

BAB 1

PENDAHULUAN

1.1 Latar Belakang Masalah

Seiring perkembangan teknologi yang semakin pesat, sistem keamanan menjadi aspek penting yang harus diperhatikan. Sistem keamanan ini berfungsi untuk melindungi sistem digital dari penyadapan informasi, pencurian, atau kerusakan pada perangkat keras, perangkat lunak, atau data elektronik seseorang. Sistem keamanan yang melemah dapat menimbulkan banyak masalah, salah satunya adalah kebocoran data. Kasus kebocoran data yang berdampak besar di Indonesia pernah terjadi pada Maret 2020 lalu, dimana data pengguna Tokopedia sebanyak 91 juta data diretas dan dijual pada situs *darkweb* [1]. Selain itu, berdasarkan data yang diambil dari *website* Surfshark pada tahun 2022, Indonesia menempati peringkat ke-8 dengan kebocoran data terbanyak di dunia [2]. Maka dari itu, sistem keamanan digital harus terus dikembangkan seiring dengan perkembangan teknologi saat ini.

Pada masa teknologi sekarang ini, telah banyak aktivitas manusia sehari-hari yang berhubungan dengan data pribadi, keuangan, pekerjaan, dan aktivitas lainnya yang menggunakan akses sistem komputer untuk menjalankannya. Data-data ini tentunya memerlukan sistem keamanan yang baik sehingga tidak disalahgunakan oleh orang lain. Biasanya, data-data ini akan disimpan menggunakan *password* yang hanya diketahui oleh pemiliknya. Namun sayangnya, dengan perkembangan teknologi yang sangat pesat membuat sistem keamanan menggunakan *password* menjadi semakin rentan.

Dalam upaya memaksimalkan sistem keamanan, kecerdasan buatan ikut digunakan sebagai salah satu basis sistem keamanan yang lebih baik. Sistem keamanan dengan kecerdasan buatan biasanya menggunakan biometrik karena memiliki ciri yang tidak dapat ditiru dan unik untuk setiap individu. Salah satu biometrik yang dapat digunakan sebagai sistem keamanan adalah wajah. Mengenali wajah seseorang merupakan suatu hal yang mudah dilakukan oleh manusia. Biasanya seseorang akan cepat untuk mengenal, menghafal, dan membedakan wajah orang lain dengan ekspresi yang berbeda-beda. Namun hal ini tidak berlaku untuk komputer. Sebuah sistem perlu diberikan perlakuan khusus sehingga dapat mendeteksi wajah seseorang dan membedakannya dengan wajah orang lain.

Terdapat beberapa metode pengenalan wajah berbasis kecerdasan buatan yang telah digunakan saat ini. Salah satunya adalah CNN (*Convolutional Neural Network*) seperti yang digunakan pada penelitian tahun 2023 [3]. Penelitian ini menggunakan CNN untuk melakukan pengenalan wajah dan pengenalan ekspresi wajah. Pengujian pada penelitian ini juga dilakukan dengan menggunakan citra seseorang dengan dan tanpa kacamata dimana penelitian ini berhasil melakukan pengenalan wajah dengan akurasi sebesar 94%. Metode lainnya yang juga digunakan dalam melakukan pengenalan wajah adalah metode *triangle face* seperti yang dilakukan pada penelitian tahun 2022 [4]. Penelitian ini menggunakan metode *triangle face* untuk melakukan pengenalan wajah dengan tingkat akurasi mencapai hingga 99%. Berdasarkan kedua penelitian tersebut, peneliti memutuskan untuk menggunakan metode *triangle face* karena memiliki tingkat akurasi yang lebih baik dari CNN. *Triangle face* adalah metode yang mendeteksi fitur-fitur pada wajah seseorang yang membentuk segitiga, yaitu mata, hidung, dan mulut. Jarak antar fitur tersebut dihitung dan digunakan sebagai parameter untuk melakukan pengenalan wajah.

Pada tahun 2023 penelitian lain dilakukan untuk melakukan diagnosis gejala penyakit jantung berdasarkan citra dengan menggunakan metode *minkowski distance* [5]. Penelitian ini menunjukkan metode *minkowski distance* berhasil melakukan diagnosis penyakit jantung berdasarkan citra dengan sempurna, yakni dengan nilai akurasi sebesar 100%. *Minkowski distance* sendiri merupakan bentuk umum dari *euclidean distance* dan *manhattan distance* yang dapat digunakan untuk mengetahui kemiripan dua buah citra. Metode ini akan digunakan peneliti untuk membandingkan citra/gambar masukan dan citra/gambar pada *database*.

