# BAB I
# PENDAHULUAN

## 1.1 Latar Belakang Penelitian

Teknologi pengenalan wajah merupakan salah satu cara yang sekarang ini banyak digunakan untuk pengamanan perangkat atau aplikasi. Pada beberapa negara, sistem pengenalan wajah sudah sangat banyak digunakan oleh perusahaan. Bahkan di Singapura sistem pengenalan wajah sudah terhubung dengan data pemerintah sebagai identitas resmi utama bagi penduduknya (Rosmalia, 2020). Di Indonesia sendiri pemanfaatan sistem pengenalan wajah sudah banyak digunakan pada aplikasi seperti *face unlock* yang digunakan pada untuk membuka akses *smartphone*, sistem absensi, verifikasi data diri pada aplikasi, dan banyak aplikasi lainnya. Tekonologi pengenalan wajah juga semakin banyak digunakan khususnya untuk sistem absensi *online* semenjak kondisi pandemi ini yang mengharuskan aktifitas seperti perkantoran dan pembelajaran sekolah dilakukan secara *online* (Saukani, 2020).

Meskipun wajah setiap orang berbeda, namun pada kenyataannya teknologi pengenalan wajah cenderung lebih rentan dibandingkan dengan biometrik lainnya seperti sidik jari dan selaput pelangi (iris mata). Dengan adanya internet dan luasnya sosial media, citra wajah seseorang menjadi sangat mudah didapatkan sehingga semakin tinggi potensi untuk digunakan sebagai tindak kejahatan pada sistem pengenalan wajah yang digunakan. Namun daripada itu, biometrik wajah tetap menjadi pilihan banyak orang karena tidak perlu terjadi kontak dengan sensor sehingga mudah digunakan dan juga murah dari segi biaya karena cukup menggunakan kamera dan tidak perlu sensor khusus dalam penggunaan sistemnya (Marcel et al., 2019). Hal ini menjadi salah satu kelebihan pengenalan wajah, terlebih dalam kondisi pandemi *Covid-19* ini yang penyebarannya dapat terjadi melalui kontak (Limonu, 2020).

Dari sekian banyak citra atau video wajah orang yang tersebar di internet dan media sosial, terdapat 33% citra maupun video wajah yang berhasil

digunakan untuk memanipulasi pengguna sistem pengenalan wajah. Meskipun jumlahnya terbilang sedikit, namun kenyataannya 33% citra dan video tersebut berhasil memanipulasi pengguna pada sebuah sistem pengenalan wajah mencapai 77% dari 74 pengguna. Pada percobaan lainnya, seorang wanita yang menggunakan *make up* wajah pengguna lain juga berhasil mengelabui sistem pengenalan wajah (Jiang et al., 2019).

Penelitian lain melakukan percobaan menggunakan citra wajah *online* yang diperoleh dari *Facebook* berhasil menipu sebanyak empat sistem pengenalan wajah (Newman, 2016). Pada kasus lainnya, sistem pengenalan wajah pada *smartphone* Samsung Galaxy S10 dan S10+ mendapat banyak kritikan karena sistem yang berhasil diakses dengan menggunakan video dari YouTube dan citra digital (Burt, 2019). Diberitakan juga (Pratomo, 2019) sebanyak 42 dari 110 *smartphone* yang menggunakan fitur pengenalan wajah dapat dibobol menggunakan foto seperti pada Huawei P20 Pro dan Sony Xperia XZ2.

Dari kasus-kasus kejahatan tersebut maka dibuktikan bahwa penggunaan sistem pengenalan wajah tidak cukup aman jika hanya dengan mengenali wajah penggunanya saja, tapi juga dibutuhkan keamaan seperti pengecekan apakah wajah yang ditangkap benar merupakan asli penggunanya atau merupakan sebuah serangan atau penipuan. Lemahnya sistem pengenalan wajah terhadap serangan pemalsuan pengguna menjadikan *presentation attack detection* diperlukan dalam sistem pengenalan wajah.

