UNIVERSITY OF SCIENCE AND TECHNOLOGY OF HANOI

Audio Steganography

Student Name	Student ID	Contribution
Duong Dang Hung	BI10-073	25%
Ta Quang Hieu	BI10-065	25%
Nguyen Hoang Minh	BI10-112	25%
Nguyen Quy Minh	BI10-118	25%

AUDIO STEGANOGRAPHY

A primer on Audio Steganography

Introduction

Techniques used in Audio Steganography

Applications of Audio Steganography

Demo

A little bit about history...

- Before the Internet, the various computer networks did not have a standard way to communicate with each other
- On January 1, 1983, with TCP/IP, the Internet was "officially" born, and allow different kinds of computers on different networks to "talk" to each other

→ Security of information became one of the most important factor

Cryptography

- A technique for securing the secrecy of communication
- It is the method to encrypt and decrypt data in order to keep the information secret
- Hide the information in a format that:
  - A normal person cannot understand
  - Attackers cannot decipher

→ What if we also need to hide the existence of the information?

Solution: Steganography!

Steganography

- "Stegos": covered
- "Graphein": to write

→ Steganography: covered writing

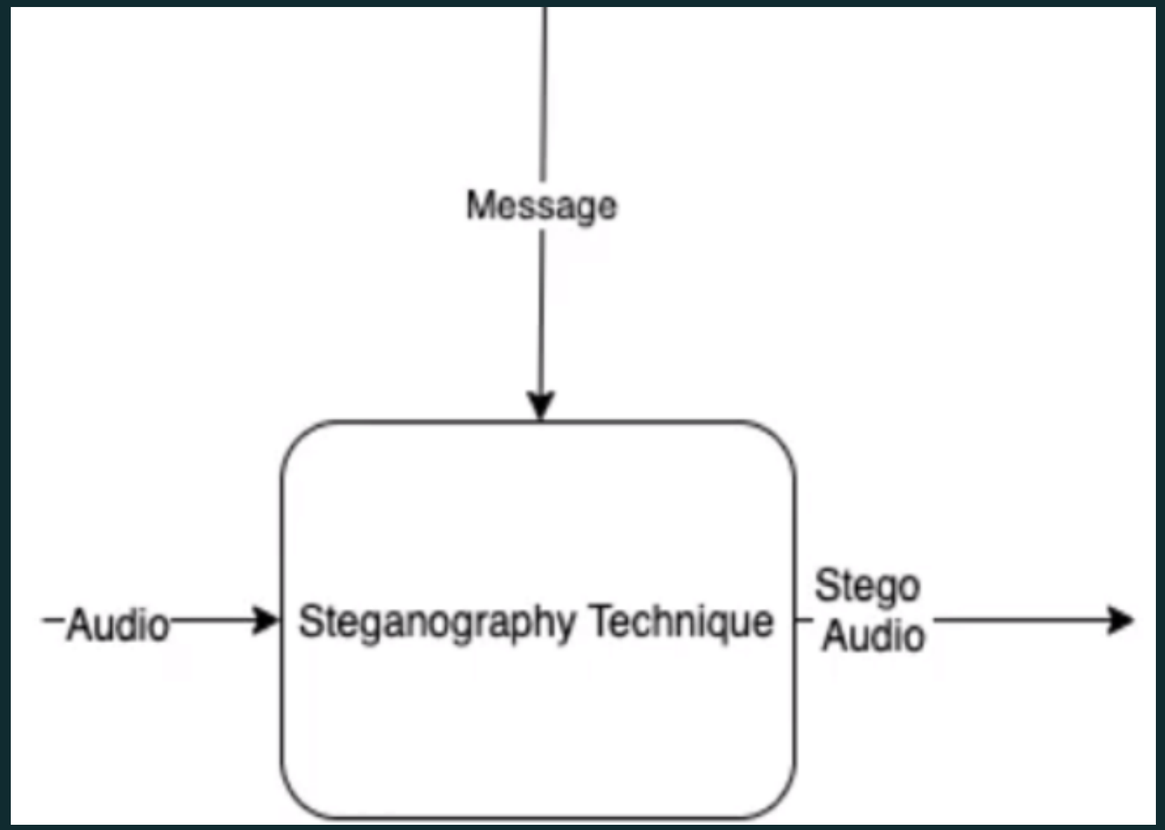
- Steganography tries to hide data in plain view and deter attackers, rather than encrypting them.
- 4 types of digital steganography: text, image, audio, video

