BAB I
PENDAHULUAN

1.1 Latar Belakang Penelitian

Rumah adalah salah satu komponen penting dalam kehidupan manusia, serta memiliki peran penting dalam memberikan kenyamanan dan keamanan yang diidamkan oleh setiap penghuninya. Untuk mencapai tujuan ini, penghuni rumah sering kali mempercayakan keamanan rumah mereka pada kunci pintu konvensional atau analog(Frobenius dkk., 2023). Namun, kunci pintu konvensional memiliki banyak kelemahan yang dapat mengurangi efektivitasnya untuk membuka rumah itu sendiri seperti, dapat dengan mudah dibobol melalui lubang kunci, memungkinkan akses yang tidak sah oleh pihak yang berniat jahat. Selain itu, kunci konvensional pada sistem pengamanan sering kali dianggap kurang andal karena mudah hilang selama penggunaan, membuat sistem ini terasa kurang praktis dan rentan terhadap aksi pencurian (Muwardi & Adisaputro, 2021).

Human error, yang dikenal sebagai kelalaian manusia adalah pelanggaran prosedural yang terjadi secara tidak sengaja dan di luar kesadaran seseorang. Dapat menyebabkan risiko kegagalan atau kecelakaan saat menjalankan tugas (Zetli, 2021). Salah satu penyebab kelalaian manusia dalam interaksi antara manusia dan kunci rumah adalah sifat pelupa. Sifat pelupa ini dapat menyebabkan kunci terselip atau hilang, mengakibatkan kegagalan untuk masuk ke dalam rumah (Frobenius dkk., 2023). Selain itu, lupa mengunci pintu atau meninggalkan kunci pada pintu dapat mengurangi keamanan rumah. Hal ini menunjukkan bahwa sistem keamanan rumah yang mengandalkan kunci pintu konvensional masih memiliki banyak kelemahan. Dalam konteks ini, perlu adanya perkembangan teknologi yang menawarkan solusi yang lebih aman dan efisien untuk sistem keamanan pintu.

Pada masa kini, perkembangan teknologi telah dimanfaatkan secara luas, termasuk dalam penerapan keamanan pintu. Salah satu kemajuan teknologi yang sangat pesat perkambangannya, ialah teknologi pengenalan wajah menjadi trend dalam kehidupan setiap individu manusia memanfaatkan teknologi ini (Danuri, 2019). Khususnya teknologi pengenalan wajah telah mengalami perkembangan pesat dalam beberapa tahun terakhir dan terus menunjukkan pertumbuhan yang signifikan. Berdasarkan data terbaru, pasar global untuk teknologi pengenalan

wajah diperkirakan akan tumbuh dengan CAGR (*Compound Annual Growth Rate*) sebesar 14,6% dari tahun 2023 hingga 2032. Pada tahun 2022, nilai pasar ini mencapai USD 5,1 miliar dan diproyeksikan akan mencapai USD 19,3 miliar pada tahun 2032 yang disajikan pada Gambar 1.1.

Gambar 1. 1 Data Statistik Global Facial Recognition Market 2022 – 2032 (market.us, 2023)

Berdasarkan Gambar 1.1, teknologi ini semakin populer di berbagai industri, Teknologi pengenalan wajah diprediksi akan menjadi tren di masa depan. Penggunaan pengenalan wajah juga telah meluas ke berbagai sektor, seperti kontrol akses dan pengawasan keamanan, di mana sistem ini memungkinkan identifikasi individu secara cepat dan akurat. Selain itu, teknologi pengenalan wajah kini diterapkan dalam berbagai perangkat konsumen, seperti smartphone dan sistem pembayaran, serta diintegrasikan dalam infrastruktur publik untuk meningkatkan efisiensi dan keamanan. Adapun manfaat dari teknologi ini untuk kontrol akses yang dikelola secara lokal, atau dapat digunakan oleh entitas atau administrator lokal yang memiliki akses terhadap sistemnya (Nalawati dkk., 2024).

