

Sudan University of Science and Technology

College of Graduate Studies

# **Front End Voice CIPHERING**

*A thesis Submitted for partial fulfillment of the M.Sc.  
degree in Computer Engineering*

Presented by:

***Omayya Mohamed Nour Mohamed Saeed***

Supervised by:

***Prof. Saad Daoud Sulaiman***

August 2009

# *Dedication*

*To my parents,,,,,*

*To my husband,,,*

*To my sons,,,*

*To all mothers ho are struggling to  
Contribute to the man kind development beyond  
their natural role.*

## Acknowledgement

*I would like to express my deep grateful to my Supervisor, Dr. Saad Daoud Sulaiman, for his guidance and support throughout the stages of this study. He put worth of effort and time for supervising this study.*

*In particular, I would like to thank my husband, for his assistance with reading materials and typing of this thesis.*

*To all those who contributed directly or indirectly to this study I would like to express my sincere appreciation and thankful.*

# **ABSTRACT**

The Atmel AVR microcontrollers are excellent for signal processing applications due to their powerful architecture, strong instruction set and built-in multi-channel 10-bit Analog to Digital Converter (ADC). The megaAVR® series further have a hardware multiplier, which is important in signal processing applications.

This thesis describes the process of designing a ciphering voice and the implementation of an ciphering using an Atmega8535 microcontroller, which is one of At mega Atmel AVR series family of microcontrollers.

The thesis in the first chapters explains the ciphering theory in brief, their main classifications according to the method of the implementation

In the third chapter the thesis establishes in details the information needed for the implementation of voice ciphering in general on AVR microcontrollers firstly, and then focuses on the process of implementing a specific on Atmega8535 from scratch. A program has been written and a circuitry has been built, then results of the implementation are analyzed to support the theory.

## تجريدة

التطبيقات المشتملة على معالجة للبيانات من مصادر تماثلية خارجية (حاساسات) غالبا ما تتطلب بعض انواع الترشيح الرقمي لتلك البيانات قيل توظيفها في الاستجابة لحدث خارجي. في مثل تلك الحالات فإن المتحكمات ذات الخانات الثمانية وذات الستة عشرة خانة تدخل في الصورة.

المتحكمات Atmega AVR متحكمات ممتازة نسبة لبنيتها الفعالة، حزمة تعليماتها القوية، والمحول التماثلي-الرقمي المضمن ذو القنوات المتعددة وذو الخانات الثنائية العشرة. سلسلة mega AVR فوق ذلك، لديها ضارب مادي، وهو مهم جدا لتطبيقات معالجة الاشارة.

البحث في ابوابه الاولى يشرح نظرية المرشحات الرقمية باختصار، الشكل الاساسي للمعادلة العامة لـ "مرشحات الاستجابة النبضية المنتهية" و "مرشحات الاستجابة النبضية غير المنتهية"، ويشرح مراحل التصميم بمساعدة حزمة برمجيات MATLAB7، وفي أبوابه الأخيرة يؤسس بالتفاصيل المعلومات المطلوبة لتطبيق المرشحات الرقمية بشكل عام على متحكمات الـ AVR أولا، ثم يتمحور حول تطبيق "مرشح استجابة نبضية منتهية" محدد على المتحكم Atmega16 من البداية. تمت كتابة البرنامج ثم بنيت الدائرة العملية وحللت نتائج التطبيق لتدعم النظرية.

# TABLE OF CONTENTS

---

Abstract .....	II
التجريدة.....	III
Table of Contents.....	IV
List of Figures.....	VII
Chapter One: INTRODUCTION	
INTRODUCTION .....	2
1.1. BACKGROUND .....	2
1.2. OBJECTIVES .....	3
1.3. CHAPTERS OUTLINES .....	3
CHAPTER TWO: Encryption & Cipher	
2, 1 Introduction .....	6
2, 2 Types of security .....	6
2, 3 ENCRYPTION .....	6
2, 3, 1 Three Types of Encryption .....	6
2, 3, 1, 1 Manual encryption .....	8
2, 3, 1, 2 Transparent encryption .....	8
2, 3, 1, 3 Semi-Transparent, or “On-the-fly”, encryption .....	9
2, 4 CIPHER .....	10
2, 4, 1 Code & cipher .....	11
2, 4, 1, 1 Codes .....	12
2, 4, 1, 2 Comparison of codes and ciphers .....	13
2, 4, 2 Cipher Key .....	15
2, 4, 3 Types of ciphers .....	16

2, 4, 3, 1 Symmetric Algorithm .....	18
2, 4, 3, 2 Block Ciphers .....	19
2, 4, 3, 3 Stream ciphering .....	20
2, 4, 3, 3, 1 Public Key Algorithms .....	21

## **CHAPTER THREE: DESIGN & IMPLEMENTATION**

3.1 Introduction .....	24
3, 1, 2 Front end voice ciphering .....	25
3, 4 Analog-to-Digital Conversion ON AVR .....	25
3, 5 IMPELEMENTION .....	28
3, 5, 1 Front end Algorithm .....	28
3, 5, 1, 1 Initialize the ports .....	29
3, 5, 1, 2 A\D conversion .....	30
3, 5, 1, 3 Ciphering algorithm .....	31
3, 5, 1, 4 Output the Result .....	32
3, 5, 1, 5 D\A conversion .....	33
3, 5, 2 the Hardware Circuitry .....	33
Chapter four: Conclusion .....	36
REFERENCES:.....	38
APPENDIX A: The Implementation Program .....	39
APPENDIX B: Atmega8535 Datasheet Summary .....	41
APPENDIX C: DAC08 Datasheets .....	62

## List of Figures:-

<b>Figure no</b>	<b>Figure name</b>	<b>Page</b>
<b>2, 1</b>	<b>outline of cipher system</b>	<b>11</b>
<b>2, 2</b>	<b>types of ciphering</b>	<b>17</b>
<b>3, 1</b>	<b>normal transmission speech steps</b>	<b>23</b>
<b>3, 2</b>	<b>front end voice ciphering speech transmission steps</b>	<b>24</b>
<b>3,3</b>	<b>ciphering algorithm Data flow</b>	<b>28</b>
<b>3, 4</b>	<b>Getting Samples from the ADC Data Flow</b>	<b>29</b>
<b>3, 5</b>	<b>ciphering data flow</b>	<b>31</b>
<b>3, 6</b>	<b>circuit block diagram</b>	<b>32</b>
<b>3, 7</b>	<b>Avr circuit</b>	<b>33</b>
<b>3,8</b>	<b>Microphone circuit</b>	<b>34</b>
<b>3,9</b>	<b>Speaker circuit</b>	<b>34</b>



