

# Aplikasi Pengenalan Wajah Menggunakan Teknik CBIR untuk Objek Tampak Depan

Sri karnila<sup>1</sup>, Rio Kurniawan<sup>2</sup>, Sri Lestari<sup>3</sup>, Suhendro Y. Irianto<sup>4</sup>

<sup>1</sup>Jurusan Sistem Informasi, Informatics & Business, Institut Darmajaya  
<sup>2,3,4</sup>Jurusan Teknik Informatika, Informatics & Business, Institut Darmajaya  
Email: <sup>1</sup>srikarnila\_dj@ darmajaya.ac.id, <sup>2</sup>riokurniawan@ darmajaya.ac.id,  
<sup>3</sup>t4ry@gmail.com, <sup>4</sup>suhendro@ darmajaya.ac.id

## Abstrak

Penelitian ini ditujukan untuk membuat sistem keamanan cerdas (*Intelligent Security System*) berbasis pengenalan wajah atau sering dikenal dengan *face recognition*. Data yang digunakan adalah data gambar wajah tampak depan, bukan tampak samping atau belakang. Dengan menggunakan citra wajah yang tidak ada penghalang (*obstacles*) dan wajah dengan *obstacles*. Data gambar wajah di simpan dalam *database* berbasis objek *file* melewati proses identifikasi dan pengenalan wajah kemudian melakukan *retrival* wajah menggunakan teknik *similarity* wajah dengan *Content Based Image Retrieval*, pada tahap identifikasi wajah, aplikasi dapat menentukan secara spesifik bentuk wajah depan, pada tahap *recognition*, dilakukan *ekstraksi fitur*, berjalan secara cerdas *similarity* (mencocokkan data wajah) yang akan membuka pintu, sehingga dapat digunakan untuk meminimalkan terjadinya kriminalitas yang terjadi saat ini. Sistem ini dapat digunakan untuk pengamanan pintu rumah, pintu ruang di kantor, pintu gerbang, *gate-gate* di *airport*, berbasis pengenalan wajah.

**Kata Kunci:** *Intelligent system, security, face recognition, CBIR*

## Abstract

*This research is purposed to construct an intelligent security system based on face recognition. The data used in this research are frontal face images and without obstacles, and facial images with obstacles. Facial image data are stored in the database object-based files through process of identification and facial recognition. Consequently, facial images are retrieved using facial similarity techniques with Content Based Image Retrieval. In this stage of identification, an application can specify shape of the front face, performs feature extraction, and running intelligently Similarity (matching face data) which open the door automatically. This system be used to minimize the occurrence of criminality occurs nowadays. This system can be used such as for house door security, office doors, and airport gates based face recognition.*

**Keyword:** *Intelligent system, Security, face recognition, CBIR*

## 1. PENDAHULUAN

Pengembangan teknik pengenalan wajah atau *face recognition* cukup sulit karena wajah manusia sangat kompleks, multidimensi, dan sering berubah sesuai dengan perubahan lingkungan dan situasi. Oleh karena itu, pembuatan sistem otomatis pengenalan wajah dan atau ekspresi wajah merupakan tantangan bagi para ahli sampai dengan saat ini. *Biometrics* merupakan teknologi pengenalan diri dengan menggunakan bagian tubuh atau perilaku manusia. Contohnya yaitu dengan pengenalan sidik jari, retina, iris, pola dari wajah [1]. Salah satu ciri *biometric* yang paling banyak digunakan dalam penelitian-penelitian selama ini adalah ciri wajah (*face*) seperti untuk *face detection* dan *face recognition* [7].

Sementara itu Arulogun [2] menyatakan bahwa *face recognition systems* atau sistem pengenalan wajah telah diperkenalkan hampir 50 tahun yang lalu, pengenalan wajah merupakan satu cabang dari bidang *pattern recognition* dan *computer vision*. *Face recognition* juga merupakan salah cabang dari sifat *biometrics* manusia [8].

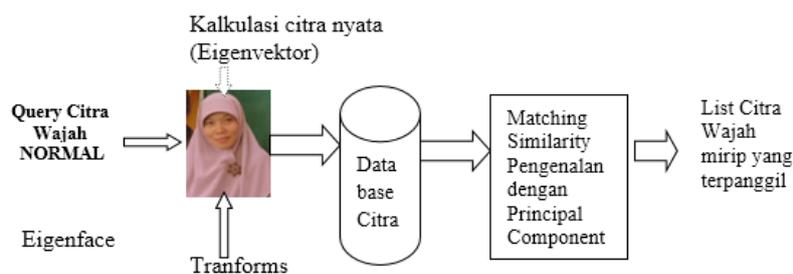
Semakin tingginya angka kriminalitas dan pencurian yang terjadi saat ini, menyebabkan sistem keamanan menjadi kebutuhan yang mutlak untuk diterapkan, untuk itu dibutuhkan suatu perangkat sistem keamanan

yang dapat menjaga *full time* untuk melindungi aset dan privasi yang kita miliki. Sehingga diharapkan dengan aplikasi sistem keamanan tersebut dapat memberikan rasa aman dan nyaman untuk kita, selain hal tersebut tentunya dengan aplikasi sistem keamanan maka dapat menekan angka kriminalitas yang terjadi di masyarakat baik pencurian maupun kejahatan yang lain.

