SYNGRESS

Information Hiding in Speech Signal for Secure Communication

Science Press
Beijing

Zhijun Wu

Information Hiding in Speech Signals for Secure Communication

语音信息隐藏
——面向网络的实时语音保密通信方法

Zhijun Wu

ELSEVIER

Science Press
Beijing

AMSTERDAM • BOSTON • HEIDELBERG • LONDON
NEW YORK • OXFORD • PARIS • SAN DIEGO
SAN FRANCISCO • SINGAPORE • SYDNEY • TOKYO

Syngress is an Imprint of Elsevier

SYNGRESS

Syngress is an imprint of Elsevier
The Boulevard, Langford Lane, Kidlington, Oxford OX5 1GB, UK
225 Wyman Street, Waltham, MA 02451, USA

First edition 2015

British Library Cataloguing in Publication Data

A catalogue record for this book is available from the British Library

Library of Congress Cataloging-in-Publication Data

A catalog record for this book is availabe from the Library of Congress

ISBN–13: 978-0-12-801328-1
ISBN 978-7-03-042125-8

For information on all Syngress publications visit our website at http://store.elsevier.com/

This edition is authorized for sale in the People's Republic of China only, excluding Hong Kong, Macao SAR and Taiwan. 本版本仅限在中华人民共和国境内（不包括香港特别行政区、澳门特别行政区和台湾）销售。

Information Hiding in Speech Signals for Secure Communication

语音信息隐藏

——面向网络的实时语音保密通信方法

Preface

In the information communication field, speech communication via network becomes an important way to transfer information. With the development of information technology, speech communication is widely used for military, diplomatic, and economic purposes as well as in cultural life and scientific research. Therefore, speech secure communication and the security of communication information have attracted more and more attention. The rapid growth of the Internet as both an individual and business communication channel has created a growing demand for security and privacy in the network communication channel. Security and privacy are essential for individual communication to continue and for e-commerce to thrive in cyberspace.

Any type of multimedia data—for example speech, transmitted via network—needs to be protected from manipulation, forgery, and theft. More sophisticated attacks require that more advanced security technologies be avoided, which have to be optimized for the particular requirements of each application scenario. As a development tendency of information security and a fresh-born technique, information hiding breaks the mentality of traditional cryptology. Information hiding technology carefully examines information security from a new perspective. Traditional secure communication approaches cannot satisfy current security requirements, and the garbled bits are likely to attract attention, or even encounter attacks from others. It is urgent to introduce a new mechanism for secure communication; thus the author undertakes it as his task to investigate a more secure communication, based on information hiding technology, which has many distinguishing characteristics. The most important characteristic is that there are univocal and continuous plain text speech signals on the communication line, so the secure communication will be more covert and safe.

OBJECTIVES

This book intends to develop the theory and system of real-time secure speech communication over a network based on information hiding technology, and to provide an overview of the research area of information hiding in secure communication. In the book, the author attempts to break the massive subject into comprehensible parts and to build, piece by piece, a development of information hiding technology in secure communication. The book emphasizes the fundamentals of algorithms and approaches concerning the technology and architecture of a secure communication field, providing a detailed discussion of leading-edge topics such as filter similarity and linear predictive coding (LPC) parameters substitution.

ORGANIZATION OF THE BOOK

This book introduces several methods to hide secret speech information in different types of digital speech coding standards. In the past 10 years, the continued advancement and exponential increase of network processing ability have enhanced

the efficiency and scope of speech communication over the network. Therefore, the author summarizes his years of research achievements in the speech information hiding realm to form this book, including a mathematical model for information hiding, the scheme of speech secure communication, an ABS-based information hiding algorithm, and an implemented speech secure communication system, which are organized into different sections in accordance with the security situation of the network. This book includes nine chapters, which introduce speech information hiding algorithms and techniques (embedding and extracting) capable of withstanding the evolved forms of attacks.

The four parts of this book are as follows:

I. Introduction, includes Chapter 1. This book begins with an introductory chapter, where the approaches of secure communication and their realization are discussed in general terms. This chapter ends with an overview of speech coding standards. This part provides a source of motivation for interested readers to wade through the rich history of the subject. The concept and algorithms involved in this part are explained in details in subsequent chapters.

