

DAFTAR ISI

Halaman Judul	ii
Halaman Pengesahan	iii
Halaman Pernyataan	iv
Halaman Pernyataan	v
Halaman Persembahan	vi
Halaman Motto	vii
PRAKATA	viii
INTISARI	xviii
ABSTRACT	xix
I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	4
1.3 Tujuan Penelitian	4
1.4 Batasan Masalah	5
1.5 Manfaat Penelitian	6
II TINJAUAN PUSTAKA	7
2.1 Pelatihan Adversarial Teroptimasi Spasial (Rao et al., 2020)	7
2.2 Segment-and-Complete (Liu et al., 2022)	8
2.3 Pertahanan menggunakan Lapisan Konvolusi Gabor (Amirkhani dan Karimi, 2022)	9
2.4 Certifiable Robustness dalam Vision Transformer Menggunakan Derandomized Smoothing (Chen et al., 2022)	9
2.5 Pertahanan Menggunakan Compressive Sensing (Wang et al., 2022)	10

2.6	TaintRadar, Pertahanan Menggunakan Analisa Critical Region (Li et al., 2021)	11
2.7	Knowledge Enhanced Machine Learning Pipeline (GÃijrel et al., 2021)	11
2.8	Pertahanan Berbasis Entropi, JEDI (Tarchoun et al., 2023)	12
2.9	Signals Are All You Need: Mendeteksi Patch Adversarial Digital dan Fisik Menggunakan Metode <i>Signal Processing</i> (Bunzel et al., 2024 . . .	13
2.10	Pertahanan Berbasis Difusi (Kang et al., 2024)	14
2.11	Jujutsu: Pertahanan Dua Langkah Menggunakan Saliency Map (Chen et al., 2023)	14
2.12	Patch Agnostic Defense (Jing et al., 2024)	15
2.13	Kontribusi dan Kebaharuan Penelitian	16
III LANDASAN TEORI		19
3.1	Serangan Adversarial	19
3.2	Serangan Adversarial Blackbox	21
3.3	Handcrafted Feature	23
3.3.1	Fitur tekstur	24
3.3.2	Fitur warna	24
3.4	Otsu Thresholding	25
3.5	Random Forest Classifier	25
3.6	XGBoost Classifier	26
3.7	Kompresi JPEG	28
3.8	Entropi dan <i>Mutual Information Citra</i>	29
3.9	Deteksi Objek YOLO	31
3.10	Generative Adversarial Network	32
3.11	GAN Inpainting	33
3.12	Structural Similarity Index Measure (SSIM)	37
3.13	Fréchet Inception Distance (FID)	38
IV RANCANGAN SISTEM		40
4.1	Alur Kerja Penelitian	40
4.2	Arsitektur Sistem	41
4.3	Dataset	42
4.4	Skenario Penyerangan	42

4.5	Metode Segmentasi	44
4.5.1	Segmentasi berbasis rekompresi	44
4.5.2	Segmentasi berbasis <i>mutual information</i>	48
4.6	Ekstraksi dan Representasi Fitur	49
4.7	Metode Klasifikasi	50
4.8	Inpainting GAN	53
4.9	Pengujian dan Evaluasi	58
4.9.1	Studi kualitatif	58
4.9.2	Studi komparatif	59
V	IMPLEMENTASI	61
5.1	Alat dan Bahan	61
5.2	Pustaka Software yang Digunakan	61
5.3	<i>Source Code</i>	62
5.3.1	Implementasi aplikator <i>adversarial patch</i> dan penyiapan dataset	63
5.3.2	Implementasi metode segmentasi berbasis rekompresi citra . . .	66
5.3.3	Implementasi metode segmentasi alternatif berbasis entropi in- formasi	71
5.3.4	Implementasi perhitungan <i>modified IoU</i>	71
5.3.5	Implementasi ekstraksi fitur dan klasifikasi	74
5.3.6	Implementasi pembangkit dataset masker biner latih <i>Inpainting</i> GAN	81
5.3.7	Implementasi generator <i>Inpainting</i> GAN	81
VI	HASIL DAN PEMBAHASAN	87
6.1	Skenario 1 & 2: Performa <i>Baseline</i> Model Deteksi Objek	87
6.2	Skenario 3: Performa Segmentasi Model Berbasiskan Rekompresi Citra	89
6.2.1	Ablasi metode segmentasi	95
6.3	Skenario 4: Performa Segmentasi Alternatif Model Berbasiskan Entropi Citra	97
6.4	Skenario 5: Performa Segmentasi Model Pada Ukuran Patch Alternatif .	101
6.5	Skenario 6: Performa Ekstraksi Fitur dan Klasifikasi	102
6.6	Skenario 7: Deteksi patch <i>end-to-end</i>	107
6.7	Skenario 8: Evaluasi detektor pada citra terekonstruksi	110

6.8	Analisa dan Diskusi	115
6.8.1	Analisa struktural rekonstruksi citra	119
VII KESIMPULAN DAN SARAN		122
7.1	Kesimpulan	122
7.2	Saran	124