1. Pendahuluan

Latar Belakang

Dengan banyaknya permintaan keamanan tingkat tinggi pada perangkat *mobile*, seperti *smart phones*, teknik biometrik mendapat cukup banyak perhatian. Sistem pengenalan wajah untuk sistem keamanan banyak dimanfaatkan, namun sistem pengenalan wajah ini rentan terhadap serangan pemalsuan atau biasa disebut *spoofing*.

Face spoofing adalah memalsukan wajah dengan menggunakan suatu media untuk masuk ke dalam sistem. Media tersebut dapat berupa cetakan atau video. Tanpa adanya *anti-spoofing*, biometrik wajah sangat rentan untuk diserang karena hasil cetakan atau video wajah manusia yang ditampilkan ke layar dapat mengelabui sistem, sehingga penelitian untuk menghindari serangan *spoofing* dilakukan [1].

Pada penelitian sebelumnya, dataset dibatasi hanya dengan menggunakan citra dengan kondisi yang sama antara data latih dan data uji [2]. Sedangkan, sangat penting membuat sistem yang dapat mengeneralisasi dengan baik terhadap dataset dengan kondisi yang baru. Untuk dapat mencapai tujuan tersebut, dibutuhkan pendekatan yang dapat menemukan bagian yang paling diskriminatif disekitar wajah. Dataset yang biasa digunakan untuk penelitian, biasanya memiliki karateristik yang berbeda, sehingga penting untuk memperoleh deskripsi fitur yang berfokus pada karateristik citra yang berbeda, seperti bentuk dan tekstur. Pada penelitian ini, untuk dapat membedakan antara citra *spoofing* dan non-*spoofing*, penulis menggunakan gabungan dari metode *low-level feature* yaitu *Speeded-Up Robust Feature* (SURF) [3] sebagai analisis tekstur yang invarian terhadap iluminasi, skala, dan rotasi citra dengan *Pyramid Histogram of Oriented Gradient* (PHOG) [4] yang mengesktrak intensitas gradient dan arah untuk mendeskripsikan bentuk citra. Klasifikasi *spoofing* dan non-*spoofing* yang digunakan adalah metode *Support Vector Machine* (SVM) dan *K-Nearest Neighbors* (KNN).

Topik dan Batasannya

Berdasarkan latar belakang diatas, dapat dirumuskan permasalahan yang akan diangkat dalam penelitian ini adalah tingkat performansi sistem dalam membedakan serangan *spoofing* dan non-*spoofing* dengan menggunakan metode *Speeded-Up Robust Features* (SURF) dan *Pyramid Histogram of Oriented Gradient* (PHOG), baik dalam skenario *intra-database* dan *cross-database*.

Tujuan

Tujuan dari penelitian Tugas Akhir ini adalah untuk membangun sistem yang dapat mendeteksi *spoofing* wajah manusia dengan menggunakan *Low-Level Features* dan analisis bentuk serta menganalisis performansi dengan melihat tingkat *Haf Total Error* (HTER) dalam mendeteksi *spoofing*.

Organisasi Tulisan

Penulisan Tugas AKhir ini disusun dalam beberapa bagian yang dari setiap bagian, berisi data-data berikut : Bagian 1 - Pendahuluan, Bagian 2 - Studi Terkait, Bagian 3 - Sistem yang dibangun, Bagian 4 - Evaluasi, Bagian 5 - Kesimpulan.