II. Theory, consists of Chapters 2 and 3. This part proposes a mathematical model, and embedding and extracting algorithms of secure communication based on information hiding. The design of a speech information hiding model and algorithm for secure communication focuses on security, hiding capacity, and speech quality. The model and algorithm may help readers to develop a deep understanding of what information-hiding-based secure communication is all about.

III. Approaches, consists of Chapters 4 through 7. This part presents a detailed embedding secret speech coded in MELP 2.4 K, with the secret speech coded in accordance with five important families of the speech coding standard, such as G.721, G.728, G.729, and GSM, which are used in Voice over Internet Protocol (VoIP) or Public Switched Telephone Network (PSTN). Next is the introduction of the process of extracting secret speech coded in MELP 2.4 K in the G.721, G.728, G.729, and GSM standards. The procedure of the realization of secure communication based on specific speech coding standards is developed.

IV. Realization, consists of Chapters 8 and 9. This part gives two applications of secure communication based on the technology of information hiding. Each chapter sets up one example to show how to implement secure communication over VoIP and PSTN by using the information-hiding-based model and algorithm individually.

Each chapter begins with a high-level summary for those who wish to understand the concepts without wading through technical explanations. Then examples and more details are provided for those who want to write their own programs. The combination of practicality and theory allows engineers and system designers to implement true secure communication procedures, and to consider probable future developments in their designs, therefore fulfilling the requirements of social development and technological progress for new types of secure communication.

CHARACTERISTICS OF THE BOOK

The author introduces readers to earlier research regarding security of transmitted speech information over networks, and combines information technology and speech signal processing to form a speech hiding model for solving the problem of secure speech communication. Taking into consideration the requirements of real time and security, the author puts forward the algorithm of LPC coefficients substitution for secret speech information hiding based on filter similarity (LPC-IH-FS) and information extraction with blind-detection-based minimum mean square error (BD-IE-MES). Compared with traditional secure communication, those proposed theories and algorithms have distinct advantages in the field of secure communication. Moreover, the chapters and sections of this book are arranged from the simple to the complex, and the chapters relate to each other closely, with a reasonable knowledge structure. The book is scientifically and systematically organized. Plenty of tables and diagrams work jointly to interpret how the approach works and to demonstrate superior performance of the proposed approach. In addition, to validate the performance of the proposed approach, plenty of experiments are conducted, and detailed experiment results and analyses are available in the book.

A few topics may be of great interest for readers, such as the new idea of speech secure communication, the introduced mathematical model for information hiding, the proposed LPC-IH-FS and BD-IE-MES algorithms, and the corresponding experimental results. The highlight of the book is that the author applied information hiding technology in secure communication for the first time and then addressed a new embedding and extracting approach based on the analysis-by-synthesis (ABS) algorithm.

NEW IDEA OF SPEECH SECURE COMMUNICATION

This new idea of speech secure communication is based on information hiding technology, which differs from the traditional speech secure communication. Conventional secure communication systems transmit encrypted or transformed noisy signals over the public channel. The proposed speech secure communication system in this book delivers clear, comprehensive and meaningful stego speech, with secret speech embedded, over the public channel. The stego speech is explicit but secret speech is implicit.

NEWLY PROPOSED SPEECH INFORMATION HIDING TECHNOLOGY

The ABS algorithm introduces speech synthesizing into speech coding, and speech embedding and coding are synchronously completed. Combined with conventional embedding approaches, ABS is capable of adjusting hiding capacity on the basis of secret speech. It may achieve a maximum hiding capacity of 3.2 kbps, under the condition of G.728 16 kbps carrier speech with MELP 2.4 kbps secret speech. The proposed approach has the advantages of high hiding capacity, good imperceptibility, and high embedding rate.

In the book, the embedding and corresponding extracting methods are illustrated with elaborate diagrams and tables. Analyses and comparisons are also given. The proposed method puts emphasis on solving the secure problems occurring in real-time speech communication, and it achieves a relatively high hiding capacity, thus the requirements of real-time communication are met.

The major contributions of this book lie in extending a new hotspot in a secure communication scope and opening up a perspective application realm of information hiding technology. The particular insight of information security and the unique ABS approach infuses this newborn technology with vitality.

POTENTIAL READERS OF THE BOOK

This book can be a valuable reference book for anyone whose profession is information security. Readers may be scientists and researchers, lecturers and tutors, academic and corporate professionals, even postgraduate and undergraduate students.

