

Bab I

Pendahuluan

1.1 Latar Belakang

Sistem biometrik salah satunya sistem pengenalan wajah banyak dikembangkan untuk berbagai kebutuhan, diantaranya: untuk kontrol akses, penegakan hukum, multimedia serta interaksi antara manusia dan komputer [14]. Namun, kerentanan sistem pengenalan wajah ini juga perlu ditanggapi serius, karena proses penyerangan sistem dapat dilakukan dengan teknik yang mudah dan biaya yang dikeluarkan juga sedikit. Kasus tersebut biasa dikenal dengan istilah serangan *spoofing*, pelaku akan memalsukan data wajah korbannya sehingga mendapatkan akses ilegal serta keuntungan untuk dirinya sendiri dan pihak yang terkait [11]. Serangan *spoofing* ini bisa dilakukan dengan menampilkan gambar cetakan wajah, video rekaman wajah, atau menggunakan model 3D dari wajah korban sebagai bentuk pemalsuannya [10].

Penelitian yang telah dilakukan untuk pendeteksian *spoofing* pada wajah manusia yaitu: mengidentifikasi tanda-tanda fisiologis wajah (kedipan mata [13], gerakan bibir [9] dan rotasi kepala [2]). Selain itu, ada juga yang mengkombinasikan antara modalitas sistem biometrik lainnya dengan wajah. Namun, metode-metode tersebut membutuhkan *user cooperation* yang membuat waktu komputasinya menjadi lebih lama dan membutuhkan peralatan yang mendukung dengan biaya yang cukup besar [5].

Maka diperlukan sistem yang lebih handal tanpa memerlukan *user cooperation* sehingga waktu komputasinya lebih cepat dan tidak memerlukan peralatan lain yang membutuhkan biaya yang besar. Pada penelitian ini, penulis mengusulkan sebuah metode analisis tekstur yang digunakan untuk menganalisis indikasi citra dengan serangan *spoofing* yang dapat membedakan citra *spoof* dengan *non-spoof*. Ini dikarenakan, perbedaan antara wajah manusia yang merupakan objek 3D kompleks dengan gambar cetakan yang hanya objek planar dapat diidentifikasi secara jelas menggunakan analisis tekstur [5]. Analisis tekstur yang digunakan untuk menangani masalah serangan *spoofing* yang pernah dilakukan adalah analisis *micro texture* menggunakan operator LBP (*Local Binary Pattern*) dengan hasil akurasi sebesar 98.0% [11]. Untuk itu, penulis mengusulkan metode pendeskripsian tekstur lainnya yaitu LDP

(*Local Derivative Pattern*). Berbeda dengan LBP (*Local Binary Pattern*) yang mengdiskriminasikan ciri pada orde pertama saja, LDP mengkodekan orde pada tingkat yang lebih tinggi dan pada arah tertentu sehingga informasi yang dihasilkan terhadap fitur diskriminasi cirinya lebih detail [19]. Selain itu, metode LDP dapat menangani masalah sensitifitas terhadap *noise* yang membuat metode ini semakin kuat dan handal [19]. Metode LDP ini digunakan sebagai proses ekstraksi ciri pada tugas akhir ini.

1.2 Perumusan Masalah

Dari latar belakang yang telah dijabarkan, rumusan masalah yang diangkat oleh penulis, antara lain:

1. Bagaimana parameter pada metode ekstraksi ciri *Local Derivative Pattern* memengaruhi performansi sistem?
2. Bagaimana pengaruh parameter pada kinerja metode *k-Nearest Neighbors* dan metode *Support Vector Machine* untuk mengklasifikasikan masukan citra pada sistem pendeteksian serangan *spoofing* wajah yang dikombinasikan dengan *Local Derivative Pattern* sebagai ekstraksi cirinya?
3. Bagaimana pengaruh pola *uniform* pada metode ekstraksi ciri *Local Derivative Pattern* terhadap waktu eksekusi sistem deteksi serangan *spoofing* pada citra wajah?

Tugas akhir ini menggunakan *NUAA Imposter and Photograph Database* sebagai datasetnya yang merupakan kumpulan citra *spoof* dan *non-spoof* dari 16 individu yang berbeda.

Berdasarkan rumusan masalah, maka tugas akhir ini memiliki batasan masalah, sebagai berikut.

1. *NUAA Imposter and Photograph Database* digunakan sebagai dataset.
2. Citra masukan *grayscale*, memiliki arah frontal dan tidak dapat dirotasi.
3. Citra telah dinormalisasi geometri berdasarkan koordinat dua bola mata.
4. Citra *spoof* yang diambil menggunakan kamera Canon dicetak pada kertas 70g A4.
5. Citra *non-spoof* diambil menggunakan kamera *webcam* dengan *frame rate* sebesar 20fps.

1.3 Tujuan

Berdasarkan rumusan masalah yang telah dijelaskan, maka tujuan dari tugas akhir ini antara lain:

1. Menganalisis pengaruh parameter pada metode ekstraksi ciri *Local Derivative Pattern* terhadap performansi sistem untuk mendeteksi *spoofing* pada citra wajah manusia.
2. Menganalisis kinerja sistem yang dipengaruhi oleh parameter pada *k-Nearest Neighbors* dan *Support Vector Machine* sebagai metode pengklasifikasi yang dikombinasikan dengan *Local Derivative Pattern* sebagai metode ekstraksi ciri untuk mendeteksi serangan *spoofing* pada citra wajah.
3. Menganalisis waktu eksekusi sistem yang dipengaruhi oleh pola *uniform* pada metode ekstraksi ciri *Local Derivative Pattern*.

