

CONTENTS

APPROVAL.....	I
SELF DECLARATION AGAINST PLAGARISM.....	II
ABSTRACT	III
ABSTRAK	IV
DEDICATION	V
ACKNOWLEDGMENTS.....	VI
PREFACE.....	VII
CONTENTS	VIII
LIST OF TABLES.....	XIII
LIST OF FIGURES.....	XV
CHAPTER 1	1
INTRODUCTION.....	1
1.1 RATIONALE.....	1
1.2 THEORETICAL FRAMEWORK.....	2
1.3 CONCEPTUAL FRAMEWORK.....	3
1.4 PROBLEM STATEMENTS.....	3
1.5 HYPOTHESES	3
1.6 ASSUMPTION.....	4
1.7 SCOPE AND DELIMITATION	4
1.8 IMPORTANCE OF THE STUDY	5
CHAPTER 2	6
2 REVIEW OF LITERATURE AND STUDIES	6
2.1 RELATED LITERATURE	6
2.1.1 Fingerprint Based Authentication System.....	6
2.1.1.1 Fingerprint Feature Extraction.....	7
2.1.1.2 Fingerprint Matching.....	9
2.1.2 Spoofing Attack	10

2.2	RELATED STUDIES	11
2.2.1	Dynamic Biometric	11
2.2.2	Voiceprint	13
2.2.3	Syllable in Indonesian	17
CHAPTER 3		18
3	RESEARCH METHODOLOGY.....	18
3.1	SYSTEM DESIGN AND IMPLEMENTATION	18
3.1.1	Registration Phase	19
3.1.1.1	Word Dictionary Generation.....	20
3.1.1.1.1	Collecting of Words for Registration Phase	21
3.1.1.1.2	Selecting Two Syllable Word	24
3.1.1.2	Selecting Word and Pronunciation to Build Voice Template.....	26
3.1.1.3	Syllable-Based Voice Segmentation.....	29
3.1.1.3.1	Amplitude Normalization	30
3.1.1.3.2	Active Signal Filtering.....	32
3.1.1.3.2.1	Envelope Signal Generation.....	33
3.1.1.3.2.2	Finding Cutter Index.....	34
3.1.1.3.2.3	Transfer Active Signal	37
3.1.1.3.3	Segmenting Voice Signal Based on Syllable	38
3.1.1.4	Syllable Template Selection	41
3.1.1.5	Fingerprint Scanning.....	41
3.1.1.6	Fingerprint Template Selection.....	42
3.1.2	Authentication Phase.....	43
3.1.2.1	Fingerprint Feature Extraction.....	44
3.1.2.2	Fingerprint Matching Strategy	47
3.1.2.2.1	Minutia Tuple Generation.....	48
3.1.2.2.1.1	Search for Five Nearest Minutiae Points.....	48
3.1.2.2.1.2	Ratio Calculation.....	49
3.1.2.2.1.3	Direction Calculation.....	50
3.1.2.2.2	Minutia Tuple Matching	52
3.1.2.3	Word Selecting and Pronunciation	53

