar dapat memproses data yang diterima dari sensorkamera sebagai input. Raspberry pi akan mengolah data yang diterima untuk dapat diteruskan ke *python* untuk ditampilkan pada layar LCD, sedangkan *python* akan memberikan perintah kepada raspberry pi untuk melakukan proses *face detection* dan *face recognition.*

3. Bagian Output

   Bagian *output* merupakan hasil dari pengolahan data dari inputan yang sudah diproses. Pada bagian *output* terdapat sebuah layar LCD berwarna yang akan difungsikan sebagai layar *interface* yang dapat menampilkan gambar dari kamera secara *realtime.* Motor DC yang dikontrol oleh

Diterima Redaksi : 03-12-2021 | Selesai Revisi : 14-12-2021 | Diterbitkan Online : 31-12-2021

motor driver akan digunakan untuk menggerakan pintu geser agar dapat terbuka dan tertutup secara otomatis saat mendeteksi wajah orang yang dikenali dan diizinkan untuk memasuki ruangan. Output *buzzer* digunakan sebagai verifikator yang akan mengeluarkan bunyi berbeda ketika kamera mendeteksi wajah orang yang dikenali dan tidak dikenali.

2.3 Perancangan *Hardware*

Perancangan hardware dibagi menjadi dua yaitu perancangan mekanik yang berupa miniatur pintu ruang server dan perancangan sistem sistem elektronik.

1. Perancangan Mekanik

Rancangan mekanik yang digunakan pada sistem ini berupa miniatur pintu geser yang berfungsi sebagai pintu keluar dan pintu masuk, *miniature* pintu geser ini terbuat dari bahan akrilik yang dihubungkan dengan sabuk yang digerakan dengan motor. Di ujung miniatur pintu geser dipasang *limit switch* satu yang berfungsi untuk mengetahui bahwa pintu terbuka dan motor berhenti, di ujung lainnya dipasang limit switch dua yang berfungsi untuk mengetahui pintu telah tertutup dan motor akan berhenti. Miniatur memiliki ukuran panjang 30 cm, lebar 15 cm dan tinggi 21 cm serta memiliki ukuran pintu dengan panjang 8 cm, tinggi 15 cm.

2. Perancangan Elektronik

Berdasarkan blok diagram pada gambar 2.1 diketahui bahwa sistem ini bekerja menggunakan *mini computer* raspberry pi 3 b+ yang diberikan tegangan sebesar 5Vsebagai unit proses. Sedangkan sebagai input pengambilan citra digital digunakan modul kamera raspi rev 1.3 yang memiliki resolusi sebesar 5 mega *pixel* serta mampu untuk merekam video dengan resolusi 720pdan 1080p. Modul kamera ini dihubungkan dengan menggunakan kabel fleksibel 15 pin ke *port* CSI yang ada di raspberry pi 3 b+.

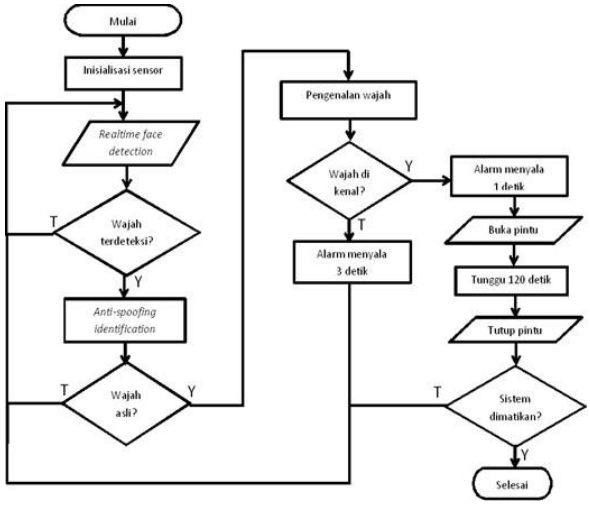
2.4 Perancangan *Software*

Pada *prototype* sistem ini digunakan perangkat lunak *LxTerminal* dan pengolahan citra. Aplikasi yang digunakan adalah aplikasi *python* yang dikomplikasikan dengan *Tensoflow Lite* dengan bantuan *image processing toolbox* yang sudah tersedia.

