

CONTENTS

APPROVAL PAGE

SELF DECLARATION AGAINST PLAGIARISM

ABSTRACT iv

ACKNOWLEDGEMENTS v

PREFACE vi

CONTENTS vii

LIST OF FIGURES x

LIST OF TABLES xi

LIST OF ABBREVIATION xii

LIST OF SYMBOL xiii

1 INTRODUCTION 1

- 1.1 Background 1
- 1.2 Research Objective 2
- 1.3 Problem Statement 3
- 1.4 Hypothesis 4
- 1.5 Research Methodology 4
- 1.6 Problem Limitation 5

ACHIEVEMENT 1

2 BASIC CONCEPT 6

- 2.1 Watermark 6
 - 2.1.1 Digital Watermarking 7
 - 2.1.2 Watermarking at the Point of Origin 8
 - 2.1.3 Types of Watermarking 8
- 2.2 Deep Neural Network 9

2.3	Architecture of Deep Neural Networks	9
2.3.1	Input Layer	10
2.3.2	Hidden Layers	10
2.3.3	Output Layer	10
2.4	Training Deep Neural Networks	11
2.4.1	Backpropagation	11
2.4.2	Regularization Techniques	11
2.5	Applications of Deep Neural Networks	11
2.6	Wet Paper Coded based on Deep Neural Network	12
2.6.1	Optimal Parameter Selection Strategy (OPSS)	13
2.7	Backdoor Attack	14
2.7.1	Impact and Security Concerns	15
2.7.2	Defenses Against Backdoor Attacks	15
2.7.3	Data Sanitization	15
2.7.4	Model Inspection	16
2.7.5	Input Anomaly Detection	16
2.7.6	Adversarial Training	17
2.8	Siamese Neural Network	18
2.9	Previous Research	19
3	SYSTEM MODEL AND THE PROPOSED DESIGN	21
3.1	General System	21
3.2	Watermarking Process Overview	22
3.2.1	The Watermark Embedding Process	23
3.2.2	The Watermark Extraction Process	27
3.3	Parameter	29
3.4	Detection Backdoor Attack Using Siamese Neural Network	30
3.4.1	Training Siamese Neural Network	30
3.4.2	Testing Siamese Neural Network	36
3.5	Performance Model	36
4	PERFORMANCE EVALUATIONS	41
4.1	Performance Environment	41
4.1.1	Training the Model with Wet Paper Coding (WPC)	41
4.1.2	Watermark Detection Using Siamese Neural Network (SNN)	41
4.2	Watermark Performance Evaluation	42
4.2.1	Impact Dataset On Watermarking Performance	43
4.2.2	Impact Layer Ratio on Watermarking Performance	44

4.2.3	Impact Alpha Prob On Watermarking Performance	45
4.2.4	Impact Dry Block Ratio On Watermarking Performance . . .	46
4.2.5	Best Configuration Recommendations	47
4.2.6	Fidelity Evaluation	48
4.3	Performance Detection Backdoor Attack	49
4.3.1	Result Watermarked as Dataset	50
4.3.2	Training Model Siamese Neural Network	51
4.3.3	Model Evaluation	51
4.4	Comparison with Previous Research	53
5	CONCLUSION	55
5.1	Conclusion	55
5.2	Future Work	56
	REFERENCES	57
	LAMPIRAN	1
	LAMPIRAN	1