Penggunaan teknologi pengenalan wajah di dunia modern semakin meningkat. Didorong oleh kebutuhan akan sistem keamanan yang lebih canggih dan otomatisasi yang lebih luas dalam berbagai sektor. Namun juga menimbulkan beberapa ancaman serius terkait data dan privasi. Pencurian data wajah dapat

menyebabkan pelanggaran privasi yang signifikan, di mana informasi pribadi dapat disalahgunakan untuk penipuan identitas. Salah satu tantangan besar yang dihadapi adalah risiko kebocoran data. Dataset sangat penting untuk pelatihan dan pengujian model karenanya ada tidaknya data maupun kumpulan data dapat menjadi tolak ukur untuk setiap ancaman siber (Fitria & Mutijarsa, 2023). Oleh karena itu, sangat penting untuk menerapkan langkah-langkah keamanan tambahan seperti menggunakan teknik pengamanan data (S. Zhang dkk., 2021). Ancaman ini tidak hanya memengaruhi individu yang datanya dicuri, tetapi juga mengancam integritas dan keandalan sistem pengamanan secara keseluruhan. Sehingga menurunkan tingkat kepercayaan pengguna terhadap teknologi pengenalan wajah.

Maka dari itu, perlu adanya suatu sistem pintu berbasis pengenalan wajah dengan pengamanan dataset yang dapat menjamin keamanan data pribadi pengguna. Sistem ini harus dirancang dengan mekanisme perlindungan yang kuat terhadap potensi kebocoran data dan pengelolaan akses yang ketat. Dengan mengintegrasikan teknologi pengenalan wajah dengan menawarkan tingkat perlindungan yang lebih tinggi, memastikan bahwa hanya individu yang berwenang yang dapat mengakses ruang-ruang tertentu. Penerapan sistem semacam ini tidak hanya meningkatkan keamanan fisik, tetapi juga membantu membangun kepercayaan pengguna terhadap teknologi pengenalan wajah yang semakin banyak digunakan di berbagai aspek kehidupan sehari-hari. Kombinasi perangkat keras dan perangkat lunak ini memungkinkan identifikasi wajah secara real-time dan memberikan tingkat keamanan yang lebih tinggi dalam sistem penguncian pintu (Zhu & Cheng, 2020).

Fokus penelitian ini adalah mengimplementasikan algoritma LBP untuk pengenalan wajah dan mengombinasikannya dengan teknik *encoding* Base64 *Shuffle* untuk melindungi dataset wajah. Algoritma LBP dipilih karena kemampuannya dalam ekstraksi fitur wajah yang cepat dan efisien, yang membuatnya sangat cocok untuk aplikasi pengenalan wajah *real-time*. Dengan menggunakan LBP, sistem dapat mengidentifikasi individu berdasarkan tekstur mikro pada gambar wajah, yang kemudian dapat digunakan untuk verifikasi identitas dengan akurasi tinggi. Untuk meningkatkan keamanan data wajah yang dikumpulkan, teknik *encoding* Base64 *Shuffle* diterapkan yang dikenal dengan

kecepatannya dalam menjaga data (Muła & Lemire, 2019). Teknik ini memastikan bahwa dataset wajah yang tersimpan tetap aman dan hanya dapat diakses oleh pihak yang berwenang. Kombinasi LBP dan teknik *encoding* Base64 *Shuffle* tidak hanya memberikan solusi pengenalan wajah yang cepat dan akurat tetapi juga melindungi data pribadi dari potensi ancaman seperti pencurian dan penyalahgunaan data. Pendekatan ini diharapkan dapat meningkatkan tingkat keamanan dan privasi dalam berbagai aplikasi, mulai dari sistem kunci pintu pintar hingga manajemen akses di fasilitas berkeamanan tinggi.