Dalam pemrosesan citra, *prototype* ini dapat mengenali wajah seseorang yang memiliki izin untuk mengakses ruangan *server* atau tidak dizinkan. Proses ini akan dilakukan oleh program *anti-spoofing* dan *face recognition*, dimana citra wajah yang terdeteksi akan di bandingkan dengan datasheet agar diketahui

Diterima Redaksi : 03-12-2021 | Selesai Revisi : 14-12-2021 | Diterbitkan Online : 31-12-2021

wajah asli serta dikenali.



Gambar 2.3 *Flowchart* Sistem Penerapan

Liveness Sebagai *Anti-Spoofing* Citra Digital Pada Sistem Keamanan Akses Kontrol Ruang Server Berbasis Raspberry Pi.

2.5 Rencana Pengujian Alat

Pengujian *prototype* sistem keamanan pengenalan wajah ini akan dilakukan terhadap kemampuan sistem dalam mengenali dan membedakan citra wajah asli atau palsu sehingga memutuskan seseorang mendapatkan hak akses. Kemudian juga akan dilakukan pengujian secara mekanisme pintu geser.

Berikut tahapan untukpengujian alat:

1. Pengujian Deteksi Wajah Asli

   Pengujian deteksi wajah asli pada sistem ini menggunakan citra objek wajah asli, foto atau gambar wajah, serta video wajah seseorang di depan input kamera yang kemudian akan diteruskan ke sistem pemroses raspberry pi, kemudian akan di lakukan pencocokan kesesuaian antara input objek dengan data hasil pembacaan dari sistem.

2. Pengujian Pengenalan Wajah dan Hak Akses Pengujian pengenalan wajah dan hak akses ini

   bertujuan untuk mengetahui apakah sistem dapat mengenali citra wajah yang sudah didaftarkan dan memberikan perintah ke output pintu, pada tahap ini akan dilakukan pengujian dengan beberapa citra wajah seseorang yang diberikan izin dan tidak diberikan izin.

3. Pengujian Mekanisme Pintu Geser

   Pada pengujian ini dilakukan pengujian kehandalan motor DC untuk membuka pintu saat terdeteksi wajah orang yang dikenali lalu dan menutup kembali, serta dilakukan pengujian input *limit switch* yang diletakan pada kedua sisi ujung pintu dalam menentukan arah putaran motor DC.

4. Pengujian Sistem Keseluruhan

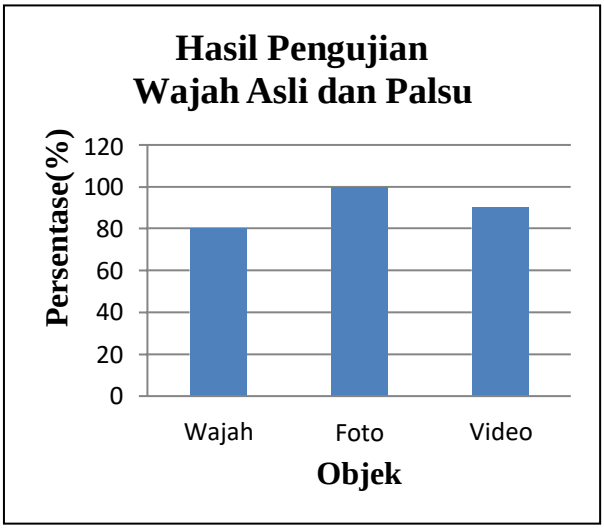
   Dalam proses pengujian sistem secara keseluruhan akan di buat beberapa skenario uji. Diantaranya yaitu pengujian sistem terhadap citra wajah yang dikenali menggunakan objek foto atau gambar, pengujian sistem terhadap citra wajah yang dikenali menggunkan objek video,

Diterima Redaksi : 03-12-2021 | Selesai Revisi : 14-12-2021 | Diterbitkan Online : 31-12-2021

pengujian kehandalan pintu geser membuka pintu ketika ada wajah asli dan dikenali, dan pengujian alarm *buzzer*ketika mendektesi wajah palsu.

