BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Pada penelitian mengenai *face presentation attack detection* telah dilakukan berbagai tahapan penelitian sehingga penulis dapat menyelesaikan penelitian ini. Sehingga berdasarkan penelitian yang telah penulis lakukan maka dapat ditarik kesimpulan bahwa:

1) Dalam penelitian ini penulis telah berhasil merancang model sistem *face presentation attack detection* dengan mengimplementasikan algoritma LBP dan RBM sebagai metode ekstraksi fitur yang digunakan. Sistem yang dirancang merupakan hasil dari tahapan pembacaan data dari *dataset* OULU-NPU, *image filtering*, *augmentation* berupa *face detection* dan *cropping* serta *resizing* untuk memperoleh bagian wajahnya saja untuk diproses kembali. Kemudian data wajah ekstraksi fitur menggunakan metode LBP dan RBM, dan terakhir merupakan pembangunan model klasifikasi dengan *classifier* MLP dan CNN.
2) Dari rancangan model sistem yang telah dibuat, penulis telah berhasil mengimplementasikannya menjadi sebuah sistem dalam bahasa pemrograman *python*. Sistem *face presentation attack detection* yang dibangun telah digunakan untuk melakukan 8 jenis eksperimen *training* model dari *dataset* yang dimiliki dan menghasilkan prediksi tipe wajah dari data. Sistem ini juga dapat mendeteksi tipe wajah yang ditangkap oleh kamera yang terhubung dengan sistem dan akan menampilkan hasil prediksi pada antarmuka sistem.
3) Setelah hasil eksperimen diperoleh, penulis telah berhasil mengevaluasi sistem yang dibangun berdasarkan tingkat akurasi dan *error* dari setiap model sistem. Dari kedelapan eksperimen pengujian model diperoleh tingkat akurasi model terbaik oleh model 1.1 yang mengimplementasikan metode ekstraksi fitur LBP dengan tingkat akurasi model sebesar 98% dan *error* yang dihitung dengan HTER sebesar 2%. Meskipun hasil ini tidak

terlalu jauh perbedaannya jika dibandingkan dengan hasil terbaik dari metode ekstraksi fitur lain yaitu dengan model RBM 2.4 yang hanya berbeda 3% lebih kecil dan 8% lebih kecil dari model LBP-RBM 3.3.

4) Penulis juga telah berhasil melakukan analisis eksperimen model sistem *face presentation attack detection* yang telah dibangun berdasarkan masing-masing metode ekstraksi fiturnya. Hasil analisis eksperimen menunjukkan bahwa metode ekstraksi fitur LBP mengekstraksi fitur tekstur gambar. Sedangkan metode ekstraksi fitur RBM mengekstraksi pola data. Dari kedua metode memiliki perbedaan fitur yang diekstraknya sehingga menyebabkan hasil yang kurang cocok ketika digabungkan.

5.2 Saran

Dari penelitian tentang *face presentation attack detection* yang telah dilakukan tentu masih terdapat banyak kekurangan. Sehingga pada sub bab ini terdapat beberapa saran yang dapat dipertimbangkan untuk penelitian selanjutnya, yaitu:

1) Karena keterbatasan perangkat yang digunakan dan lamanya waktu training sehingga eksperimen yang dilakukan menjadi lebih terbatas, sehingga pada kesempatan lain skenario eksperimen dapat ditambahkan.
2) Pada tahap ekstraksi fitur menggunakan metode RBM pada model LBP-RBM proses *training* masih mengalami *underfitting*, sehingga dapat dilakukan *training* kembali dengan menambahkan *component* RBM nya.
3) Model yang dibangun merupakan hasil pengolahan citra yang berfokus hanya pada bagian wajah saja. Sehingga kedepannya dalam membangun model *face presentation attack detection* yang untuk *attack* jenis *photo* dan *video*, citra yang diolah dapat dipertimbangkan dengan mengolah *background* pada citra juga meskipun biaya dan waktu komputasi menjadi lebih tinggi.
4) Model yang dibangun masih terbatas untuk mendeteksi *attack* jenis *photo* dan *video*, sedangkan tipe attack akan terus bertambah. Sehingga kedepannya dapat ditambahkan jenis *attack* yang dapat dikenali.

5) Dari hasil simulasi yang dilakukan dapat diketahui bahwa kegagalan prediksi juga disebabkan oleh variasi data *test* yang tidak tersedia pada *training set*, sehingga kedepannya agar dapat menambah variasi *training set* sesuai kebutuhan.
6) Pada penelitian yang dilakukan, data diklasifikasikan kedalam dua kelas yaitu *real* dan *attack*. Pada penelitian selanjutnya dapat pertimbangkan untuk mengelompokkan data secara lebih detail dengan mengenali kelas *attack* sesuai jenis *attack*-nya.