Menggabungkan algoritma LBP dengan teknik *encoding* Base64 *Shuffle* untuk dataset wajah dan *file* pelatihan menghadirkan beberapa keuntungan signifikan dalam hal keamanan dan kinerja. Dengan penerapan teknik *encoding* Base64 *Shuffle*, setiap data wajah yang dihasilkan oleh LBP kemudian dikodekan sebelum disimpan atau ditransmisikan, memberikan lapisan perlindungan tambahan terhadap akses tidak sah. Teknik *encoding* Base64 *Shuffle*, yang dikenal karena kemudahannya dalam menangani data biner, memastikan bahwa data sensitif tetap terlindungi bahkan jika terjadi pelanggaran keamanan (Muła & Lemire, 2019). Kombinasi ini tidak hanya meningkatkan keamanan data tetapi juga menjaga integritas dan keaslian informasi, sehingga cocok untuk aplikasi yang memerlukan tingkat keamanan tinggi seperti kontrol akses di fasilitas kritis dan sistem keamanan rumah pintar. Melalui pendekatan ini, penelitian ini berkontribusi pada pengembangan teknologi keamanan yang lebih andal dan efisien, menjawab tantangan yang ada dalam perlindungan data biometrik.

Keunikan dari penelitian ini terletak pada penggunaan teknik *encoding* Base64 *Shuffle* terhadap dataset wajah yang nantinya digunakan untuk membuka kunci pintu. Berbeda dengan penelitian sebelumnya yang berfokus pada teknologi pengenalan wajah menggunakan algoritma yang berbeda, penelitian ini juga melakukan pengujian akurasi yang mendalam. Dengan demikian, penelitian ini memberikan kontribusi baru dalam konteks pengamanan dataset wajah pada kunci pintu, serta memberikan metode pengujian untuk memastikan keamanan dan efektivitas solusi yang diusulkan.

1.2 Rumusan Masalah Penelitian

Berdasarkan paparan latar belakang diatas, peneliti merumuskan beberapa rumusan masalah yaitu:

1. Bagaimana pengembangan sistem kunci pintu dengan pengenalan wajah menggunakan algoritma LBP dapat diwujudkan?
2. Bagaimana penerapan teknik pengamanan Base64 *Shuffle* dapat diintegrasikan dalam sistem kunci pintu untuk meningkatkan keamanan data?
3. Bagaimana kinerja sistem kunci pintu dengan pengenalan wajah algoritma lbp dan pengamanan data Base64 *shuffle* yang akan dibuat?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah penelitian diatas, maka tujuan dari penelitian ini yaitu:

1. Mengembangkan sistem kunci pintu dengan algoritma *Local binary pattern* LBP sebagai metode pengenalan wajah.
2. Menerapkan sistem pengamanan pintu yang mengintegrasikan teknik *encoding* Base64 *Shuffle* untuk melindungi dataset wajah dan *file* training.
3. Mengevaluasi kinerja penggunaan sistem kunci pintu dengan pengenalan wajah algoritma lbp dan pengamanan data Base64 *shuffle*.

1.4 Batasan Penelitian

Berdasarkan tujuan penelitian diatas, maka batasan masalah dari penelitian ini yaitu:

1. Penelitian ini berfokus pada deteksi wajah bagian depan manusia. Deteksi hanya dilakukan pada wajah yang terlihat utuh dan tanpa terhalang oleh objek lain.
2. Pada penelitian ini jarak objek dibatasi hingga 160 cm dari kamera,
3. Pada penelitian ini digunakan *web cam* dengan resolusi 1080 piksel.
4. Penelitian ini dilakukan pada lingkungan pengujian *indoor* dengan rentang intensitas cahaya dari 0 – 100 *lux*.
5. Aplikasi ini dikembangkan bahasa pemrograman python.
6. Dataset wajah disimpan dalam format gambar PNG serta data hasil training berformat .xml

1.5 Manfaat Penelitian

Berdasarkan tujuan Penelitian yang telah dipaparkan sebelumnya, Penelitian ini diharapkan bermanfaat bagi perkembangan teknologi terutama dalam bidang pengenalan wajah dan keamanan data.