*Presentation attack detection* diperlukan untuk mencegah terjadinya serangan pemalsuan pengguna sistem. *Liveness detection* dapat digunakan untuk mendeteksi serangan pada sistem dengan menambahkan beberapa alat seperti *thermal sensor* dan *scanner 3D*. Namun, penambahan alat tersebut membutuhkan biaya yang cukup mahal dan masih jarang ditemukan pada *smartphone* yang beredar sehingga diperlukan sistem *face presentation attack detection* yang dapat mendeteksi serangan pada sistem pengenalan wajah. Sistem *anti-spoofing* yang telah ada kebanyakan dilakukan dengan mendeteksi

adanya gerakan dari pengguna seperti gerakan mulut atau mata, namun cara tersebut juga masih dapat dengan mudah dimanipulasi dari serangan jenis video atau dengan menggunakan topeng pengguna aslinya (Marcel et al., 2019).

Beberapa penelitian terkait *face presentation attack detection* telah dilakukan dengan menganalisis tekstur citra atau video yang ditangkap kamera sehingga dapat diketahui keaslian pengguna sistem tersebut. Berbagai metode digunakan dalam penelitian, mulai dari metode tradisional hingga metode modern, seperti *Local Binary Pattern* (Ojala et al., 1994), *Image Quality Assessment* (Galbally & Marcel, 2014), *Convolutional Neural Network* (LeCun et al., 1999), *Recurrent Neural Network* (Rumelhart et al., 1986), dan metode-metode lainnya.

Dari penelitian-penelitian tersebut diketahui bahwa penelitian dengan menggunakan metode LBP mengungguli metode lain dengan menganalisis tekstur citra (Boulkenafet et al., 2015). Penelitian dengan menggunakan metode IQA dapat berhasil mengungguli metode *Difference of Gaussian* saat menggunakan citra beresolusi tinggi, namun masih tetap lebih baik LBP (Galbally & Marcel, 2014). Kemudian pada penelitian dengan menggunakan metode CNN untuk ekstraksi fitur hasil yang diperoleh sudah cukup baik, namun meskipun begitu saat model digunakan untuk data baru hasil masih kurang memuaskan (Yang et al., 2014).

Berdasarkan dari uraian di atas, penulis melakukan penelitian untuk merancang model baru untuk sistem *face presentation attack detection* dengan mengimplementasikan metode *local binary pattern* dan kemudian digabungkan dengan metode *machine learning* modern *restricted boltzmann machines*. Metode LBP ini dipilih berdasarkan studi literatur dari penelitian terkait yang menunjukkan bahwa LBP mengungguli metode lain dalam ekstraksi fitur *micro texture* wajah. Sedangkan metode RBM dipilih dengan harapan dapat digunakan untuk menutupi kekurangan metode LBP yang digunakan yang tidak *invariant* terhadap rotasi dan skala. RBM juga

diharapkan dapat digunakan untuk mencari hubungan dari masing-masing data dan untuk mereduksi dimensi data. Metode RBM juga telah dibuktikan berhasil digunakan untuk ekstraksi fitur pada beberapa penelitian terkait *face recognition* dan *facial expression recognition*. Harapannya dari penelitian yang dilakukan penulis dapat dihasilkan model yang baik dan dapat siap digunakan untuk *real time detection* pada sistem pengenalan wajah.

## 1.2 Rumusan Masalah Penelitian

Berdasarkan permasalahan yang terdapat pada latar belakang masalah, maka disusun rumusan permasalahan penelitian sebagai berikut.

1. Bagaimana desain rancangan model *face presentation attack detection* yang akan dibuat?
2. Bagaimana rancangan model *face presentation attack detection* dapat diimplementasikan menjadi sistem *face presentation attack detection*?
3. Bagaimana hasil kinerja model *face presentation attack detection* yang telah dibuat?
4. Bagaimana pengaruh metode *local binary pattern* dan *restricted Boltzmann machines* terhadap *dataset* wajah yang digunakan pada proses ekstraksi fitur?

## 1.3 Tujuan Penelitian

Mengacu pada rumusan masalah yang telah diperoleh sebelumnya, maka tujuan dilakukannya penelitian ini adalah sebagai berikut.

