

DAFTAR ISI

HALAMAN PERSETUJUAN.....	i
PERNYATAAN BEBAS PLAGIASI.....	ii
PRAKATA.....	iii
DAFTAR ISI.....	v
DAFTAR GAMBAR.....	x
DAFTAR TABEL.....	xii
INTISARI.....	xiv
ABSTRACT.....	xv
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	4
1.3 Batasan Masalah.....	4
1.4 Tujuan Penelitian.....	5
1.5 Manfaat Penelitian.....	5
BAB II TINJAUAN PUSTAKA.....	6
BAB III LANDASAN TEORI.....	14
3.1 Serangan Adversarial.....	14
3.1.1 Fast Gradient Sign Method.....	15
3.1.2 Projected Gradient Descent.....	15
3.1.3 Carlini & Wagner.....	16
3.1.4 DeepFool.....	17

3.1.5	One-Pixel Attack	18
3.2	Radiografi Dada	19
3.2.1	Pneumonia.....	20
3.3	Fundus Retina.....	20
3.3.1	Diabetic Retinopathy.....	21
3.4	Augmentasi.....	22
3.5	Convolutional Neural Network	23
3.5.1	Input Layer	23
3.5.2	Convolutional Layer.....	24
3.5.3	Pooling Layer	25
3.5.4	Batch Normalization	26
3.5.5	Dropout Layer	26
3.5.6	Activation.....	27
3.5.7	Fully Connected Layer	28
3.6	XceptionNet.....	28
3.7	Pertahanan Adversarial.....	30
3.8	Denoising.....	30
3.8.1	Denoising AutoEncoder	31
3.8.2	Feature Denoising Block.....	32
3.9	Convolutional Block Attention Module	33
3.10	Evaluasi	34
BAB IV METODOLOGI PENELITIAN		38
4.1	Gambaran Umum Penelitian	38

4.2	Dataset	39
4.3	Pra-pemrosesan	41
4.4	Augmentasi.....	41
4.5	Arsitektur Basis Model.....	42
4.6	Serangan Adversarial.....	44
4.6.1	Fast Gradient Sign Method	46
4.6.2	Projected Gradient Descent.....	46
4.6.3	Carlini & Wagner	46
4.6.4	DeepFool.....	47
4.6.5	One-Pixel Attack	47
4.7	Pertahanan Adversarial.....	48
4.7.1	Denoising AutoEncoder	49
4.7.2	Convolutional Block Attention Module.....	50
4.7.3	Selective Feature Denoising Block.....	51
4.8	Parameter Tuning	53
4.9	Skenario Pengujian.....	53
4.10	Evaluasi	54
BAB V IMPLEMENTASI SISTEM.....		55
5.1	Alat dan Bahan	55
5.2	Pra-pemrosesan	55
5.3	Augmentasi.....	57
5.4	Basis Model.....	58
5.5	Serangan Adversarial.....	59

5.5.1	Fast Gradient Sign Method	60
5.5.2	Projected Gradient Descent.....	61
5.5.3	Carlini & Wagner	63
5.5.4	DeepFool.....	66
5.5.5	One-Pixel Attack	68
5.6	Pertahanan Adversarial.....	72
5.6.1	Denoising AutoEncoder	73
5.6.2	Convolutional Block Attention Module	74
5.6.3	Selective Feature Denoising Block.....	75
5.7	Evaluasi	77
BAB VI HASIL DAN PEMBAHASAN.....		80
6.1	Augmentasi.....	80
6.2	Basis Model.....	81
6.3	Serangan Adversarial.....	83
6.3.1	Fast Gradient Sign Method	87
6.3.2	Projected Gradient Descent.....	88
6.3.3	Carlini & Wagner	89
6.3.4	DeepFool.....	90
6.3.5	One-Pixel Attack	91
6.4	Pertahanan Adversarial.....	93
6.4.1	Denoising AutoEncoder	95
6.4.2	Convolutional Block Attention Module	96
6.4.3	Feature Denoising Block.....	97

6.4.4	Kombinasi dan Mekanisme Selektif	99
6.5	Perbandingan Hasil.....	104
BAB VII KESIMPULAN DAN SARAN		110
7.1	Kesimpulan.....	110
7.2	Saran	111
DAFTAR PUSTAKA		112