Pintu menjadi hal yang paling penting dalam sistem keamanan rumah, perusahaan, dan kantor-kantor pemerintah, dan gedung-gedung penting lainnya hal ini karena fungsi pintu sebagai akses utama untuk masuk. Adanya pemasangan sistem keamanan pada pintu tersebut merupakan suatu bentuk otomatisasi sebagai dampak positif dari perkembangan teknologi. Dengan otomatisasi tersebut maka peran manusia akan digantikan oleh suatu alat atau mesin, karena pada dasarnya pintu gerbang akan terbuka sendiri jika *password* yang dimasukkan benar sehingga diharapkan nantinya setiap pintu tidak harus dijaga terus-menerus oleh manusia karena sistem ini juga telah dilengkapi dengan alarm yang akan berbunyi jika pintu dibuka secara paksa sistem cerdas yang akan dibangun dalam penelitian ini adalah dengan menggunakan metode *Content Based Image Retrieval*. Sistem cerdas ini ditargetkan untuk menggantikan sistem pengamanan konvensional yang berbasis teks yang sangat mudah untuk “di-hack” oleh orang yang tidak berhak.

## 2. METODE

Metode pada penelitian ini menggunakan model *waterfall*, yang mencakup tahapan *system requirement, analysis, design, implementasi, testing, dan maintenance*. Sementara itu untuk model Proses Sistem yang akan diusulkan digambarkan dalam bentuk model *SDLC* dan *flowchart general process*. Tahapan *analysis* dilakukan untuk mengetahui permasalahan yang terjadi yaitu, pentingnya *pengamanan* otomatis pada pintu dengan mengenali wajah melalui teknik *Content Based Image Retrieval* (CBIR). Desain sistem secara umum digambarkan pada gambar sistem pengenalan wajah tanpa penghalang diilustrasikan dengan bentuk sistem yang dijelaskan pada Gambar 1.



Gambar 1. Sistem pengenalan wajah tanpa penghalang

### 2.1. Metode atau Teknik *Matching Image*

Pendekatan *Eigenfaces* dilakukan untuk ekstraksi fitur-fitur vektor yang nantinya akan kita gunakan untuk mengklasifikasikan *generating pattern* wajah. Secara sederhana *Eigenfaces* mempunyai prosedur sebagai berikut:

- 1). Pertama diasumsikan bahwa citra wajah latihan (*training set images*) adalah  $I_1, I_2, I_3, \dots, I_n$ . Di mana setiap citra wajah mempunyai dimensi  $I(x, y)$ , kemudian setiap citra wajah dikonversi menjadi vektor yang mempunyai matriks  $(m \times p)$ , dan  $m$  merupakan jumlah dari citra wajah latihan sedangkan  $p$  adalah  $p \times y$ .
- 2). Setelah itu hitung *Mean* atau rata dari matriks wajah.
- 3). Setelah itu hitung setiap matriks wajah dengan *Mean*.

- 4). Setelah itu dikerjakan transformasi matriks, sehingga vektor matriks akan berkurang. Kemudian dihitung *Eigenvektor* dan *Eigenvalues* sehingga berdasarkan *egigenfaces* ini setiap citra akan mempunyai vektor wajah.
- 5). Akhirnya citra wajah akan dapat direkayasa atau dibentuk dengan vektor masing-masing dan vektor-vektor sebelumnya.

## 2.2. Kemiripan

Untuk menghitung kemiripan (*similarity*) antara citra *query* dengan citra wajah yang ada dalam *database* secara langsung diperlukan algoritma yang kompleks dan proses yang cukup lama. Untuk mengatasi masalah ini, maka dalam penelitian ini dilakukan tiga tahapan dalam *matching* citra wajah. Pertama mencari kemiripan topologi dari wajah *query* dengan wajah dalam *database* yang merupakan filter, kedua penggunaan informasi untuk memperbaiki calon citra wajah yang akan terpanggil, dan akhirnya metoda penghitungan *matching* dikerjakan untuk menentukan kemiripan (*similarity*) antara citra *query* dengan citra wajah yang ada dalam *database*.

