RESEARCH ARTICLE

Steganographic Method for Data Hiding In Audio Signals with LSB & DCT

Linu Babu[1], Jais John S[2], Parameshachari B D[3], Muruganantham C[4], H S DivakaraMurthy[5]

1M.Tech Student, Department of ECE, Nehru College of Engineering and Research Centre, Pampady, Thiruvilawamala, Kerala, India

2Assistant Professor, Department of ECE, Nehru College of Engineering and Research Centre, Pampady, Thiruvilawamala, Kerala, India

3Associate Professor, Department of ECE, Nehru College of Engineering and Research Centre, Pampady, Thiruvilawamala, Kerala, India

(Research Scholar, Dept. of ECE, Jain University, Bangalore, Karnataka, India)

4Assistant Professor, Department of ECE, Nehru College of Engineering and Research Centre, Pampady, Thiruvilawamala, Kerala, India

5Dean and HOD, Department of ECE, Nehru College of Engineering and Research Centre, Pampady, Thiruvilawamala, Kerala, India

[1] linubabup@gmail.com
[3] parameshbkit@gmail.com

Abstract— Data hiding, a form of steganography, is one of the emerging techniques that embeds secret data into a digital media and thus ensures secured data transfer. In this paper, the steganographic method used, is based on audio steganography which is concerned with embedding secret data in an audio file. The basic idea of proposed method is that the host signal (the sound wave cover media) undergoes preprocessing, and then the results takes the shape of an image in which the data can be securely hidden in the image layers. The secret data is then hidden in a preprocessed sound wave using a traditional steganographic technique. The least significant-bit (LSB) based technique are very popular for steganography in spatial domain. The simplest LSB technique simply replaces the LSB in the cover image with the bits from secret information. Further advanced techniques use some criteria to identify the pixels in which LSB(s) can be replaced with the bits of secret information. In DCT based technique insertion of secret information in carrier depends on the DCT coefficients. Any DCT coefficient value above proper threshold is a potential place for insertion of secret information. The proposed methods offer high quality of steganography process in terms of Peak Signal–to-Noise Ratio (PSNR). Only minor changes in the contents of the audio file occur, which are indiscernible to human ears. In addition, several attacks on the sound wave were performed; the results showed that the hidden secret data can be retrieved with minimal distortion. An implementation of both these methods and their performance analysis has been done in this paper.

Key Terms: - steganography; data hiding; attacks; PSNR; LSB; DCT

Full Text: http://www.ijcsmc.com/docs/papers/August2013/V2I8201315.pdf