RISET TENAGA PENGAJAR

LAPORAN AKHIR

SISTEM DETEKSI WAJAH PALSU MENGGUNAKAN ARSITEKTUR MOBILENETS

Oleh:
I Kadek Dendy Senapartha, S.T., M.Eng.
Gabriel Indra Widi Tamtama, S.Kom., M.Kom

FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS KRISTEN DUTA WACANA
NOVEMBER 2022

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

RINGKASAN

Sistem pengenalan wajah merupakan salah satu metode dalam teknik *biometric* yang menggunakan wajah untuk proses identifikasi dan verifikasi seseorang. Teknologi pengenalan wajah saat ini menjadi *booming* dikarenakan tidak memerlukan kontak fisik seperti verifikasi sidik jari. Terdapat dua fase utama dalam sistem biometrik pengenalan wajah otomatis, yaitu pengenalan wajah palsu (*Presentation Attack* (PA) *detection*) dan pengenalan wajah (*face recognition*). Penelitian ini melakukan eksperimen untuk membangun sebuah model pembelajaran mesin (*machine learning*) untuk melakukan deteksi wajah palsu ataupun memverifikasi keaslian wajah yang pengguna menggunakan arsitektur Mobilenets.

Model *antispoof* wajah dibangun dengan menggunakan arsitektur MobilenetV2 dengan menambahkan 3 layer *neural network* yang digunakan sebagai layer klasifikasi. Model dilatih dengan menggunakan 3 jenis dataset publik, yaitu REPLAY-Mobile, RECOD-MPAD, dan LLC-FSAD. Kemudian pengujian secara terkontrol dilakukan dengan menggunakan program komputer menghasilkan nilai HTER 0.17. sedangkan hasil pengujian secara tidak terkontrol menggunakan aplikasi prototipe Android menghasilkan nilai HTER sebesar 0.21. Dari hasil pengujian ini menghasilkan selisih nilai HTER sebesar 0.04 yang mengindikasikan bahwa model *antispoof* wajah akan memiliki performa yang cenderung menurun bila digunakan secara *real*.

BAB I
PENDAHULUAN

1.1 Latar Belakang

Sistem pengenalan diri merupakan salah satu cabang ilmu dari biometrika yang menggunakan bagian tubuh atau perilaku manusia. Sistem akan mencari dan mencocokkan identitas seseorang dengan basis data acuan yang sudah dibuat sebelumnya melalui proses pendaftaran. Sidik jari merupakan salah satu contoh dari biometrika untuk mengenali dan mengidentifikasi seseorang berdasarkan bagian dari tubuh manusia. Beberapa contoh manfaat penerapan biometrika dapat dijumpai dalam sistem presensi kehadiran maupun sistem keamanan.

Perkembangan perangkat komputer saat ini telah memungkinkan seseorang untuk melakukan autentikasi biometri secara otomatis. Dan semenjak pandemik Covid-19, sistem biometrik ini semakin luas diadopsi pada berbagai sektor seperti pembayaran *on-line* dan *e-commerce*, autentikasi berbasis smartphone, dan sistem akses kontrol keamanan. Sistem autentikasi wajah dengan merupakan salah satu sistem yang popular digunakan pada berbagai perangkat [1].

Terdapat dua fase utama dalam sistem biometrik pengenalan wajah otomatis, yaitu pengenalan wajah palsu (*Presentation Attack* (PA) *detection*) dan pengenalan wajah (*face recognition*). Sistem ini dapat menerapkan dua jenis skema yaitu skema paralel atau skema serial. Pada skema paralel, fase PA *detection* dan pengenalan wajah dilakukan secara bersamaan, sedangkan pada skema serial, fase PA *detection* dilakukan sebelum melakukan pengenalan wajah. Penggunaan metode *deep learning* menjadi sangat popular digunakan karena saat ini merupakan *state-of-the-art* pada area tersebut [2].