HASIL DAN PEMBAHASAN

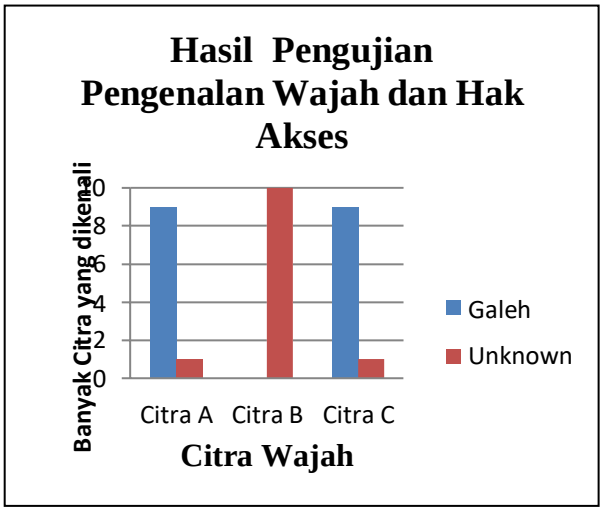
Pengujian wajah asli dan palsu ini dilakukandengan memberikan tiga objek di depan kamera yaitu objek wajah asli, video serta gambar/foto sebanyak 10kali sampling per objek. Berikut ini hasil pengujian wajah asli dan palsu.



Gambar 3.1 Diagram Pengujian Wajah Asli dan Palsu

Hasil pengujian deteksi keaslian wajah yang telah dilakukan didapatkan keakuratan sistem 90%.Terdapat tiga citra digital atau 10% dari 30 sampel tidak sesuai.

Pengujian pengenalan wajah dan hak aksesdilakukan menggunakan tiga citra wajah, yaitu citra A atau wajah orang yang sudah terdaftar, citra B atau wajah orang yang tidak didaftarkan dan citra C atau wajah orang yang sudah terdaftar namun mengalami pergeseran data. Berikut ini menunjukkan hasil dari pengujian pengenalan wajah dan hak akses wajah yang sesuai dengan dataset sebanyak 10 kali setiap citra wajah
digital.

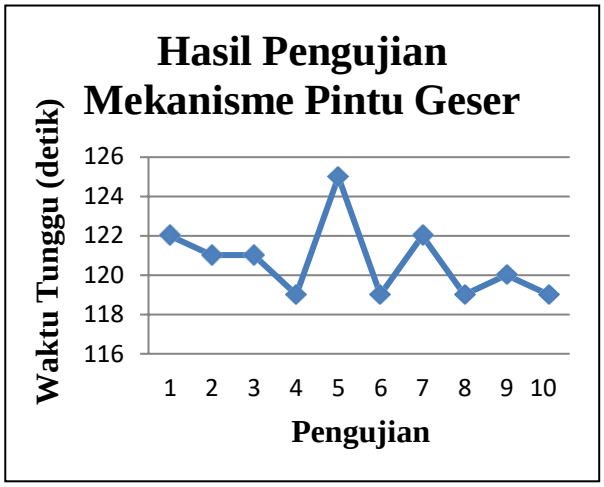


Gambar 3.2 Diagram Hasil Pengujian Pengenalan Wajah dan Hak Akses

Hasil pengujian yang telah dilakukan didapatkan akurasi sistem dalam mengenali wajah sebesar 93,3%. Terdapat 16,7% atau 2 dari 30 citra data yang ada tidak sesuai dalam pencocokannya.

Diterima Redaksi : 03-12-2021 | Selesai Revisi : 14-12-2021 | Diterbitkan Online : 31-12-2021

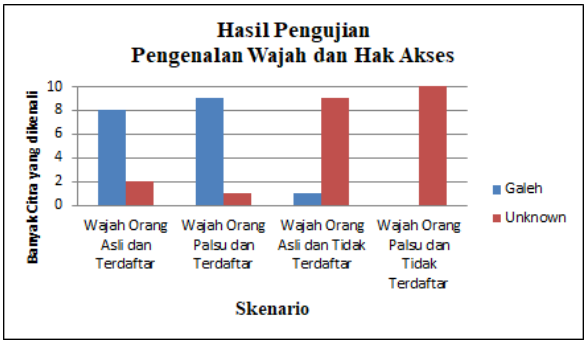
Hasil pengujian mekanisme pintu geser dilakukan dengan cara mencoba kesesuaian mekanisme pintu geser ketika terdeteksi wajah orang yang diizinkan. Pengujian dilakukan sebanyak 10 kali ulangan, berikut ini hasil pengujian mekanisme pintu geser.



Gambar 3.3 Diagram Hasil Pengujian Mekanisme Pintu Geser

Hasil uji coba mekanisme pintu geser dapat diketahui bahwa mekanisme pintu geser sudah sesuai dengan perencanaan namun memiliki waktu tunggu yang berbeda-beda dengan rata-rata nilai tunggu 120,7 detik dengan waktu tunggu tercepat adalah 119 detik dan waktu terlama adalah 125 detik.

