Steganography Using Audio File

Dr. Moceheb Lazam Shuwandy
CS -CCMS -TU

Subject: Multimedia and Network Security
Fourth Stage

Lecture 6

INTRODUCTION

- As the need of security increases only encryption is not sufficient. So stegnograpghy is the supplementary to encryption.
- It is not the replacement of encryption. But Steganography along with encryption gives more security to data.
- The word steganography is of Greek origin and means "concealed writing" from the Greek words stegnos meaning "covered or protected", and graphei meaning "writing".

INTRODUCTION …CON.

- Steganography is the technique to hide the information in some media so that third party can't recognize that information is hidden into the cover media.
- That media may be text, image ,audio or video.The information that to be hidden is called stego and the media in which the information is hidden is called host.
- The stego object can be text, image, audio or video.When the information is hidden into the audio then it is called Audio steganography.

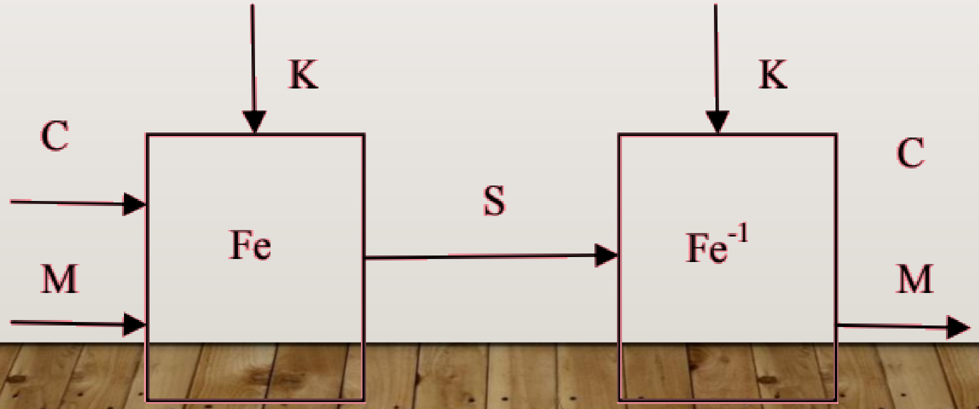
INTRODUCTION …CON.

- The process of Steganography is as shown in Figure1.The random selection of the samples used for embedding introduces low power additive white Gaussian noise (AWGN).
- The human auditory system (HAS) is highly sensitive to the AWGN.

INTRODUCTION …CON.

Hiding information in a media requires the following elements

- The cover media(**C**) that will hold the hidden data
- The secret message (**M**), may be plain text, cipher text, or any type of data
- The stego function (**Fe**) and it is inverse (**Fe-1**)
- An optional stego-key (**K**) or password may be used to hide and unhide the message.



DEFINITIONS

An effective steganographic scheme should possess the following desired characteristics:

Secrecy: A person should not be able to extract covert data from the host medium without the knowledge of the proper secret key used in the extracting procedure.

Imperceptibility: The medium after being embedded with the covert data should be indiscernible from the original medium. One should not become suspicious of the existence of covert data within the medium.

High capacity: The maximum length of the covert message that can be embedded should be as long as possible.

Resistance: The covert data should be able to survive when the host medium has been manipulated, for example by some lossy compression scheme.

Accurate extraction: The extraction of covert data from the medium should be accurate and reliable. Basically, the purpose of steganography is to provide secret communication like cryptography.

AUDIO STEGANOGRAPHY

- Like the document images, the sound files may be modified in such a way that they contain hidden information.
- like copyright information; those modifications must be done in such a way that it should be impossible for hackers to remove it, at least not without destroying the original signal.
- The methods that embed data in sound files use the properties of the Human Auditory System (HAS).
- The HAS perceives the additive random noise and also the perturbations in a sound file can also be detected.
- But there are some “holes” we can exploit. While the HAS has a large dynamic range, it has a fairly small differential range.

TECHNIQUE FOR DATA HIDING IN AUDIO

There are four techniques for hiding data in Audio as follows:

1. Least Significant Bit (LSB) Encoding
2. Phase Coding
3. Echo Hiding
4. Spread Spectrum

1. LEAST SIGNIFICANT BIT (LSB) ENCODING

- Least significant bit (LSB) coding is the simplest way to embed information in a digital audio file.
- By substituting the least significant bit of each sampling point with a binary message, LSB coding allows for a large amount of data to be encoded.
- In LSB coding, the ideal data transmission rate is 1 kbps per 1 kHz.
- In some implementations of LSB coding, the two least significant bits of a sample are replaced with two message bits.
- This increases the amount of data that can be encoded but also increases the amount of resulting noise in the audio file as well.

1. LEAST SIGNIFICANT BIT (LSB) ENCODING CON.

- A novel method which increases the limit up to four bits by Nedeljko C., Tapio S. & mediaTeam at Information Processing Laboratory.
- To extract a secret message from an LSB-encoded sound file, the receiver needs access to the sequence of sample indices used in the embedding process.
- **The length of the secret message to be encoded is smaller than the total number of samples in a sound file.**
- One must decide then how to choose the subset of samples that will contain the secret message and communicate that decision to the receiver.