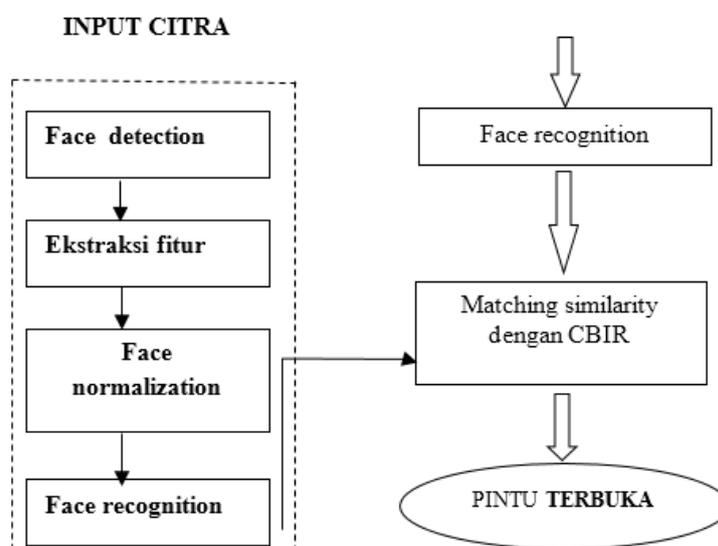
Sementara itu untuk mengukur efektivitas dari pencarian gambar dengan menggunakan *precision* dan *recall*, *precision* adalah jumlah citra yang mirip yang terpanggil dibagi dengan semua citra yang terpanggil (*retrieved*). Sedang *recall* adalah jumlah citra yang terpanggil dibagi dengan jumlah citra yang dalam kategori [3].

$$p = \frac{a}{z} \quad r = \frac{b}{y} \quad (1)$$

Dimana  $p$  adalah *precision* dan  $r$  adalah *recall*, sementara  $a$  adalah jumlah citra yang relevan atau mirip terpanggil,  $z$  adalah jumlah semua citra yang terpanggil, dan  $y$  jumlah citra relevan yang ada dalam *database*.

## 3. HASIL DAN PEMBAHASAN

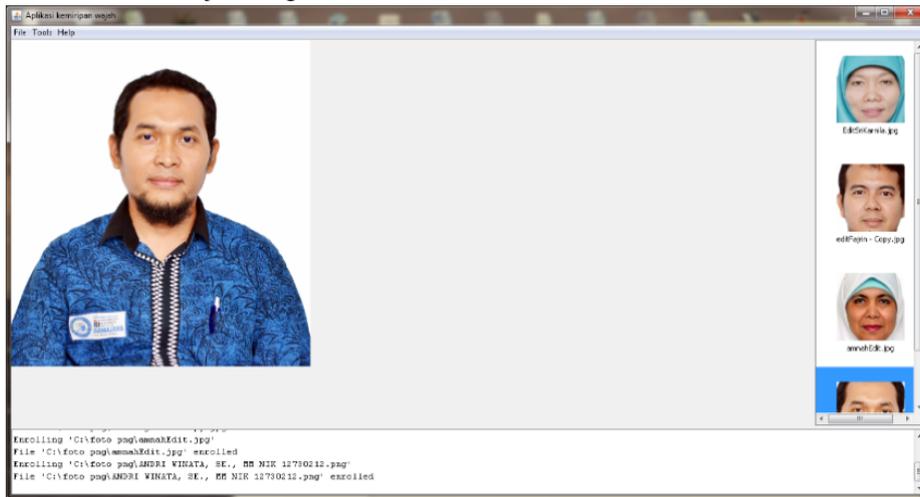
*Algoritma face recognition* untuk aplikasi pengenalan wajah mulai dari gambar wajah yang terekstraksi dan tersimpan dalam *database* sebagai keamanan pintu menggunakan teknik CBIR dijelaskan pada Gambar 2.