1.5.1. Manfaat Teoritis

1. Penelitian ini memperkaya literatur akademik dengan menggali implementasi algoritma *Local binary pattern* dalam pengenalan wajah serta penggunaan teknik *encoding* Base64 *Shuffle* untuk melindungi dataset wajah.
2. Penelitian ini memperkenalkan metodologi baru untuk menilai kinerja dan keamanan sistem pengenalan wajah dengan pengamanan data menggunakan Base64 *Shuffle*.

1.5.2. Manfaat Praktis

1. Implementasi kombinasi *Local binary pattern* (LBP) dan teknik *encoding* Base64 *Shuffle* dalam sistem kunci pintu meningkatkan keamanan dan keandalan sistem penguncian pintu.
2. Dengan menggunakan teknik *encoding* Base64 *Shuffle* untuk mengamankan data wajah pengguna, sistem ini menjamin perlindungan privasi dan keamanan data biometrik.

1.5.3. Manfaat Kebijakan

Manfaat kebijakan mengenai peraturan tentang penyalahgunaan foto pribadi sangat signifikan dalam menjaga privasi dan keamanan individu di era digital.

1.6 Struktur Organisasi Skripsi

Berdasarkan pada Peraturan Rektor UPI (Universitas Pendidikan Indonesia) Nomor.7867/UN40/HK/2021 tentang Pedoman penulisan Karya Ilmiah Universitas Pendidikan Indonesia Tahun Akademik 2021. Sistematika penulisan karya ilmiah ini terdiri atas 5 bagian, yaitu pendahuluan, kajian pustaka, metode penelitian, temuan dan pembahasan, serta simpulan, implikasi, dan rekomendasi. Adapun rincian setiap bagiannya sebagai berikut:

1. PENDAHULUAN

Pada bab ini penulis membahas latar belakang penelitian, mengidentifikasi permasalahan yang akan diselesaikan, merincikan tujuan, menentukan batasan pada penelitian yang dilakukan serta manfaat penelitian dari penelitian yang dilakukan. Selain itu struktur organisasi dijelaskan agar memberikan gambaran terhadap arah penulisan.

2. KAJIAN PUSTAKA

Pada bab ini, penulis membahas mengenai kajian teoritis dari penelitian, Fokus utama dari bab ini adalah pemahaman mengenai algoritma *Local binary pattern* dan metode *encoding* Base64 *Shuffle* serta mikrokontroller ESP32 sebagai hardware utama pengembangan sistem.

3. METODOLOGI PENELITIAN

Pada bab ini, penulis membahas mengenai metodologi penelitian yang digunakan dalam penelitian ini. Pendekatan yang digunakan adalah *Design and Development* (D&D) yang memberikan kerangka kerja sistematis dan iteratif untuk pengembangan.

4. HASIL DAN PEMBAHASAN

Pada bab ini membahas hasil temuan dari penelitian, mencakup presentasi data, analisis mendalam, dan interpretasi hasil. Pembahasan melibatkan perbandingan dengan literatur terkait, analisis implikasi hasil, serta pengidentifikasian kelemahan penelitian.

5. SIMPULAN, IMPLIKASI, DAN REKOMENDASI

Pada bab ini, penulis membahas penutup laporan. Simpulan memberikan ringkasan temuan penting dan jawaban terhadap pertanyaan penelitian, menyoroti hasil akurasi yang digunakan dalam penelitian ini. Implikasi membahas dampak temuan terhadap teori keamanan data dan praktik pengembangan aplikasi pengamanan data teks. Rekomendasi diberikan untuk penelitian selanjutnya dan penerapan hasil temuan dalam konteks praktis, termasuk saran untuk pengembangan lebih lanjut dari metode LBP dan Base64 *Shuffle* dalam aplikasi nyata.