Audio Steganography

- Steganography using audio
- The art of covertly transmitting hidden information by embedding messages into an *audio* signal
- The host audio before steganography vs. the stego audio after steganography: same characteristics!
- One of the most effective way to protect the information privacy

Audio Steganography

- Audio Steganography basic workflow:



Audio Steganography

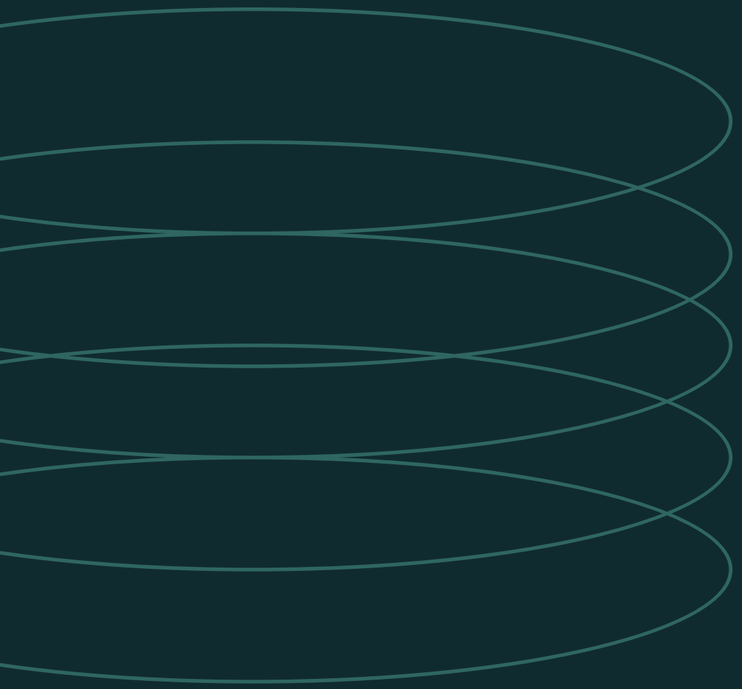
Hiding capacity

Inaudibility of distortion

Robustness

Why Audio Steganography?

- Audio provides more features which can be used to hide information
- All 3 characteristics: Amplitude, Frequency and Phase can be manipulated
- An audio signal is perceived differently as a human. We can use this "weakness" to hide more information



Applications of Audio Steganography

Some notable applications are...

- Hide a secret chemical formula or plans for a new invention
- Sending out trade secrets
- DVDs watermark
- etc.

Techniques used in Audio Steganography

Numerous techniques were developed:

- *Least Significant Bit (LSB)*
- *Phase Coding*
- Echo Hiding
- Parity Coding
- Hide in silence Intervals
- Spread Spectrum
- Discrete Wavelet Transform
- Tone insertion

Least Significant Bit (LSB)

- Step 1: Convert the audio signal into a binary format
- Step 2: Divide the audio signal into smaller chunks
- Step 3: Convert the secret message into binary
- Step 4: Replace each last bit of the chunks by bits from the message

Least Significant Bit (LSB)

