IE406.E31
Introduction to Steganography and its Applications

Index Huynh

Lecturer: M.S. Nghi Hoàng Khoa

HCMC, Ngày 11 tháng 8 năm 2025

Mục lục

Preface

Chương 1

Introduction

1.1 Introduction and history

Steganography is the art of hidden writing, a term derived from Greek. It's the art and science of communicating in a way that conceals the very existence of the communication itself. The goal is to ensure that an outsider, or third party, doesn't realize that a secret message is being transmitted.

1.2 Fundamental concepts

Data hiding is an overarching concept that refers to methods of concealing information within another medium. Its purpose is to protect information from unauthorized access and to maintain its confidentiality and integrity.

Steganography and **watermarking** are two specialized sub-branches of data hiding, which differ primarily in their objectives.

1.3 Differentiating techniques

Steganography aims to conceal the very existence of a message, prioritizing un-detectability. The system is considered to have failed if the message is discovered.

In contrast, **digital watermarking** seeks to embed an identifying mark into data, prioritizing robustness. For the system to be successful, the watermark must survive attacks intended to remove or destroy it.

Cryptography aims to protect the content of a message. It transforms readable text into an unreadable form (ciphertext), making it obvious that a message exists, but its meaning remains a secret.

1.4 Introduction to techniques and applications

The following is a distinction of steganography methods based on the host medium:

- **Text Steganography:** Considered the most difficult due to the limited amount of redundant data available for embedding.

- **Image Steganography:** The most popular and widely researched method, as images provide a suitable medium for concealment.

- **Audio Steganography:** Involves embedding data into bits or frequencies that are imperceptible to the human ear.
- **Video Steganography:** Leverages the large data capacity of video by combining both image and audio steganography techniques.
- **Network Steganography:** Involves hiding information within network packets, often in fields like TCP/IP headers.

1.5 Basic Technique: LSB Substitution

LSB substitution (Least Significant Bit substitution) is a fundamental and widely-used steganography technique. It works by replacing the least significant bit (the last bit) of the bytes in a cover medium (like an image or audio file) with the bits of the secret message.

This method is effective because the least significant bit has the smallest impact on the overall value of a byte. For example, in an image, changing the LSB of a pixel's color value results in a negligible color shift that is typically imperceptible to the humman eye.

1.5.1 How it works

Imagine a single pixel's red color value is represented by the byte 11010010. The LSB is the last 0. To embed a secret message bit, say a 1, you would simply replace the LSB, changing the byte to 11010011. This minor alteration is difficult for an observer to notice without specialized tools, effectively hiding the seret message.

1.5.2 Advantages and Disadvantages

It is simple to understand and easy to iplement. But it is not very robust. The hidden data can be easily destroyed by common operations like image compression or simple steganalysis attacks.

Chương 2

Data hiding on image

To a computer, an image is a matrix of pixels. The three main types of images are:

- **Bitmap (Binary) Images:** each pixel is represented by a single bit (0 for white, 1 for black).
- **Grayscale Images:** Each pixel uses an 8-bit value to represent a range of black to white intensities.
- **RGB Images:** Each pixel is composed of three 8-bit color channels (Red, Green, Blue).

The most crucial component for steganography is the **data redundancy** within an image. Steganography leverages two key factors:

- **Redundant data:** insignificant bits whose alteration does not noticeably affect the image.
- **The imperceptibility of the human eye:** The human visual system cannot perceive very small changes in color.

Images with high detail are better suited for steganography because they contain more redundant data. Regarding file formats, **BMP** (uncompressed) files are large and can appear suspicious, whereas **JPEG** (compressed) is the most common format and is well-suited for modern steganography techniques.

2.1 Spatial domain techniques and vulnerabilities

2.2 Frequency domain techniques and hide data in a jpeg image

2.3 Advanced methods