Berdasarkan masalah tersebut, peneliti tertarik untuk membuat sistem keamanan berbasis pengenalan wajah menggunakan dua metode, yaitu metode *triangle face* dan penerapan *minkowski distance* untuk melindungi data-data pribadi seseorang. Kedua metode ini digunakan karena memiliki tingkat akurasi yang cukup tinggi sehingga memiliki peluang besar untuk menciptakan sistem keamanan yang lebih baik. Sistem yang dibuat akan digunakan pada sebuah aplikasi Android untuk melakukan *login* untuk dapat mengakses data-data pribadi yang disimpan.

Pada penelitian sebelumnya dengan judul "Penerapan Minkowski Distance pada Metode Triangle Face dalam Sistem Keamanan File"[6] ditemukan bahwa sistem pengenalan wajah yang dibangun diterapkan pada aplikasi *Windows* dan dibuat untuk menyimpan data dalam bentuk *file*. Pada penelitian ini dilakukan inovasi dengan menerapkan sistem tersebut pada aplikasi *Android* dan digunakan

untuk menyimpan data-data pribadi seseorang. Selain itu, pada penelitian ini juga akan dilakukan pengembangan algoritma sehingga diharapkan dapat meningkatkan akurasi dari sistem pengenalan wajah yang dibangun.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, maka rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Bagaimana merancang dan membangun sistem yang dapat mengenali wajah seseorang menggunakan metode *triangle face* dengan penerapan *minkowski distance*?
2. Berapa tingkat akurasi sistem pengenalan wajah yang dibuat menggunakan metode *triangle face* dengan penerapan *minkowski distance*?

1.3 Batasan Permasalahan

Adapun batasan masalah pada penelitian ini adalah:

1. *Dataset* citra wajah yang digunakan diambil dari *website* Kaggle yang berisi gambar 1.680 orang dengan 2 - 50 gambar per orang.
2. Jarak kamera dan wajah minimal sebesar 20 cm.

1.4 Tujuan Penelitian

Tujuan dilakukannya penelitian ini adalah:

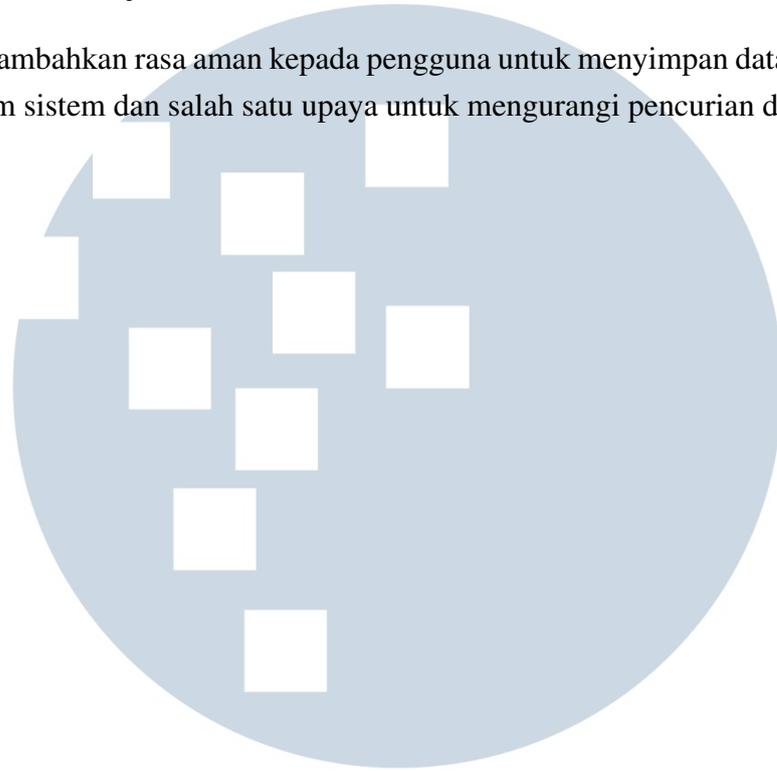
1. Membangun suatu sistem yang dapat mengenali wajah seseorang menggunakan metode *triangle face* dengan penerapan *minkowksi distance*.
2. Mengetahui tingkat akurasi sistem pengenalan wajah yang dibuat menggunakan metode *triangle face* dengan penerapan *minkowksi distance*.

1.5 Manfaat Penelitian

Manfaat penelitian ini adalah:

1. Menambah pengetahuan peneliti dalam ilmu pengolahan citra digital dan membangun aplikasi Android menggunakan bahasa pemrograman *Python*.

2. Menjadi tambahan referensi dalam mengembangkan sistem dengan pengenalan wajah untuk akses sebuah sistem.
3. Menambahkan rasa aman kepada pengguna untuk menyimpan data pribadi ke dalam sistem dan salah satu upaya untuk mengurangi pencurian data.



UMMN

UNIVERSITAS
MULTIMEDIA
NUSANTARA