Abstract

Digital Steganograpic techniques hide secret messages in a cover media (mostly image, audio or video) in an imperceptible manner which cannot be detected by unintended recipient. In addition to imperceptibility, security, capacity and robustness are the other major challenges for an effective steganographic technique. This article proposes a novel steganographic method, considering maximum secrecy, high capacity and robustness against certain attacks. The method utilizes uncompressed digital audio signals as the carrier and hides different types of digital payloads (image/text/audio) in the time domain. In the process of embedding multiple payload bits (either 2 bits or 3 bits) are embedded in each of the sample values at pseudo-random positions. The pseudo-random positions are generated using a logical expression which is devised as a function of both the cover and the payload involved to make the algorithm inherently robust against potential collusion attacks. Various objective and subjective metrics have been used to measure the performance of the proposed technique. Also test results have been presented to analyse its robustness against white noise and collusion attack.
- Bret Dunbar, SANS Institute, Info. Sec. Reading Room, "A Detailed look at Steganographic Techniques and their use in an Open-Systems Environment".

Volume 7 - No. 9, October 2010.

Index Terms

Computer Science  Security

Keywords

Steganography  HAS  MSE  SNR  PSNR  MOS  SHA-1  White Noise Attack  Collusion Attack