

1. Pendahuluan

Latar Belakang

Teknologi biometrik biasa didefinisikan sebagai metode untuk mengidentifikasi identitas diri seseorang. Secara umum, ciri khas dari diri seseorang bisa berupa wajah, sidik jari, iris mata, cara berjalan, tanda tangan, suara, dll. Saat ini otentikasi sistem biometrik pengenalan wajah menjadi alternatif untuk memperkuat tingkat keamanan dari sebuah sistem informasi. Namun, sistem tersebut masih rentan terhadap sebuah serangan yang disebut dengan serangan *spoofing*. Penyerangan tersebut dapat dilakukan dengan cara menampilkan foto atau video rekaman dari wajah asli dari pengguna sistem yang sah [6]. Seiring dengan meningkatnya pertumbuhan internet khususnya dari jejaring sosial dimana banyak orang yang tidak keberatan untuk menyebarkan informasi pribadi mereka khususnya foto dan video dari muka mereka. Hal tersebut akan memudahkan penyerang dalam mendapatkan foto atau video seseorang untuk digunakan oleh mereka dalam menyerang sistem. Berdasarkan masalah tersebut, penulis membangun sebuah sistem yang dapat mendeteksi *spoofing* pada wajah manusia, apakah wajah tersebut merupakan wajah asli atau palsu. Berikut adalah contoh dari serangan *spoofing* dengan cara menampilkan foto wajah (yang dicetak) dari pemilik atau pengguna sistem yang dapat dilihat pada Gambar 1. Sedangkan contoh dari serangan *spoofing* dengan cara menampilkan rekaman video wajah dari pemilik atau pengguna sistem yang sah dapat dilihat pada Gambar 2.



Gambar 1. Contoh *Spoofing Print Photo* bersumber dari *dataset CASIA*



Gambar 2. Contoh *Spoofing Replayed Video* bersumber dari *dataset CASIA*

Penelitian mengenai deteksi *spoofing* sudah banyak dilakukan oleh beberapa peneliti di dunia. Salah satunya dengan cara mengkombinasikan modalitas sistem biometrik lainnya dengan wajah. Namun, metode tersebut membutuhkan *user cooperation* yang membuat waktu komputasinya menjadi lebih lama [12]. Maka diperlukan sistem yang lebih handal agar waktu komputasinya lebih cepat. Pada penelitian ini, penulis mengusulkan metode untuk mendeteksi serangan *spoofing* pada video menggunakan analisis tekstur yaitu LDP. Dengan metode analisis tekstur akan

lebih mudah dalam mengidentifikasi perbedaan antara wajah asli manusia dan wajah palsu berdasarkan penelitian [6]. Pada penelitian tersebut, metode analisis tekstur yang digunakan dalam menangani masalah serangan *spoofing* adalah analisis *micro texture* menggunakan metode ekstraksi ciri *Local Binary Pattern* (LBP) dengan akurasi yang didapat sebesar 98%. Pada dasarnya, LBP adalah pola lokal orde pertama *non-directional* dari LDP [1]. Selain itu, LDP (*Local Derivative Pattern*) merupakan perluasan dari metode LBP yang dapat membedakan karakteristik orde pertama untuk semua arah yang sudah ditentukan [1]. Operator pada metode LDP dapat mengambil ciri dari setiap citra atau gambar ke beberapa tingkat orde untuk semua arah yang sudah ditentukan, sehingga informasi yang diperoleh dari citra atau gambar akan lebih rinci [1]. Selain itu, pola LDP juga dapat menangani masalah kesensitifan terhadap noise yang membuat sistem menjadi lebih handal.

Dalam penelitian Tugas Akhir (TA) ini, penulis menggunakan metode *Local Derivative Pattern* (LDP) dari *Three Orthogonal Planes* (TOP) untuk ekstraksi cirinya. Inovasi dari penelitian Tugas Akhir (TA) ini adalah untuk meningkatkan kinerja metode *Local Derivative Pattern* (LDP) dengan cara menggabungkan beberapa tingkatan orde pada LDP agar informasi yang diambil dari citra semakin detail. Kemudian, untuk proses klasifikasi menggunakan algoritma klasifikasi *K-Nearest Neighbors* (KNN) dan *Support Vector Machine* (SVM).

Topik dan Batasannya

Berdasarkan latar belakang diatas, maka dapat dirumuskan permasalahan yang diangkat dalam penelitian Tugas Akhir (TA) ini yaitu bagaimana pengaruh parameter dari ekstraksi ciri *Local Derivative Pattern* dari *Three Orthogonal Planes* (LDP-TOP).

Batasan-batasan yang diterapkan pada penelitian Tugas Akhir (TA) ini adalah data yang digunakan merupakan video yang berisikan wajah manusia.

Tujuan

Tujuan dari penelitian Tugas Akhir (TA) ini adalah membangun sebuah sistem yang dapat mendeteksi *spoofing* pada wajah manusia berbasis video dengan menggunakan *Local Derivative Pattern* dari *Three Orthogonal Planes* (LDP-TOP) sebagai metode ekstraksi cirinya dan mengetahui apa peranan metode tersebut terhadap akurasi dari sistem yang dibangun.

Organisasi Tulisan

Penelitian Tugas Akhir (TA) ini disusun dengan struktur sebagai berikut : Pada bagian pertama menjelaskan tentang pendahuluan. Pada bagian kedua menjelaskan

tentang studi terkait. Pada bagian ketiga menjelaskan tentang pemodelan sistem pada bagian kerja evaluasi. Pada bagian keempat menjelaskan tentang evaluasi dari performansi sistem terhadap sistem yang dibangun. Dan pada bagian kelima adalah menjelaskan kesimpulan.