Audio Steganography for Information Hiding and Covert Communication – A Tutorial

K. Gopalan
Professor Emeritus
Department of Electrical and Computer Engineering
Purdue University Northwest
Hammond, IN

Abstract

Steganography is concerned with hiding information in a medium such as text, image, audio or video. From Egyptian hieroglyphs, Greek tattooed writing, and Chinese papyrus to text display or printout from a word processor, this data hiding technique has a long and varied history. Human auditory and visual imperfections, which lead to psychoacoustic masking effects in hearing and vision, respectively, are exploited in modern multimedia hiding methods for modifying a host, or cover, signal in accordance with a given piece of covert information. Since the modification is carried out in the masked regions of perceptibility, the information-embedded medium, or the 'stego' signal, appears to be the same as the original host signal in human perception. While encryption of a media signal (an audio, image or video) alters the signal to conceal its contents so that it becomes unintelligible, embedding uses the media signal as a carrier for hiding covert information without altering the perceptual quality of the carrier. Hence, the success of embedding information in a media signal depends, among others, on the detectability of any difference between the original host signal and the embedded, stego signal. Watermarking is a subset of steganography for unobtrusively concealing a small amount of information such as the authenticity of the cover media signal. Recovery of the hidden information without requiring the original host media signal – oblivious recovery – and robustness of the hidden information under adverse conditions during transmission are also essential in many applications of steganography. Additionally, the hidden information must withstand intentional or unintentional attacks in attempts to illegally access the information from the stego.

Applications of general steganographic techniques abound in modern Internet based communication and file sharing. Watermarking of an audio signal, for instance, is used to determine the legal use of a music file that carries a hidden copyright logo or other information. Embedding biometric data such as a person's fingerprint features in his/her picture identification card for use in access-controlled areas can thwart illegal entry. By concealing the existence of hidden information, the technique can be applied for covert communication using unclassified channels without undue demand for bandwidth.

Outline

Steganography and Information Hiding – Historical Overview
Audio versus Image Steganography – Criteria
Psychoacoustic Masking and Imperceptibility
Spectral and Cepstral Domain Audio Hiding
Tone Insertion Steganography
Bit Modification Audio Steganography
Extension to Image Steganography

978-1-5386-5398-2/18/$31.00 ©2018 IEEE

Discussion and Challenges

Learning Objectives

At the end of the tutorial, attendees will be able to

- understand the concepts of steganography and distinguish between steganography and cryptography
- appreciate the challenges of imperceptible hiding in audio vs. image/video signals
- understand and compare different techniques of audio steganography exploiting psychoacoustic masking phenomenon of hearing for covert communication
- identify measures for imperceptibility between host and stego audio signals
- recognize further challenges in audio steganography for covert communication

Why attendees will select this tutorial

As an international conference focused on basic and applied research as they relate to Electrical and Computer Engineering, Information Technology, and related applications, the topic is highly relevant to attendees – this tutorial provides a forum for researchers interested in learning and applying methods for covert communication. Knowledge and understanding of the current steganography practices can benefit attendees to extend and/or develop improved methods for secure communications of patient information, banking transactions, etc. Additionally, signal processing specialists will find the challenging field of audio steganography highly useful for bandwidth-restricted communications in civilian and military disciplines.

K. 'Gopal' Gopalan is a recently retired senior professor with the Department of Electrical and Computer Engineering at Purdue University Northwest, Hammond, Indiana. While at Purdue, he had conducted research at Argonne National Laboratory, Wright-Patterson Air Force Base, and the Air Force Research Laboratory (AFRL), Rome, NY. His research in speech processing has been funded by AFRL. He has received three U.S. patents, all on audio steganography.
Gopalan has given keynote addresses and tutorials on speech processing, most recently at MILCOM 2015 and SPIN 2017.
Gopalan is a Life Senior Member of the IEEE and is the author of two textbooks, *Introduction to Digital Microelectronic Circuits* (McGraw-Hill), and *Introduction to Signal and System Analysis* (Cengage).