1.4 Metodologi Penyelesaian Masalah

Penyelesaian masalah pada tugas akhir ini, menggunakan beberapa metodologi, diantaranya:

- Studi Literatur

Studi literatur adalah proses mengkaji bidang yang dilakukan pada penelitian ini. Tahap pertama yang dilakukan adalah memahami prinsip-prinsip dasar dari sistem biometrik, lalu serangan *spoofing* itu sendiri. Setelah itu, melakukan pengumpulan, pembelajaran dan pendalaman literatur yang berkaitan dengan LDP (*Local Derivative Pattern*), k-NN (*k-Nearest Neighbors*) dan SVM (*Support Vector Machine*) serta perhitungan performansi sistem. Literatur yang digunakan berasal buku, *paper*, jurnal serta tugas akhir yang terkait dan telah diselesaikan.

- Pengumpulan Data

Data yang digunakan pada penelitian ini berasal dari dataset yang telah ada yaitu *NAA Imposter and Photograph Database* berupa citra *spoof* dan *non-spoof*. Citra tersebut telah dinormalisasi secara geometri berdasarkan koordinat bola mata [8]. Proses pengumpulan dataset ini dilakukan selama tiga sesi dalam jangka waktu dua minggu dengan berbagai perubahan lingkungan dan pencahayaan [11]. Pembagian dari data ini adalah 7509 citra *spoof* dan 5105 citra *non-spoof*.

- Analisis Kebutuhan Sistem

Analisis kebutuhan sistem ini meliputi kebutuhan perangkat keras maupun perangkat lunak untuk sistem pendeteksian serangan *spoofing* pada wajah yang dibangun pada tugas akhir ini.

- Perancangan Sistem

Sistem dirancang untuk mendeteksi adanya indikasi serangan *spoofing* pada citra wajah. Masukan yang diterima oleh sistem adalah sebuah citra. Sistem melakukan ekstraksi ciri citra dengan *Local Derivative Pattern*. Setelah itu, dilakukan perancangan model klasifikasi menggunakan metode *k-Nearest Neighbors* dan *Support Vector Machine*. Model yang telah dibangun ini kemudian digunakan pada proses pengujian. Keluaran dari proses pengujian sistem ini adalah hasil performansi serta hasil klasifikasi terhadap masukan citra baru yang menyatakan bahwa citra tersebut *spoof* atau *non-spoof*. Selain itu, model yang telah didapat juga diuji waktu eksekusinya untuk mengetahui pengaruh pola *uniform* pada metode *Local Derivative Pattern*.

- Implementasi Sistem

Sistem yang sudah dirancang, kemudian diimplementasikan yang terdiri dari dua proses utama yaitu ekstraksi ciri citra dengan *Local Derivative Pattern* dan proses klasifikasi menggunakan *k-Nearest Neighbors* dan *Support Vector Machine*. Implementasi ini dilakukan sesuai rancangan skema yang telah dibuat sebelumnya.

- Pengujian Sistem dan Analisis

Pengujian dilakukan untuk mengetahui sistem yang dibangun sudah sesuai dengan rancangan atau belum berdasarkan nilai performansinya yang direpresentasikan dalam bentuk *F1-Score*. Selain itu, pengujian juga dilakukan untuk menganalisa kehandalan sistem dalam menangani masalah yang ada dengan menggunakan komponen terukur yaitu H-TER (*Half Total Error Rate*). Analisis terhadap waktu eksekusi sistem juga dilakukan pada tahap ini. Hasil yang telah didapat dari penelitian direpresentasikan dalam bentuk tabel dan grafik.

- Pembuatan Laporan Tugas Akhir

Laporan dibuat untuk mendokumentasikan segala kegiatan dan hasil yang didapat dari pengerjaan tugas akhir ini.

1.5 Sistematika Penulisan

Penulisan tugas akhir ini dibagi menjadi beberapa bab, diantaranya:

1. Bab 1: Pendahuluan

Bab ini berisikan latar belakang, perumusan masalah, tujuan, hipotesis, metodologi penyelesaian masalah dan sistematika penulisan tugas akhir ini.

2. Bab 2: Kajian Pustaka

Pada bab ini memuat dasar teori yang berkaitan dengan tugas akhir "Deteksi Serangan Spoofing pada Citra Wajah menggunakan Local Derivative Pattern". Isi dari Bab 2 ini yaitu ulasan *paper* atau jurnal acuan, *face spoofing attack*, analisis tekstur, *Local Derivative Pattern*, *k-Nearest Neighbors*, *Support Vector Machine* dan pengukuran performansi yang digunakan.

3. Bab 3: Metodologi dan Desain Sistem

Pembahasan pada bab ini tentang perancangan sistem yang dibangun untuk mendeteksi serangan *spoofing* pada citra wajah menggunakan metode *Local Derivative Pattern* sebagai ekstraksi cirinya serta *k-Nearest Neighbors* dan *Support Vector Machine* sebagai metode klasifikasinya.

4. Bab 4: Pengujian dan Analisis Sistem

Pembahasan tentang analisis hasil yang didapat dari sistem deteksi *spoofing* pada citra wajah menggunakan metode *Local Derivative Pattern* sebagai ekstraksi ciri serta *k-Nearest Neighbors* dan *Support Vector Machine* sebagai metode klasifikasi terdapat pada bab ini.

5. Bab 5: Kesimpulan dan Saran

Bab ini memuat kesimpulan dari hasil pengujian dan analisis sistem. Selain itu, terdapat saran yang dituliskan penulis untuk pengembangan sistem kedepannya.