Pengujian pengenalan wajah dan hak akses dilakukan 10 kali ulangan pada masing-masing skenario untuk menguji ketepatan sistem dalam mencocokkan data citra wajah. yang diambil dengan hak akses yang diberikan. Hak akses diberikan ketika sistem mengenali sebagai wajah asli dan sudah terdaftar sebelumnya.



Gambar 3.4 Diagram Hasil Pengujian Pengenalan Wajah dan Hak Akses

Hasil pengujian menunjukkan telah terjadi lima kali kesalahan pada saat proses pengenalan wajah dan dua kali saat pengenalan wajah asli. Secara keseluruhan dapat disimpulkan bahwa sistem bekerja dengan baik dan sesui dengan prosedur, keberhasilan diatas 95%. Terdapat 2 kali sistem yang tidak sesuai dengan empat skenario yang diharapkan dari 40 kali uji coba.

KESIMPULAN

Berdasarkan hasil perancangan, pembuatan, dan pengujian alat yang dilakukan dengan cara keseluruhan sistem dapat disimpulkan sebagai berikut:

1. Untuk meningkatkan sistem keamanan agar

Diterima Redaksi : 03-12-2021 | Selesai Revisi : 14-12-2021 | Diterbitkan Online : 31-12-2021

terhindar dari pemalsuan wajah, bisa dilakukan dengan cara menerapkan sistem *anti spoofing* dengan menggunakan metode *Local Binary Pattern* dan *Convolution Neural Network*

2. Penggunaan metode *Local Binary Pattern* dan *Convolution Neural Network* memiliki keakuratan pendeteksian wajah asli dan palsu sebesar 90% dan akurasisistem dalam mengenali wajah sebesar 93,3%.
3. Hasil pengujian hanya terjadi 5 kali kesalahan saat proses pengenalan wajah dan 2 kali saat pengenalan wajah asli, dari 4 skenario dengan 40 kali uji coba. Sehingga sebesar 95% sistem bekerja dengan baik dan sesuai dengan perencanaan.

SARAN

Proses penulisan karya ilmiah ini masih banyak mengandung kekurangan baik perbagian ataupun pada saat integrasi sistem, sehingga diperlukan beberapa hal untuk memperbaiki kekurangan dan kesalahan dari alat ini kedepannya. Saran – saran yang diperlukan di antara nya:

1. Penggunaan hardware yang memiliki spesifikasi lebih tinggi, dikarenakan dengan menggunakan raspberry pi 3 b+ memiliki kekurangan yaitu turunnya fps.
2. Dalam pendaftaran user, diperlukan pencahayaan yang terang agar di dapat hasil pengenalan yang lebih akurat.

DAFTAR PUSTAKA

[1] Muhannad, Fadel. 2018. "Sistem Keamanan Pintu Masuk Menggunakan Face Recognition Berbasis Raspberry Pi. Skripsi dipublikasikan. Makasar: Universitas Hasanuddin".

[2] Sudarma, Made, dkk. 2016. "Aplikasi Verifikasi Wajah Untuk Absensi Pada Platform Android Dengan Menggunakan Algoritma Fisherface". Teknologi Elektro. Vol. 15, No. 2.

[3] Sujaini, Herry. 2005. "Aplikasi Sistem Keamanan Dengan Pengolahan Citra Dan SMS". *SNATI 200*.

[4] Rakhman Edi, Candrasyah Faisal, D.sutera Fajar.
2014. Raspberry Pi Mikrokontroler Mungil yang Serba Bisa. Yogyakarta: Penerbit Andi.

[5] Dinata, Andi. 2017. Physical Computing dengan Raspberry Pi. Jakarta : PT Elex Media Komputindo.

[6] Musa Purnawarman, Nuryuliani, Missa Lamsani. 2012. Rancang Bangun Pengendalian Pintu Automatis Berdasarkan Ciri Wajah Menggunakan Metode Euclidean Distance Dan Fuzzy C-Mean. Depok: Repository Gunadarma

[7] Basuki Achmad, Jozua F. Palandi, dan

Diterima Redaksi : 03-12-2021 | Selesai Revisi : 14-12-2021 | Diterbitkan Online : 31-12-2021

Fathurrochman. 2005. Pengolahan Citra Digital Menggunakan Visual Basic. Bandung: Graha Ilmu.

Diterima Redaksi : 03-12-2021 | Selesai Revisi : 14-12-2021 | Diterbitkan Online : 31-12-2021