Readers will learn related concepts and theory about speech secure communication. This book offers readers in-depth knowledge of the theory, modules, algorithms, and systems about information hiding or secure communication proposed by the author. The knowledge allows potential customers to protect their secure speech communication against even the most evolved wiretapping and information analysis attacks. Furthermore, by combining the theory with practice, readers can not only conduct related experiments in accordance with the contents of the book, but also implement a secure communication system by programming. In short, the achievements presented in this book can be used for network security in practice.

To better understand this book, readers should have prerequisite knowledge in communication principles, networking theory, basic theory of information hiding, and speech signal processing technology.

Acknowledgments

Many people have contributed to the publication of this book.

I sincerely express my thanks to Professors Yang Yixian and Niu Xinxin, my mentors in the research area of information hiding at Beijing University of Posts & Telecommunications, for writing a section of the book, and for putting forward many valuable suggestions to improve the book.

I really appreciate my research team member Mr. Yang Wei at Beijing University of Posts & Telecommunications, who completed the analysis-by-synthesis (ABS) research and implementation of speech coding, and made a great contribution to the core algorithm in this book.

I would like to express my thanks to Associate Professor Ms. Ma Lan at Civil Aviation University of China, who made a great contribution to the information hiding model and analysis of speech coding standards.

I am truly indebted to Professor Wang Jian, Professor Zhang Yanling, Professor Yin Hengguang and Dr. Ma Yuzhao at Civil Aviation University of China, for improving the language of the book.

The input from anonymous reviewers of the book is also appreciated.

I want to very much thank my team members, lecturer Ms. Lei Jin and Mr. Yue Meng, for their strong support in every aspect.

I am grateful to my graduate students, Mr. Wang Chen and Ms. Liu Wanhui, for the simulation experiments (using MATLAB) in VoIP that are included in this book, and for their work on some sections of the book.

I thank my graduate students Ms. Cao Haijuan and Ms. Zhao Ting, for preparing the figures included in Chapters 2, 3, 8, and 9.

I thank my lab colleagues, Mr. Yang Wei, Dr. Bai Jian, and Dr. Yang Yu, for their kind permission to reproduce their figures in the book.

I am grateful to Ms. Chen Jing, Technical Editor of the Science Press on Information Technology, for helpful comments on the organization of the book, and for her patience and meticulous work on improving the book.

I thank the editor Mr. Zhang Pu at Science Press for getting in touch with me early, and helping me to complete the proposal and evaluation of the book.

I am indebted to my graduate students, Ms. Cao Haijuan and Ms. Ma Shaopu, for their help in checking the typos in all chapters and the references.

I thank Professor Ms. Han Ping, the Dean of School of Electronics & Information Engineering, Civil Aviation University of China, for approving and providing financial aid for the publication of the book.

I thank my colleagues in the School of Electronics & Information Engineering, Civil Aviation University of China, for their selfless assistance and sincere concern.

I also want to extend my sincerest thanks to everyone who supported me during my time as an author.

I am deeply grateful to the China National Science Foundation and Tianjin Natural Science Foundation. This work is partly financially supported by the China

National Science Foundation (No. 61170328), Tianjin Natural Science Foundation (No. 12JCZDJC20900, U1333116), the Fundamental Research Funds for the Central Universities-Civil Aviation University of China (CAUC) under grant 31122013P007, 3122013D003, and 3122013D007, the Civil Aviation Science and Technology Innovation Fund in 2013, the research laboratory construction funds of Civil Aviation University of China (CAUC) in 2014-2016, and the postgraduate courses construction funds of Civil Aviation University of China (CAUC) in 2013 under grant 10501034.

Overview

This book focuses on secure speech communication via VoIP (Voice over Internet Protocol) and PSTN (Public Switched Telephone Network) by using the technology of information hiding, an emerging steganographic subject. Secure speech communication is the practice of hiding secret speech digital information in public speech, requiring hiding capacity, robustness, and imperceptibility by means of steganographic techniques. This book addresses the key problems currently faced by communication security, and the technology under study facilitates communication information confidentiality and ensures the integrity and security of communication information. This book proposes the approach of analysis-by-synthesis speech information hiding (ABS-SIH) to hide secret speech into public/carrier speech for the purpose of secure communication. A number of different types of speech coding schemes used in VoIP and PSTN, such as G.711, G.721, G.728, G.729, and GSM, are applied to realize secure communication by using the proposed algorithms of linear predictive coding (LPC) parameter substitution for secret speech information hiding based on filter similarity (LPC-IH-FS) and secret speech information extraction with blind detection based on minimum mean square error (BD-IE-MES). Each scheme is described in a number of different operational environments, such as VoIP and PSTN.

