# BAB 1

# PENDAHULUAN

## 1.1 Latar Belakang Masalah

Ada berbagai macam sistem pengenalan wajah, contohnya mulai dari *Biometric Face* milik Android, Lenovo VeriFace, Asus Smart-Logon, dan Toshiba SmartFace. Sayangnya, berdasarkan penelitian yang dilakukan oleh Wen, Han dan Jain (2015), 70% dari database *spoofing* yang mereka ujikan dapat melewati pengenalan wajah dan terverifikasi sebagai *user* asli dalam sistem pengenalan wajah *Commercial off-the-shelf* (COTS). Hal ini menandakan bahwa sistem pengenalan wajah komersil yang ada tidak ampuh dalam membedakan wajah asli dan palsu.

Adapun *spoofing attack* yang umum di dalam pengenalan wajah, yaitu *photo attack, video attack,* 3D *mask attack* (Hernandez-Ortega, dkk., 2019). Jenis *photo attack* dan *video attack* adalah yang paling umum digunakan karena tingkat eksposisi wajah yang sangat tinggi seperti foto dan video yang tersebar di sosial media dan rekaman CCTV, dan biaya rendah untuk kamera, *printer* dan layar beresolusi tinggi (Hernandez-Ortega, dkk., 2019).

Ada beberapa metode yang dapat dipakai untuk menanggulangi *spoofing attack*, beberapa contohnya adalah *motion analysis, contextual based analysis, texture analysis, image quality analysis* (Boulkenafet dkk., 2017), dan *life sign* (Bloecher dkk., 2017). *Life sign* merupakan indikator yang dipakai dalam *liveness detection* untuk mengukur pergerakan spesifik dari muka (Parveen dkk., 2015)

seperti kedipan mata (Pan dkk., 2007) atau meminta respon dari *user* secara *realtime* seperti senyuman (Deniz dkk., 2007). Menurut Chakraborty dan Das (2015), kekurangan *liveness detection* adalah dibutuhkan interaksi dari *user*, memerlukan *sequence* dari video dan sangat bergantung pada *facial landmark detection*.

*Challenge-Response* adalah metode yang dapat dipakai untuk menerapkan *liveness detection* dan secara intrusif mempersulit seseorang melakukan *spoofing* terhadap sistem (Boulkenafet dkk., 2017). Menurut Boulkenafet dkk., (2017), salah satu kelemahan sistem pengukuran yang intrusif seperti *challenge-response* ini adalah mudah ditebak dan diprediksi apa yang akan diukur, misal meminta *user* untuk menyebut sejenis kata atau memutar kepala, sehingga diketahui pengukuran yang dipakai (analisis bibir/geometri 3D). Berhubungan dengan sistem pengukuran, kelemahan pendekatan *challenge-response* ini bisa diatasi dengan metode *randomness* dimana pengukurannya dapat meliputi semua data yang didapatkan sehingga dapat mengacak *challenge* yang diberikan.

Pada penelitian ini dikembangkan sistem *anti-spoofing* dengan *liveness detection* pada aplikasi pengenalan wajah. Sistem akan menggunakan *library* Dlib untuk mengenali wajah penggunanya, dengan akurasi sebesar 99,38% menggunakan *benchmark Labeled Faces in the Wild* (King, 2017). *Library* ini juga dapat mengekstrak *face annotation* yang dibutuhkan oleh *liveness detection*. Implementasi dilakukan dengan cara mengimplementasikan metode *challenge-response* dengan metode *liveness-detection* dalam sistem berbasis C++, menggunakan *library* dlib sebagai alat untuk mengenali wajah seseorang dan untuk

mengambil variabel-variabel yang dibutuhkan dalam penelitian ini dari sebuah *frame* dalam video *real-time*. Pengujian dilakukan dengan cara melakukan white box texting. Evaluasi dilakukan dengan menggunakan dataset pribadi yang berisi *spoofing attack* berupa *printed attack* dan *video attack*.

### 1.2. Rumusan Masalah

Berdasarkan latar belakang yang sudah ditulis diatas, maka rumusan masalah dalam penelitian ini adalah sebagai berikut.

- Bagaimana mengimplementasi *liveness detection* untuk pencegahan *spoofing attack* dalam pengenalan wajah?
- Berapa tingkat akurasi dan F-score dari hasil implementasi *liveness detection* untuk pencegahan *spoofing attack* dalam pengenalan wajah?

### 1.3. Batasan Masalah

Adapun batasan-batasan masalah dalam penelitian ini adalah sebagai berikut.

- untuk mengenali wajah menggunakan *pre-trained* CNN ResNet-29 *model* dari *library* Dlib.
- untuk mendeteksi wajah menggunakan *pre-trained* CNN MMOD *model* dari *library* Dlib.
- Maksimal wajah yang dideteksi secara bersamaan adalah satu wajah saja, atau dianggap sebagai *attack*.

- *Spoofing attack* yang akan dibahas adalah *printed attack* dan *video replay attack*.

## 1.4. Tujuan Penelitian

Tujuan yang ingin dicapai pada penelitian ini adalah sebagai berikut.

- Mengetahui cara untuk mengimplementasi *liveness detection* untuk pencegahan *spoofing attack* dalam pengenalan wajah.
- Mengetahui tingkat akurasi dan F-score dari hasil implementasi *liveness* detection untuk pencegahan *spoofing attack* dalam pengenalan wajah.

## 1.5. Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat sebagai berikut.

1. Menyediakan sebuah fitur pencegahan *spoofing attack* untuk aplikasi pengenalan wajah.
2. Mengetahui cara kerja *liveness detection* yang diaplikasikan untuk pencegahan *spoofing attack*.

## 1.6. Sistematika Penulisan

Sistematika penulisan dalam skripsi ini adalah sebagai berikut.

1. BAB 1 PENDAHULUAN

   Bab ini berisi latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan.

2. BAB 2 LANDASAN TEORI

   Bab ini berisi tentang teori-teori yang menjelaskan tentang *facial features, liveness detection, spoofing attack,* akurasi dan *f-score* yang akan dipakai di peneliian.

3. BAB 3 METODOLOGI PENELITIAN

   Bab ini berisi penjelasan dan penjabaran tentang metodologi penelitian yang dipakai, dari telaah literatur, perancangan, implementasi, pengujian, dan evaluasi.

4. BAB 4 IMPLEMENTASI DAN UJICOBA

   Bab ini berisi proses implementasi ke dalam sistem yang dibuat, serta hasil ujicoba dan evaluasi terhadap sistem tersebut.

5. BAB 5 KESIMPULAN DAN SARAN

   Bab ini berisi kesimpulan dan saran dari penelitian yang telah dilakukan dan saran untuk penelitian selanjutnya.