Audio stream sample (16-bits)	"Hi" in binary	Stego audio Stream (w embedded message)
1 1 0 1 1 1 0 1 1 1 0 0 1 0 0 **1**	0	1 1 0 1 1 1 0 1 1 1 0 0 1 0 0 **0**
0 0 0 1 1 0 0 0 0 1 1 0 0 1 1 **0**	1	0 0 0 1 1 0 0 0 0 1 1 0 0 1 1 **1**
1 1 1 0 0 1 0 1 1 1 0 1 1 0 1 **0**	0	1 1 1 0 0 1 0 1 1 1 0 1 1 0 1 **0**
0 0 0 1 1 0 0 0 0 1 1 0 0 0 0 **0**	0	0 0 0 1 1 0 0 0 0 1 1 0 0 0 0 **0**
1 1 1 0 0 0 0 1 1 1 0 1 0 1 1 **0**	1	1 1 1 0 0 0 0 1 1 1 0 1 0 1 1 **1**
0 0 0 0 1 0 1 1 0 0 1 0 0 0 0 **0**	0	0 0 0 0 1 0 1 1 0 0 1 0 0 0 0 **0**
1 1 1 1 1 0 0 0 1 1 0 0 0 1 1 **1**	0	1 1 1 1 1 0 0 0 1 1 0 0 0 1 1 **0**
0 1 0 0 1 1 1 1 0 1 0 1 1 0 1 **0**	0	0 1 0 0 1 1 1 1 0 1 0 1 1 0 1 **0**
0 1 0 0 0 0 0 0 0 1 1 0 0 0 1 **1**	0	0 1 0 0 0 0 0 0 0 1 1 0 0 0 1 **0**
0 0 1 1 1 0 1 1 0 1 0 0 1 1 1 **0**	1	0 0 1 1 1 0 1 1 0 1 0 0 1 1 1 **1**
0 1 1 0 0 0 0 0 0 0 1 1 0 0 1 **0**	1	0 1 1 0 0 0 0 0 0 0 1 1 0 0 1 **1**
1 0 0 0 1 1 0 1 0 1 0 1 1 1 0 **0**	0	1 0 0 0 1 1 0 1 0 1 0 1 1 1 0 **0**
0 1 1 0 0 0 1 0 1 0 1 0 0 0 1 **0**	1	0 1 1 0 0 0 1 0 1 0 1 0 0 0 1 **1**
1 1 0 0 1 0 0 0 0 1 0 0 0 0 0 **0**	0	1 1 0 0 1 0 0 0 0 1 0 0 0 0 0 **0**
0 0 0 0 0 0 1 0 1 1 1 1 1 0 1 **1**	0	0 0 0 0 0 0 1 0 1 1 1 1 1 0 1 **0**
1 1 0 1 1 1 0 0 1 1 0 0 0 1 0 **1**	1	1 1 0 1 1 1 0 0 1 1 0 0 0 1 0 **1**

Least Significant Bit (LSB)

- Most popular + most frequently used
- Advantages:
  - Easy to understand
  - Simple to implement
  - Does the job most of the time
- Disadvantages:
  - Very low transfer capacity
  - Changes can sometimes be perceived if there is a lot of information in the audio

Phase Coding

- Step 1: Divide the audio into smaller segments:
  - Extract the header information from the audio
  - Divide the rest into chunks whose sizes are equal to the size of the secret message
- Step 2: Apply DFT (Discrete Fourier Transform) to each segment to create a matrix of the phases.

Phase Coding

- Step 3: Convert the secret message to binary and insert it into the phase vector of *only the first signal segment* as follow:
  - If secret message bit = 0:

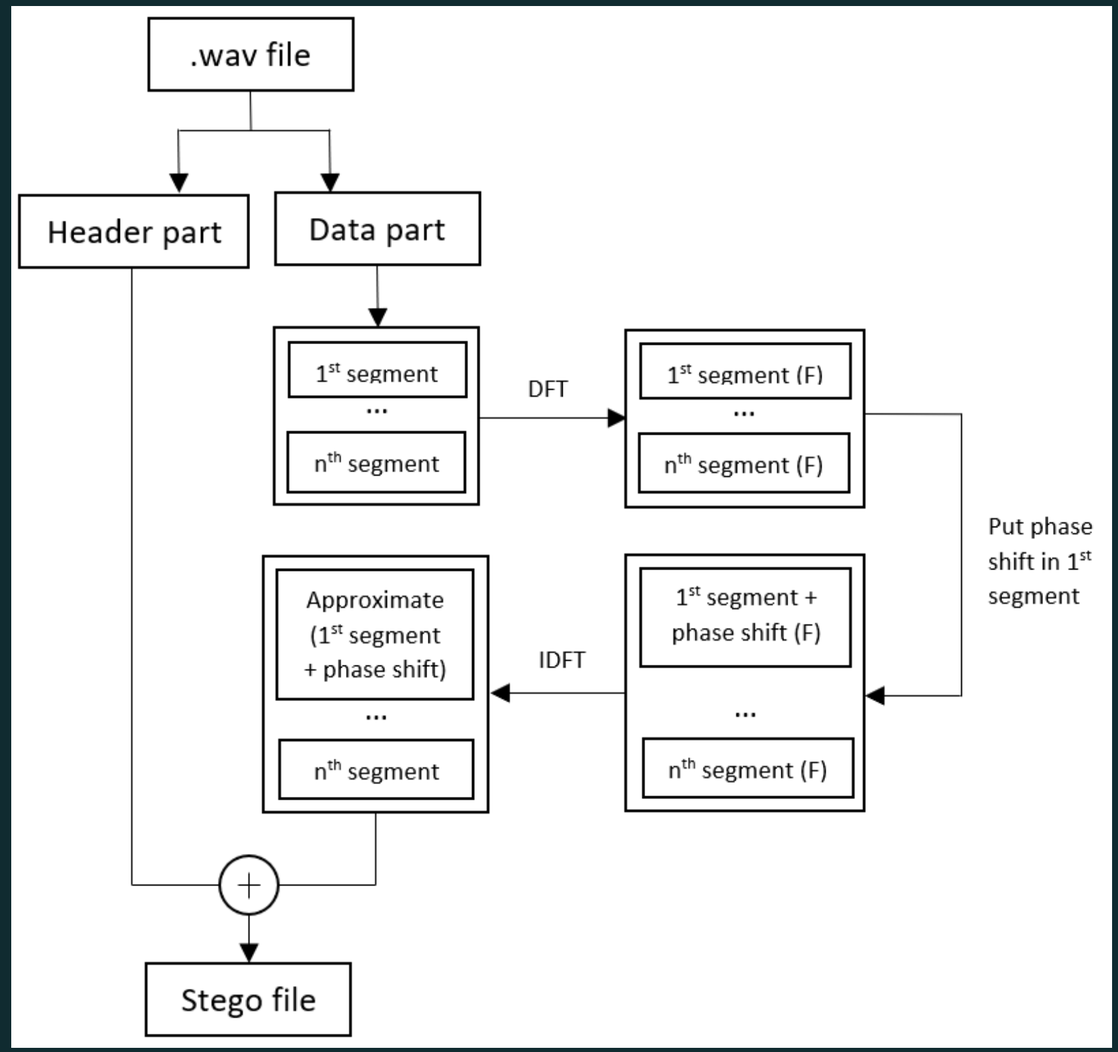
    new phase = old phase + π/2
  - If secret message bit = 1:

    new phase = old phase - π/2

Phase Coding

- Step 4: Create a new phase matrix using the new phase of the first segment and the original phase matrix
- Step 5: Apply the Inverse DFT using the new phase matrix
- Step 6: Combine the sound segments with the original header to create the new sound signal.

Phase Coding



Phase Coding

- Exploit human auditory system’s insensitivity to relative phase of different spectral component
- Advantages:
  - Is the most resistant to signal distortion
  - Provides far better transfer capacity compared to LSB
  - The difference in the audio is not perceivable to human
- Disadvantages:
  - The secret message is not distributed over the audio (localized at the first block) → can easily be removed using cropping attack

Demo

Conclusion

1

WHAT IS AUDIO STEGANOGRAPHY?

Technique to embed secret messages into an audio file without loss of audio quality.

2

WHY AUDIO STEGANOGRAPHY?

There are some real-life situations where we need to hide the information along with its existence.

3

HOW TO IMPLEMENT AUDIO STEGANOGRAPHY?

There are many methods. Our system focuses mainly on Least Significant Bit and Phase Coding.

Thank you for listening!