Studi literatur yang telah dilakukan [2], merangkum metode-metode *deep learning* untuk membuat sistem PA *detection*. Metode yang digunakan adalah *binary cross-entropy loss* (*Binary* CE *loss*) atau *pixel-wise supervision.* Metode *binary CE loss* menggunakan asumsi bahwa PA *detection* merupakan permasalahan klasifikasi biner, yaitu wajah asli atau wajah palsu. Sedangkan metode *pixel-wise* berusaha menggali informasi lebih mendalam dengan cara menganalisis texture gambar wajah dengan menggunakan pola-pola tertentu. Arsitektur MobileNets merupakan arsitektur *deep learning* yang didesain untuk perangkat bergerak dan *embedded* [3].

Melihat beberapa tinjauan yang sudah dilakukan, penelitian ini akan membuat suatu model PA *detection* menggunakan arsitektur MobileNets yang merupakan salah satu metode

dalam *deep learning.* Tujuan dari penelitian ini adalah membuat model yang bersifat *light-weight* sehingga dapat digunakan dalam perangkat bergerak untuk membedakan wajah yang palsu dengan yang asli secara *real-time*.

1.2 Perumusan Masalah

Mempertimbangkan latar belakang masalah yang ada, maka masalah untuk penelitian ini dapat dirumuskan yakni bagaimana performa MobileNets bila digunakan untuk PA *detection*?

1.3 Batasan Masalah

Beberapa batasan masalah yang ada untuk penelitian ini yaitu:

1. Penelitian ini hanya berfokus pada sistem PA *detection*.
2. Prototipe aplikasi yang dibangun berbasis perangkat bergerak.
3. Data *training* berupa foto wajah yang palsu dan asli menggunakan set data *antispoof* wajah publik.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah

1. Mengimplementasikan sebuah model *machine learning* dan aplikasi *mobile* yang dapat melakukan menentukan keaslian wajah tersebut dengan menggunakan arsitektur MobileNets.
2. Meningkatkan kualitas dan kapabilitas dosen dalam mengembangkan bahan ajar maupun publikasi karya.
3. Mengembangkan bahan ajar kepada mahasiswa berkaitan dengan *machine learning, computer vision,* dan *deep learning.*

1.5 Manfaat Penelitian

Penelitian ini dapat meningkatkan pengetahuan tentang pemanfaatan biometri dan pengembangannya dalam berbagai aspek kehidupan sehari-hari.

1.6 Luaran Penelitian

Luaran yang diharapkan pada penelitian ini adalah:

1. Model *machine learning* dan prototipe aplikasi perangkat bergerak.
2. Artikel ilmiah pada prosiding seminar lokal atau nasional.

BAB VII
KESIMPULAN DAN SARAN

7.1.Kesimpulan

Model *antispoof* wajah yang dibangun dengan menggunakan arsitektur MobileNet telah berhasil dibangun dan digunakan. Pengujian secara terkontrol menggunakan program komputer menghasilkan nilai HTER 0.17 sedangkan hasil pengujian secara tidak terkontrol pada aplikasi prototipe Android menghasilkan nilai HTER sebesar 0.21. Dari hasil pengujian ini terdapat selisih nilai HTER sebesar 0.04 yang mengindikasikan bahwa model *antispoof* wajah akan memiliki performa yang cendrung menurun bila digunakan secara *real*. Ini mungkin dapat disebabkan oleh beberapa faktor seperti kualitas kamera yang ada, tingkat pencahayaan saat sistem digunakan dan sudut tangkap wajah terhadap kamera.

7.2.Saran

Model *antispoof* wajah perlu dibangun dan dilatih dengan menggunakan dataset yang lebih banyak dan bervariatif. Selain itu, motede *antispoof* wajah dapat menggunakan metode selain *machine learning* dan *deep learning* seperti memprediksi jumlah kedipan mata. Dengan demikian sistem *antispoof* wajah dapat menjadi lebih tangguh menghadapi berbagai jenis serangan. Selain itu pengujian lebih jauh perlu dilakukan untuk membuktikan faktor-faktor yang menentukan performa model pada pengguna yang sebenarnya.

DAFTAR PUSTAKA

[1] S. Chakraborty and D. Das, "An Overview of Face Liveness Detection," *Int. J. Inf. Theory*, vol. 3, no. 2, pp. 11–25, Apr. 2014, doi: 10.5121/ijit.2014.3202.