Also included in the book are details of the new emerging and synthetic technology-information hiding, which aims at hiding useful or important messages in other information to disguise the existence of the messages themselves. The research primarily focuses on the fundamentals of information theory, applying information hiding theory and technology in real-time speech communication. This text not only puts forward the mathematical model used for speech information hiding, but also designs and realizes five concrete schemes based on different speech coding standards. It is more important that the book proposes LPC-IH-FS speech embedding and BD-IE-MES extracting algorithms, and develops a real-time speech secure communication system based on speech information hiding technology with DSP (digital signal processor) arrays.

The contents of this book include:

- Proposing a constraint speech secure communication model based on the theory and technology of information hiding.
- Presenting a secret speech information embedding algorithm LPC-IH-FS by using LPC parameters substitution based on filter similarity.
- Putting forward a secret speech information extracting algorithm BD-IE-MES with blind detection based on MES.
- Proposing an approach of information embedding and extracting for concrete speech coding schemes, such as G.711, G.721, G.728, G.729, and GSM, by using LPC-IH-FS and BD-IE-MES algorithms.
- Presenting an approach of secure communication over VoIP based on matrix coding.
- Bringing forward a scheme of real-time secure communication via PSTN based on the technology of information hiding.

The proposed LPC-IH-FS and BD-IE-MES algorithms guarantee information is transmitted through VoIP and PSTN secretly. They use the characteristics of LPC in the ABS coding method, choose different speech coding schemes (for example, G.711, G.721, G.728, G.729, and GSM) as the public speech carrier and the Mixed-Excitation Linear Predictive (MELP) 2.4 K scheme as secret speech, thus realizing the security of speech information. When comparing the secure communication method based on information hiding technology with the traditional secure communication method, results show that the proposed method is more efficient than the traditional secure communication method in terms of security and speech quality.

The real-time secure speech communication using the technology of information hiding is an innovative approach. This approach combines information security technology and emerging communication technology, opening up a new research field for studying the method of secure communication. Meanwhile, this approach makes it possible to explore a new application for information hiding technology in the communication field.

Contents

CHAPTER

1 Introduction

Information communication is one of the most significant features of an information society. As an important part of information communication, secure communication protects state secrets, commercial secrets, and personal privacy, which is crucial for the nation, society, and individuals. Human beings are living in an information society, and communication security and confidentiality are used not only for military purposes, but also for public life, such as network voice communication, mobile communication, electronic payment, and mobile banking on the Internet [1].

There are many kinds of methods for secure communication over networks, although the available methods have different levels of shortcomings [2]. New approaches of secure speech communication are proposed to transmit security information via Voice over Internet Protocol (VoIP) and Public Switched Telephone Network (PSTN) based on the techniques of information hiding discussed in this chapter.

1.1 BACKGROUND

With the development of network communication technology, speech communication technology has seen a gradual transition to VoIP communication from the original PSTN network communication [3]. At present, the speech communication network has become a hotspot in international and domestic telecommunications development. More and more speech services through networks are realized.

As we know, network-based threats have become more sophisticated, and PSTN and VoIP calls are vulnerable to threats such as session hijacking and man-in-the-middle attacks [2]. Without proper protective measures, attackers could intercept a PSTN or VoIP call and modify the call parameters or addresses (numbers). Even without modifying PSTN numbers or VoIP packets, attackers may be able to eavesdrop on telephone conversations being carried over a PSTN or VoIP network. If VoIP packets are traveling unprotected over the Internet, the attackers have the opportunity to access the information that these packets carry [4–7].

With a standard PSTN or VoIP connection, intercepting conversations requires physical access to telephone lines or access to the private branch exchange (PBX) and switch or router. Speech or data networks, which typically use the public Internet

Information Hiding in Speech Signals for Secure Communication. DOI: 10.1016/B978-0-12-801328-1.00001-X