Gambar 2. Sistem *face recognition* untuk pembuka pintu dengan teknik CBIR

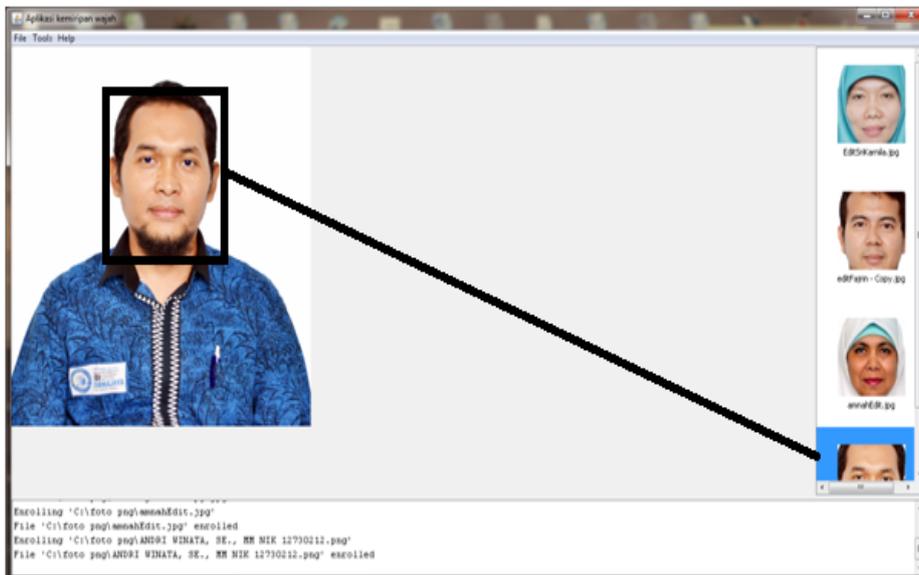
### 3.1. Tampilan aplikasi face recognition

Pengenalan wajah normal atau wajah tanpa penghalang diilustrasikan dengan Gambar 3 dan Gambar 4 untuk wajah dengan *obstacles*.



**Gambar 3.** Gambar pengenalan wajah normal

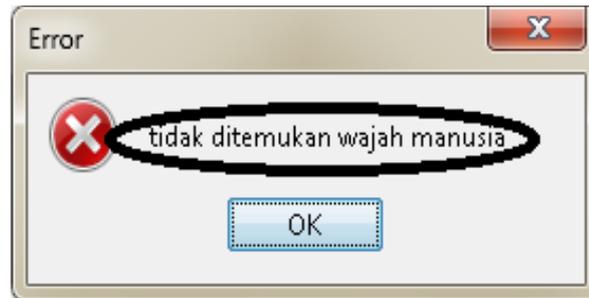
Gambar yang tersimpan dalam *database* adalah gambar tampak depan dan tanpa penghalang. Data gambar yang terdeteksi *similarity* maka pintu akan terbuka.



**Gambar 4.** Gambar pengenalan wajah normal *similarity*

## 4. SIMPULAN

Aplikasi dapat mengenali wajah menggunakan teknik CBIR Sistem cerdas yang dibangun adalah dengan menggunakan metode *Content Based Image Retrieval* dan *Real Time Face Recognition*. Dari desain dan aplikasi yang dibuat cukup baik dimana deteksi wajah dapat dikerjakan dengan akurasi tinggi. Jika wajah tidak ada didalam *database* maka aplikasi memberi *warning* 'tidak ditemukan wajah manusia, begitu sebaliknya jika ditemukan selain wajah manusia, dan informasi tentang gambar wajah orang tersebut ditampilkan jika dikenali atau *similarity* atau data wajah cocok seperti Gambar 5.



**Gambar 5.** Validasi *input data image*

Proses pengecekan *matching* data pada *image retrieval* dengan cara mencari nilai *similarity* pada *database content* yang sudah di sediakan melalui proses *input* wajah pada *database content*.

## 5. REFERENSI

- [1] Anil K.J., Arun, R., Salil, P. 2004. An Introduction to Biometric Recognition. *IEEE Transactions on Circuits and Systems for Video Technology*. Vol. 14(1): 4-20.
- [2] Arulogun, T., Omidiora, E., Olaniyi, O.M., Ipadeola, A.A. Development of Security System using Facial Recognition. *The Pacific Journal of Science and Technology*. Vol. 9(2): 377-385.
- [3] Debnath, B., Rahul, R., Farkhod, A.A., Minkyu C. 2013. Biometric Authentication: A Review. *International Journal of u- and e- Service, Science and Technology*. Vol. 2(3): 13-27.
- [4] Irianto, Y., Suhendro, Zaini, T.M., Sri, K. 2013. Face Image Retrieval Approach for Criminal Identification in the DC Domain. *World Academy of Science, Engineering and Technology*. Vol. 82: 1480-1483.
- [5] Irianto, Y., Suhendro. 2009. Keyword And Image Content Features For Image Indexing And Retrieval Within Compressed Domain. *Jurnal Informatika*. Vol. 10(2): 73-78.
- [6] Irianto, Y., Suhendro. 2013. Segmentation for Image Indexing and Retrieval on Discrete Cosines Domain. *Jurnal TELKOMNIKA*. Vol. 11(1): 119-126.
- [7] Kwok-Wai, W., Kin-Man, L., Wan-Chi, S. 2002. An efficient algorithm for human face detection and facial feature extraction under different conditions. *Pattern recognition*. Vol. 34(10): 1993-2004
- [8] Xizho, Z., Yuwen, X., Jifeng, D., Lu, Y., Yichen, W. 2017. Deep Feature Flow for Video Recognition, *arXiv*. 2349-2358.