1. LEAST SIGNIFICANT BIT (LSB) ENCODING CON.

- One trivial technique is to start at the beginning of the sound file and perform LSB coding until the message has been completely embedded, leaving the remaining samples unchanged.
- This creates a security problem, however in that the first part of the sound file will have different statistical properties than the second part of the sound file that was not modified. **(How to solve this issue?)**
- **One solution to this problem is to pad the secret message with random bits so that the length of the message is equal to the total number of samples.**

1. LEAST SIGNIFICANT BIT (LSB) ENCODING DISADVANTAGES

- **There are two main disadvantages associated with the use of methods like LSB coding.**
  - The human ear is very sensitive and can often detect even the slightest bit of noise introduced into a sound file,
  - Second disadvantage, this is not robust. If a sound file embedded with a secret message using either LSB coding was resample, the embedded information would be lost.
- **How Solve this issues?**
  - Robustness can be improved somewhat by using a **redundancy technique** (reduce data transmission rate significantly) while encoding the secret message.

2. PHASE CODING

- Phase coding addresses the disadvantages of the noise inducing methods of audio steganography.
- Phase coding relies on the fact that the phase components of sound are not as perceptible to the human ear as noise is.
- Rather than introducing perturbations, the technique encodes the message bits as phase shifts in the phase spectrum of a digital signal, achieving an inaudible encoding in terms of signal-to perceived noise ratio.

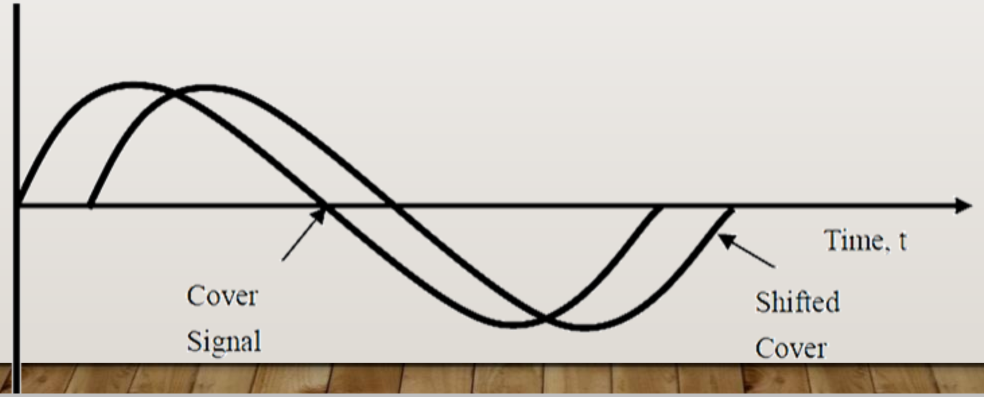


Figure: illustrate the original cover signal and encoded shifted signal of phase coding technique.

2. PHASE CODING … CON.

Phase coding is explained in the following procedure:

- The original sound signal is broken up into smaller segments whose lengths equal the size of the message to be encoded.
- A Discrete Fourier Transform (DFT) is applied to each segment to create a matrix of the phases and Fourier transform magnitudes.
- Phase differences between adjacent segments are calculated.
- Phase shifts between consecutive segments are easily detected.
  - The absolute phases of the segments can be changed but the relative phase differences between adjacent segments must be preserved.

  → The secret message is only inserted in the phase vector of the first signal segment as follows:

2. PHASE CODING … CON.

$$\text{Phase\_new} = \begin{cases} \pi / 2 \text{ if message bit } = 1 \\ \pi / 2 \text{ if message bit } \\ = 0 \end{cases}$$

- A new phase matrix is created using the new phase of the first segment and the original phase differences.
- Using the new phase matrix and original magnitude matrix, the sound signal is reconstructed by applying the inverse DFT and then concatenating the sound segments back together.

2. PHASE CODING … CON.

To extract the secret message from the sound file:

1- The receiver must know the segment length.

2- The receiver can then use the DFT to get the phases and extract the information.

- One disadvantage associated with phase coding is **a low data transmission rate** *due to the fact that the secret message is encoded in the first signal segment only. (***The solution:** *increasing the length of the signal segment).*
- This would change phase relations between each frequency component of the segment more drastically, making the encoding easier to detect.
- **As a result,** the phase coding method is used when only a small amount of data, such as a watermark, needs to be concealed.

3. ECHO HIDING

- In echo hiding, information is embedded in a sound file by introducing an echo into the discrete signal.
- It too provides advantages in that it allows for a high data transmission rate and provides superior robustness when compared to the noise inducing methods. ***(Like the spread spectrum method)***
- To hide the data successfully, three parameters of the echo are varied: ***amplitude, decay rate, and offset (delay time)*** from the original signal.
- All three parameters are **set below the human hearing threshold** ***so the echo is not easily resolved.***

3. ECHO HIDING

- To extract the secret message from the stego-signal, the receiver must be able to break up the signal into the same block sequence used during the encoding process.
- Then the autocorrelation function of the signal's cepstrum (the cepstrum is the Forward Fourier Transform of the signal's frequency spectrum) can be used to decode the message

  (because it reveals a spike at each echo time offset, allowing the message to be reconstructed)
- For a discrete signal $f(t)$, an echo $f(t-dt)$, with some delay can be introduced to produce the stego signal $s(t) = f(t) + f(t-dt)$.
- In echo hiding, information is embedded in a sound file by introducing an echo into the discrete signal.