1. Merancang model sistem *face presentation attack detection* dengan menggunakan metode ekstraksi fitur LBP dan RBM dari data *real* dan *attack* jenis foto dan video.
2. Mengimplementasikan rancangan model *face presentation attack detection* yang telah dibangun ke dalam kode program menjadi sebuah sistem *face presentation attack detection*.

3. Mengevaluasi hasil kinerja sistem *face presentation attack detection* yang telah dibangun berdasarkan tingkat akurasi dan *error*-nya.
4. Menganalisis hasil latih dan prediksi dari model sistem *face presentation attack detection* yang telah dibangun berdasarkan metode ekstraksi fitur yang digunakan.

## 1.4 Manfaat Penelitian

Manfaat penelitian tentang *face presentation attack detection* ini untuk merancang dan menganalisis model yang dapat digunakan dalam membedakan wajah pengguna yang asli dan wajah hasil serangan untuk pengembangan sistem pengenalan wajah. Penelitian ini juga bermanfaat untuk memahami pengaruh metode *local binary pattern* dan *restricted Boltzmann machines* terhadap data wajah. Pada penelitian ini juga memberikan hasil evaluasi rancangan model agar diperoleh hasil yang lebih baik.

## 1.5 Batasan Penelitian

Adapun batasan dalam pelaksanaan penelitian *face presentation attack detection* ini yaitu sebagai berikut:

1. Model dirancang untuk sistem *face presentation attack detection* dengan citra warna RGB.
2. Model dirancang dengan menggunakan metode analisis statis dengan mengekstraksi tekstur citra.
3. Model dibuat untuk mendeteksi adanya serangan pemalsuan jenis *photo-attack* dan *video-attack*.
4. Model dibuat untuk mendeteksi keaslian wajah pengguna dengan mengklasifikasikannya ke dalam dua kelas, wajah asli dan wajah hasil *attack*.

## 1.6 Sistematika Penulisan

Sistematika penulisan pada penelitian ini terdiri dari:

BAB I PENDAHULUAN.

Bab ini berisi latar belakang masalah, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan penelitian, dan sistematika penulisan. Pada bab ini penulis membahas latar belakang masalah terkait *face presentation attack detection* dan alasan pentingnya tema penelitian diangkat. Alasan metode dipilih dan harapan yang dicapai juga penulis cantumkan pada bab ini.

BAB II KAJIAN PUSTAKA.

Bab ini membahas penelitian-penelitian terkait *face presentation attack detection* dan landasan teori serta sumber dari metode-metode terkait seperti *face recognition* dan *face presentation attack detection* sebagai teori dasar dari objek penelitian. Pada bab ini juga dibahas mengenai metode *local binary pattern* dan *restricted Boltzmann machines* sebagai dasar teori dari metode ekstraksi fitur yang akan digunakan pada penelitian. Metode-metode lain pendukung penelitian juga akan dibahas pada bab ini.

BAB III METODOLOGI PENELITIAN.

Pada bab ini penulis menjelaskan desain penelitian yang berisi tahapan pelaksanaan penelitian yang akan dilakukan, mulai dari perumusan masalah hingga penarikan kesimpulan. Penulis juga menjelaskan tentang rancangan model sistem *face presentation attack detection* yang akan dibuat juga bahan atau data dan perangkat yang dibutuhkan untuk mendukung pelaksanaan penelitian.

BAB IV HASIL DAN PEMBAHASAN

Bab ini membahas proses pengumpulan data wajah *real* dan wajah *attack*, perancangan *computational model* untuk sistem *face presentation attack detection* dan implementasinya ke dalam kode program, dan hasil eksperimen yang diperoleh selama penelitian. Evaluasi dan analisis hasil eksperimen penelitian berdasarkan metode ekstraksi fitur LBP dan RBM juga dibahas pada bab ini.

# BAB V PENUTUP

Bab ini berisi kesimpulan dari penelitian tentang *face presentation attack detection* yang telah dilakukan penulis. Hal-hal yang berhasil penulis capai dijelaskan pada bagian kesimpulan. Penulis juga memberikan saran dan *future work* terkait penelitian.