3.1.2.4	Voice Feature Extraction	53
3.1.2.4.1	Amplitude Normalization	54
3.1.2.4.2	Active Signal Filtering.....	54
3.1.2.4.3	Voiceprint Generation	54
3.1.2.5	Voice Matching	56
3.1.2.5.1	Template Reconstruction	57
3.1.2.5.2	Time Normalization.....	58
3.1.2.5.3	Cross Correlation.....	60
3.1.2.6	Decision Making.....	61
3.2	EXPERIMENT SCENARIO.....	62
3.2.1	The Capability Evaluation of User Authentication Using Fingerprint and Voice 63	
3.2.1.1	Capability Evaluation of User Authentication Using Fingerprint and Voice of Unenrolled Person Using Words in Existing Database.....	63
3.2.1.2	Capability Evaluation of User Authentication Using Fingerprint and Voice of Unenrolled Person Using Words Which Is Not Existed in Database ..	64
3.2.1.3	Capability Evaluation of User Authentication Using Fingerprint and Voice of Enrolled Person Using Words in Existing Database.....	64
3.2.1.4	Capability Evaluation of User Authentication Using Fingerprint and Voice of Enrolled Person Using Words Which Is Not Existed in Database	65
3.2.2	Security Evaluation of User Authentication Using Fingerprint and Voice Against Spoofing Attack.....	65
3.2.3	Security Evaluation Against Guessing Attack Based on Syllable Occurrence	66
3.3	POPULATION AND SAMPLES	67
3.3.1	Sample for Capability Evaluation.....	67
3.3.1.1	Sample for Training Phase in Capability Evaluation	67
3.3.1.2	Sample for Testing Phase in Capability Evaluation	70
3.3.1	Sample for Security Evaluation Against Spoofing Attack.....	73
3.3.2	Sample for Security Evaluation Against Guessing Attack	73
3.4	DATA ANALYSIS TOOLS	75

CHAPTER 4	76
4 DATA PRESENTATION, ANALYSIS AND INTERPRETATION	76
4.1 PRESENTATION OF DATA.....	76
4.1.1 The Capability Evaluation of User Authentication Using Fingerprint and Voice	76
4.1.1.1 The Capability Evaluation of User Authentication Using Fingerprint and Voice of Unenrolled Person Using Words in Existing Database.....	77
4.1.1.2 The Capability Evaluation of User Verification Using Fingerprint and Voice of Unenrolled Person Using Words Which Is Not Existed in Database ..	79
4.1.1.3 The Capability Evaluation of User Authentication Using Fingerprint and Voice of Enrolled Person Using Words in Existing Database.....	81
4.1.1.4 The Capability Evaluation of User Authentication Using Fingerprint and Voice of Enrolled Person Using Words Which Is Not Existed in Database	83
4.1.2 The Security Evaluation of User Authentication Using Fingerprint and Voice Against Spoofing Attack.....	84
4.1.3 The Security Evaluation Against Guessing Attack Based on Syllable Occurrence	86
4.1.3.1 Number of Words.....	87
4.1.3.2 The Security Evaluation Against Guessing Attack.....	88
4.1.3.2.1 Guessing Attack Based on Brute Force Approach.....	89
4.1.3.2.2 Guessing Attack Based on Conditional Probability.....	89
4.2 ANALYSIS OF DATA	89
4.2.1 Capability Analysis of User Authentication Using Fingerprint and Voice	89
4.2.1.1 Capability Analysis of User Authentication Using Fingerprint and Voice of Unenrolled Person Using Words in Existing Database.....	90
4.2.1.2 Capability Analysis of User Authentication Using Fingerprint and Voice of Unenrolled Person Using Words Which Is Not Existed in Database ..	93
4.2.1.3 Capability Analysis of User Authentication Using Fingerprint and Voice of Enrolled Persons Using Word in Existing Database.....	95

4.2.1.4	Capability Analysis of User Authentication Using Fingerprint and Voice of Enrolled Persons Using Words Which Is Not Exist in Database	100
4.2.2	Security Analysis of User Authentication Using Fingerprint and Voice Against Spoofing Attack	104
4.2.3	Security Analysis Against Guessing Attack Based on Syllable Occurrence	109
4.2.3.1	Number of Words	109
4.2.3.2	Security Analysis Against Guessing Attack	112
4.2.3.2.1	Analysis of Guessing Attack Based on Brute Force Approach	112
4.2.3.2.2	Analysis of Guessing Attack Based on Conditional Probability Approach	113
4.3	SUMMARY OF FINDING	113
CHAPTER 5		115
5 CONCLUSION AND RECOMMENDATIONS		115
5.1	CONCLUSION	115
5.2	RECOMMENDATION	116
BIBLIOGRAPHY		117
APPENDIX A		121
CAPABILITY EVALUATION RESULT		121
APPENDIX B		134
DATASET FOR EXPERIMENT		134