

PENGEMBANGAN *ONE-CLASS KNOWLEDGE DISTILLATION* DENGAN INTEGRASI OC-SOFTMAX DAN *ATTENTIVE TEMPORAL POOLING* PADA DETEKSI AUDIO ANTI-SPOOFING

Nama Mahasiswa : Nabila Chairunnisa
NIM : 11221005
Dosen Pembimbing Utama : Bima Prihasto, S.Si., M.Si., Ph.D
Dosen Pembimbing Pendamping : Bobby Mugi Pratama, S.Si., M.Han.

ABSTRAK

Perkembangan teknologi kecerdasan buatan telah memicu peningkatan keamanan berupa serangan *audio spoofing* atau *deepfake audio*, yang sekarang semakin sulit dibedakan dari suara asli (*bona fide*). Sebagian besar penelitian deteksi *audio anti-spoofing* saat ini masih berfokus pada klasifikasi biner menggunakan dataset berbahasa Inggris, yang sering mengalami penurunan performa ketika dihadapkan pada serangan yang belum pernah ditemui sebelumnya (*unseen attacks*), variasi linguistik, dan gangguan lingkungan (*noise*). Penelitian ini bertujuan untuk membangun sistem deteksi *audio anti-spoofing* bahasa Indonesia yang efisien dan tangguh melalui pendekatan *One-Class Knowledge Distillation* (OCKD). Menggunakan skema *teacher-student*, model *teacher* (ResNet-50) mentransfer representasi fiturnya kepada *student* (ResNet-18) melalui fungsi *loss* MSE dan *Cosine Similarity*. Strategi *one-class learning* dengan fungsi *loss One-Class Softmax* (OC-Softmax) diterapkan pada model *student* untuk memodelkan distribusi suara *bona fide* secara spesifik agar serangan akan dianggap sebagai anomali. Selain itu, mekanisme *Attentive Temporal Pooling* (ATP) diintegrasikan untuk meningkatkan kemampuan model dalam menangkap variasi sinyal audio dari segi temporal. Ekstraksi fitur dilakukan menggunakan *Linear Frequency Cepstral Coefficients* (LFCC). Hasil penelitian menunjukkan bahwa dalam kondisi bersih, model yang diusulkan berhasil memangkas nilai *Equal Error Rate* (EER) dari 10,0000% menjadi 1,3333% dan mereduksi nilai minimum t-DCF menjadi 0,0133. Pada uji berderau berat dengan SNR 0 hingga 15 dB, model tetap tangguh dan mempertahankan kemampuan generalisasi dengan EER terendah sebesar 35,3333%. Dari segi efisiensi komputasi, kerangka kerja OCKD berhasil mengurangi jumlah parameter sebesar 53,67% menjadi 11,66 M. Waktu inferensi juga dipercepat hingga 54,28% menjadi hanya 1,642 ms dibandingkan dengan model *teacher*.

Kata kunci: *Audio Anti-Spoofing*, *One-Class Knowledge Distillation*, ResNet, LFCC, Bahasa Indonesia