[2] Z. Yu, Y. Qin, X. Li, C. Zhao, Z. Lei, and G. Zhao, "Deep Learning for Face Anti-Spoofing: A Survey." arXiv, May 16, 2022. Accessed: Jul. 20, 2022. [Online]. Available: http://arxiv.org/abs/2106.14948

[3] A. G. Howard *et al.*, "MobileNets: Efficient Convolutional Neural Networks for Mobile Vision Applications." arXiv, Apr. 16, 2017. Accessed: Jul. 20, 2022. [Online]. Available: http://arxiv.org/abs/1704.04861

[4] W. Z. Khan, E. Ahmed, S. Hakak, I. Yaqoob, and A. Ahmed, "Edge computing: A survey," *Future Gener. Comput. Syst.*, vol. 97, pp. 219–235, Aug. 2019, doi: 10.1016/j.future.2019.02.050.

[5] Z. Ming, M. Visani, M. M. Luqman, and J.-C. Burie, "A Survey On Anti-Spoofing Methods For Face Recognition with RGB Cameras of Generic Consumer Devices." arXiv, Oct. 08, 2020. Accessed: Jul. 20, 2022. [Online]. Available: http://arxiv.org/abs/2010.04145

[6] I. K. D. Senapartha, "Studi Literatur Presentation Attack dan Set Data Anti-Spoof Wajah," vol. 14, no. 1, p. 8, 2022.

[7] A. Costa-Pazo, S. Bhattacharjee, E. Vazquez-Fernandez, and S. Marcel, "The Replay-Mobile Face Presentation-Attack Database," in *2016 International Conference of the Biometrics Special Interest Group (BIOSIG)*, Darmstadt, Sep. 2016, pp. 1–7. doi: 10.1109/BIOSIG.2016.7736936.

[8] W. R. Almeida *et al.*, "Detecting face presentation attacks in mobile devices with a patch-based CNN and a sensor-aware loss function," *PLOS ONE*, vol. 15, no. 9, p. e0238058, Sep. 2020, doi: 10.1371/journal.pone.0238058.

[9] D. Timoshenko, K. Simonchik, V. Shutov, P. Zhelezneva, and V. Grishkin, "Large Crowdcollected Facial Anti-Spoofing Dataset," in *2019 Computer Science and Information Technologies (CSIT)*, Yerevan, Armenia, Sep. 2019, pp. 123–126. doi: 10.1109/CSITechnol.2019.8895208.

[10] S. Ioffe and C. Szegedy, "Batch Normalization: Accelerating Deep Network Training by Reducing Internal Covariate Shift." arXiv, Mar. 02, 2015. Accessed: Jul. 25, 2022. [Online]. Available: http://arxiv.org/abs/1502.03167

[11] N. Srivastava, G. Hinton, A. Krizhevsky, I. Sutskever, and R. Salakhutdinov, “Dropout: A Simple Way to Prevent Neural Networks from Overfitting,” p. 30.

[12] F. Zhuang *et al.*, “A Comprehensive Survey on Transfer Learning.” arXiv, Jun. 23, 2020. doi: 10.48550/arXiv.1911.02685.

[13] J. Deng, W. Dong, R. Socher, L.-J. Li, K. Li, and L. Fei-Fei, “ImageNet: A Large-Scale Hierarchical Image Database,” p. 8.

[14] B. Pang, E. Nijkamp, and Y. N. Wu, “Deep Learning With TensorFlow: A Review,” *J. Educ. Behav. Stat.*, vol. 45, no. 2, pp. 227–248, Apr. 2020, doi: 10.3102/1076998619872761.

[15] R. David *et al.*, “TensorFlow Lite Micro: Embedded Machine Learning on TinyML Systems.” arXiv, Mar. 13, 2021. Accessed: Aug. 01, 2022. [Online]. Available: http://arxiv.org/abs/2010.08678

[16] “Illuminance - Recommended Light Level,” *Illuminance - Recommended Light Level*. https://www.engineeringtoolbox.com/light-level-rooms-d_708.html (accessed Nov. 02, 2022).