

TABLE OF CONTENT

UNDERGRADUATE THESIS	i
PAGE OF APPROVAL	ii
STATEMENT	iii
MOTTO AND OFFERING PAGE	iv
PREFACE	v
ABBREVIATIONS AND ACRONYMS	vi
TABLE OF CONTENT	vii
LIST OF FIGURES	x
LIST OF TABLES	xii
ABSTRACT	xiii
CHAPTER I. INTRODUCTION	1
1.1 Background	1
1.2 Research Problem	4
1.3 Research Scope.....	4
1.4 Research Objectives.....	4
1.5 Research Benefits	5
1.6 Research Methodology	5
1.7 Thesis Organization	6
CHAPTER II. LITERATURE REVIEW.....	7
CHAPTER III. THEORETICAL FRAMEWORK.....	12
3.1 Classical Cryptosystem.....	12
3.2 Symmetric Key Cryptosystem.....	12
3.3 Asymmetric Key Cryptosystem	13
3.4 Homomorphic Cryptosystem	14
3.5 Paillier's Cryptosystem.....	15
3.6 Machine Learning.....	16
3.6.1 Supervised Learning	17
3.6.2 Unsupervised Learning	17

3.7	Artificial Neural Network	17
3.8	Convolutional Neural Network	19
3.8.1	Input Layer	20
3.8.2	Convolutional Layer	20
3.8.3	Pooling Layer	21
3.8.4	Fully Connected Layer.....	23
CHAPTER IV. ANALYSIS AND DESIGN		25
4.1	Research Description	25
4.2	Research Data.....	25
4.3	Model Design	26
4.3.1	Data Gathering	27
4.3.2	Key Pair Generation	28
4.3.3	Model Initiation	29
4.3.4	Data Pre-processing	30
4.3.5	Encryption of Testing Data	31
4.3.6	Model Training	32
4.3.7	Modification of CNN Model.....	32
4.3.8	Model Testing.....	38
4.3.9	Decryption of Testing Predictions	39
4.3.10	Result Matching.....	40
4.4	Evaluation Design.....	41
CHAPTER V. IMPLEMENTATION.....		42
5.1	Hardware and Software Specifications	42
5.2	Model Implementation.....	42
5.2.1	Data Gathering	43
5.2.2	Key Pair Generation	44
5.2.3	Model Initiation	46
5.2.4	Data Pre-processing	47
5.2.5	Encryption of Testing Data	49
5.2.6	Model Training	49
5.2.7	Modification of CNN Model.....	50

5.2.8	Model Testing.....	50
5.2.9	Decryption of Testing Predictions.....	50
5.2.10	Result Matching.....	51
CHAPTER VI. RESULTS AND DISCUSSIONS		52
6.1	Results.....	52
6.1.1	Key Pair Generation	52
6.1.2	Data Preprocessing	54
6.1.3	Encryption of Testing Data	54
6.1.4	Model Training.....	55
6.1.5	Result Matching.....	56
6.2	Discussions.....	56
6.2.1	Successful Classification using CNN on Encrypted Data	57
6.2.2	Unavailability of Non-Linear Activation Function	57
6.2.3	The Unsuitability of using K-Fold Cross-Validation	59
CHAPTER VII. CONCLUSION AND FUTURE WORK.....		60
7.1	Conclusion.....	60
7.2	Future Work	60
REFERENCES		61