A High-Capacity Covering Code for Voice-Over-IP Steganography

Hui Tian, National Huaqiao University, Xiamen, China
Jie Qin, National Huaqiao University, Xiamen, China
Yongfeng Huang, Tsinghua University, Beijing, China
Xu An Wang, Engineering University of CAPF, Xian, China
Jin Liu, National Huaqiao University, Xiamen, China
Yonghong Chen, National Huaqiao University, Xiamen, China
Tian Wang, National Huaqiao University, Xiamen, China
Yiqiao Cai, National Huaqiao University, Xiamen, China

ABSTRACT

Although steganographic transparency and embedding capacity are considered to be two conflicting objectives in the design of steganographic systems, it is possible and necessary to strike a good balance between them in Voice-over-IP steganography. In this paper, to improve steganographic transparency while maintaining relatively large embedding capacity, the authors present a \((2n-1, 2n)\) covering code, which can hide \(2n-1\) bits of secret messages into \(2n\) bits of cover messages with not more than \(n\)-bit changed. Specifically, each \((2n-1)\)-bit secret message is first transformed into two \(2n\)-bit candidate codewords. In embedding process, the cover message is replaced with the optimal codeword more similar with it. In this way, the embedding distortion can be largely reduced. The proposed method is evaluated by comparing with existing ones with a large number of ITU-T G.729a encoded speech samples. The experimental results show that the authors’ scheme can provide good performance on both steganographic transparency and embedding capacity, and achieve better balance between the two objectives than the existing ones.

Keywords: Covering Code, Information Hiding, Steganographic Transparency, Steganography

1. INTRODUCTION

With the rapid development of networks, how to achieve secure communication in an open environment is becoming increasingly important. So far, lots of research effort has been made in this field (Yang, 2004). Particularly in recent years, a new alternative technique for secure communications, called steganography, has attracted increasing attention, of which the target

DOI: 10.4018/IJITWE.2015070104
is to conceal secret data into public covers (e.g., images, audios, videos and texts) to achieve covert communications (Provos et al., 2003, Zielinska et al., 2014). In contrast with traditional techniques based on cryptographies, whose purpose are to hide the content of secret messages being exchanged between two communicating parties, the goal of steganography is to conceal not only the content but also its very existence. Thus, steganography can provide better protection for secret data in a sense.

Hitherto, a great number of researches on steganography have been carried out, and target steganographic covers have been also extended from initial images to almost all multimedia (Zielinska et al., 2014, El-Eman et al., 2015, Li et al., 2015, Ramalingam et al., 2015, Satir et al., 2014). Recently, a novel dynamic steganographic cover, Voice over Internet Protocol (VoIP, also named IP telephony), has attracted increasing interest (Huang et al., 2011a, Lubacz et al., 2010, Mazurczyk et al., 2013, Tian et al., 2011, 2012, 2015a, 2015b), which has three main advantages over traditional storage media (Tian et al., 2011, 2012a, 2015a, 2015b). First, the real-time nature of VoIP provides better security for secret messages by virtue of its instantaneity, because it gives eavesdroppers almost no time to discover possible abnormality owing to concealed messages. Second, VoIP can be considered a multi-dimensional carrier in that both the packet protocol headers and the payload data can be employed to conceal information. Third, the duration of a VoIP conversation is dynamic and variable, so it can offer adequate cover data according to the requirement of covert communication. In virtue of the above advanced characteristics, VoIP-based steganography can provide another sophisticated solution for secure communication.

Up to now, a large variety of VoIP-based steganographic methods have been presented. The interested reader can refer to an up-to-date survey given by Mazurczyk (Mazurczyk et al., 2013). They can be roughly divided into two categories: approaches based on protocol steganography and the ones based on payload modification. The first category employs specific protocols of VoIP as the carriers and embeds secret messages into unused or optional fields of protocol headers (Bai et al., 2008, Huang et al., 2011b, Tian et al., 2012b) or by modulating inter-packet times (packet rates) (Lubacz et al., 2014, Mazurczyk et al., 2010, 2012), while the other one utilizes payloads as the carriers and conceals secret messages into the redundant parts of digital speech signals. In contrast, most researchers focus on the latter category, and have presented a good number of successful techniques, such as Least-Significant-Bit (LSB) steganography (Kratzer et al., 2006, Liu et al., 2012, Tian et al., 2008, Wang et al., 2007), quantization-index-modulation steganography (Xiao et al., 2008, Tian et al., 2014), echo-based steganography (Chen et al., 2008, Rachoń et al., 2007), inactive-frame steganography (Huang et al., 2011a) and trans-coding steganography (Mazurczyk et al., 2014). Among them, LSB steganography has gained the most attention (Lubacz et al., 2010, Mazurczyk et al., 2013, Tian et al., 2011, 2012, 2015a, 2015b), due to its relatively high capacity and low complexity. However, how to improve its steganographic security is still an important problem, which much research effort has been devoted for. For example, Huang et al. (Huang et al., 2008) attempted to introduce LSB matching steganography to the VoIP-based covert communication; Xu et al. (Xu et al., 2011) presented an adaptive approach to reduce the embedding distortion by randomly choosing both cover packets and embedding intervals between LSBs; Miao et al. (Miao et al., 2011) proposed an adaptive steganography scheme to improve the security by choosing lower embedding bit rates in the flat blocks and higher embedding bit rates in the sharp blocks. Besides the above methods, another feasible approach is to introduce covering codes to improve the embedding performance. Matrix encoding (ME) based on Hamming codes is such a covering code that can be used in the steganography. It was first discovered by Crandall (Crandall, 1998), and popularized by Westfeld who incorporated a typical implementation in his F5 algorithm (Westfeld, 2001). Generally, using the ME, $r$ bits can be hidden into $2^r-1$ cover bits with no more than 1-bit changed. However, as we can see, the embedding rate

Copyright © 2015, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
Related Content

A Graphical Based Approach to the Conceptual Modeling, Validation and Generation of XML Schema Definitions

A Systematic Map of Evaluation Criteria Applicable for Evaluating E-Portfolio Systems
[www.igi-global.com/chapter/a-systematic-map-of-evaluation-criteria-applicable-for-evaluating-e-portfolio-systems/137341?camid=4v1a](www.igi-global.com/chapter/a-systematic-map-of-evaluation-criteria-applicable-for-evaluating-e-portfolio-systems/137341?camid=4v1a)
Business Transformation though Cloud Computing in Sustainable Business
www.igi-global.com/chapter/business-transformation-though-cloud-computing-in-sustainable-business/140900?camid=4v1a

Enterprise Architecture's Identity Crisis: New Approaches to Complexity for a Maturing Discipline
www.igi-global.com/chapter/enterprise-architectures-identity-crisis/137419?camid=4v1a