

# TABLE OF CONTENTS

<b>APPROVAL</b>	<b>i</b>
<b>SELF DECLARATION AGAINST PLAGIARISM</b>	<b>ii</b>
<b>ABSTRACT</b>	<b>iii</b>
<b>ABSTRAK</b>	<b>iv</b>
<b>ACKNOWLEDGEMENTS</b>	<b>v</b>
<b>LIST OF CONTENTS</b>	<b>vi</b>
<b>List of Figures</b>	<b>x</b>
<b>List of Tables</b>	<b>xii</b>
<b>Abbreviations</b>	<b>xv</b>
<b>Terms</b>	<b>xvii</b>
<b>Symbols</b>	<b>xxi</b>
<b>1 INTRODUCTION</b>	<b>1</b>
1.1 Rationale . . . . .	1
1.2 Theoretical Framework . . . . .	2
1.3 Conceptual Framework . . . . .	3
1.4 Problem Statements . . . . .	4
1.5 Hypothesis . . . . .	5
1.6 Assumption . . . . .	7
1.7 Scope and Delimitation . . . . .	7
1.8 Importance of The Study . . . . .	8
<b>2 REVIEW OF LITERATURE AND STUDIES</b>	<b>9</b>
2.1 Related Literature . . . . .	9
2.1.1 Visual Cryptography . . . . .	9
2.1.1.1 VCS Model . . . . .	10
2.1.1.2 2 out of 2 VCS Construction . . . . .	13

---

2.1.2	Non-Identical Mathematical Support . . . . .	14
2.1.3	Alignment Problem . . . . .	16
2.1.4	Liu et.al's Alignment Method . . . . .	18
2.1.4.1	Basic Construction . . . . .	19
2.1.4.2	Implementation of Liu et.al's Method . . . . .	21
2.1.4.3	(2,2)-VCS Construction with Liu et.al's Method . . . . .	24
2.2	Related Studies . . . . .	27
2.2.1	Chameleon Hash Function . . . . .	27
2.2.1.1	The Properties of Chameleon Hash Function . . . . .	27
2.2.1.2	The Scheme of Chameleon Hash Function . . . . .	28
2.2.1.3	The Construction of Chameleon Hash Function . . . . .	30
2.3	Probability . . . . .	31
2.4	Entropy . . . . .	33
2.4.1	Marginal Entropy . . . . .	33
2.4.2	Joint Entropy and Conditional Entropy . . . . .	34
2.4.3	Mutual Information and Dependence Reduction . . . . .	35
2.5	Perfect Secrecy . . . . .	37
2.5.1	Perfect Secrecy on OTP . . . . .	38
2.5.2	Perfect Secrecy on IMSVCS . . . . .	39
2.5.3	Perfect Secrecy on NIMSVCS . . . . .	42
<b>3</b>	<b>RESEARCH METHODOLOGY</b> . . . . .	<b>44</b>
3.1	Research Design . . . . .	44
3.1.1	Encoding . . . . .	49
3.1.1.1	Pre-Decomposing . . . . .	51
3.1.1.2	Decomposing . . . . .	64
3.1.1.3	Post-Decomposing . . . . .	76
3.1.2	Decoding . . . . .	78
3.1.2.1	Calculating <i>3OP</i> . . . . .	79
3.1.2.2	Stacking . . . . .	81
3.2	Experiment Scenario . . . . .	85
3.2.1	Functionality Analysis . . . . .	86
3.2.1.1	Functionality in Identical Mathematical Support VCS . . . . .	86
3.2.1.2	Functionality in Non-Identical Mathematical Support VCS . . . . .	87
3.2.2	Time Complexity Analysis . . . . .	87
3.2.2.1	Time Complexity Requirement in Identical Mathematical Support VCS . . . . .	88
3.2.2.2	Time Complexity Requirement in Non-Identical Mathematical Support VCS . . . . .	89
3.2.3	Security Analysis . . . . .	92
3.3	Population or Samples . . . . .	92
3.3.1	Chameleon Variables . . . . .	93
3.3.2	Basis Matrices . . . . .	93

---

3.3.3	Data Used in Functional Experiment . . . . .	94
3.3.3.1	Data of Functional Experiment for Identical Mathematical Support <i>VCS</i> . . . . .	94
3.3.3.2	Data of Functional Experiment for Non Identical Mathematical Support <i>VCS</i> . . . . .	95
3.3.4	Data Used in Time Complexity Experiment . . . . .	97
3.3.4.1	Data of Time Complexity Experiment for Identical Mathematical Support <i>VCS</i> . . . . .	97
3.3.4.2	Data of Time Complexity Experiment for Non Identical Mathematical Support <i>VCS</i> . . . . .	98
3.4	Data Analysis Tools . . . . .	104
3.4.1	Data Analysis Tools For Functionality . . . . .	104
3.4.2	Data Analysis Tools For Time Complexity . . . . .	105
3.4.2.1	Identical Mathematical Support <i>VCS</i> . . . . .	105
3.4.2.2	Non Identical Mathematical Support <i>VCS</i> . . . . .	107
3.4.3	Data Analysis Tools For Security . . . . .	109
<b>4</b>	<b>PRESENTATION, ANALYSIS AND INTERPRETATION OF DATA</b>	<b>110</b>
4.1	Presentation of Data . . . . .	110
4.1.1	The Result of The Functional Experiment . . . . .	110
4.1.1.1	The Result of <i>IMSVCS</i> . . . . .	111
4.1.1.2	The Result of <i>NIMSVCS</i> . . . . .	112
4.1.2	The Result of The Time Complexity Experiment . . . . .	113
4.1.2.1	The Result for Identical Mathematical Support <i>VCS</i> ( <i>IMSVCS</i> ) . . . . .	114
4.1.2.2	The Result for Non Identical Mathematical Support <i>VCS</i> ( <i>NIMSVCS</i> ) . . . . .	115
4.2	Data Analysis . . . . .	117
4.2.1	Analysis of The Functionality . . . . .	117
4.2.2	Analysis of The Time Complexity . . . . .	118
4.2.2.1	The Analysis of Identical Mathematical Support <i>VCS</i> . . . . .	118
4.2.2.2	The Analysis of Non Identical Mathematical Support <i>VCS</i> . . . . .	121
4.2.3	Analysis of The Security . . . . .	130
4.3	Summary of Findings . . . . .	134
4.3.1	The Functionality . . . . .	134
4.3.2	The Time Complexity . . . . .	134
4.3.2.1	Identical Mathematical Support <i>VCS</i> . . . . .	134
4.3.2.2	Non Identical Mathematical Support <i>VCS</i> . . . . .	135
4.3.3	The Security . . . . .	136
4.4	Table of Summary . . . . .	137
<b>5</b>	<b>CONCLUSION AND RECOMMENDATIONS</b>	<b>138</b>
5.1	Conclusion . . . . .	138
5.2	Recommendation . . . . .	139

<b>A The Result of Functional Experiment</b>	<b>140</b>
<b>B Data Presentation of Time Complexity Experiment</b>	<b>149</b>
<b>C Curriculum Vitae</b>	<b>153</b>
<b>Bibliography</b>	<b>155</b>