Algorithms of Information Security: Steganography I

Faculty of Information Technology
Czech Technical University in Prague

December 6, 2023

Steganography

- The word *steganography* is a composite of the Greek word *steganos,* which means "covered", and *graphia,* which means "writing".
- In the other words, steganography is the art of concealed communication where the very existence of a message is secret.
- Steganography is the practice of communicating a secret message by hidding it in a cover object.

Steganography throughout history

- The first written evidence about steganography being used to send messages is due to Herodotus, who tells of a slave sent by his master, Histiaeus, to the Ionian city of Miletus with a secret message tattooed on his scalp.
- After the tattooing of the message, the slave grew his hair back in order to conceal the message. He then travelled to Miletus and, upon arriving, shaved his head to reveal the message to the city's regent, Aristagoras. The message encouraged Aristagoras to start a revolt against the Persian king.
- Perhaps the best-known form of steganography is writing with invisible ink. The first invisible inks were organics liquids, such as milk, urine, vinegar, diluted honey, or sugar solution.
- To make them perceptible, the letter was simply heated up above a candle. Later, more sophisticated versions were invented by replacing the message-extraction algorithm with safer alternatives, such as using ultraviolet light.

Steganography throughout history

- In 1966, an inventive and impromptu steganographic method enabled a prisoner of war, Commander Jeremiah Denton, to secretly communicate one word when he was forced by his Vietnamese captors to give an interview on TV.
- Knowing that he could not say anything critical of his captors, as he spoke, he blinked his eyes in Morse code, spelling out T-O-R-T-U-R-E.

Steganography introduction

- Every steganographic system discussed in our lectures consists of two basic components - the embedding and extraction algorithms.
- The embedding algorithm accepts three inputs - the secret message to be communicated, the secret shared key that controls the embedding and extraction algorithm, and the *cover object*, which will be modified to convey the message.
- The output of the embedding algorithm is called the *stego object*.
- When the stego object is presented as an input to the message-extraction algorithm, it produces the secret message.

Steganography as the prisoners' problem

- Steganography is usually described as the prisoners' problem in which two prisoners, Alice and Bob are imprisoned in separate cells and want to hatch as escape plan. They are allowed to communicate but their communication is monitored by the warden (Eva), who will cut the communication once she suspects covert exchange of data.
- Note that in the prisoners' problem, all that Eva needs to achieve is to detect the presence of secret messages rather than know their content. In other words, when Eva discovers that Alice and Bob communicate secretly, the steganographic system is considered broken.
- This is in contrast to encryption, where a successful attack means that the attacker gains acces to the decrypted content or partially recovers the encryption key.

Steganography types

- The main goal of steganography is to communicate securely in a completely undetectable manner and to avoid drawing suspicion to the transmission of a hidden data.
- It is not to keep others from knowing the hidden information, but it is to keep others from thinking that the information even exists.
- The data can be hidden in basic formats like: Audio, Video, Text and Images etc.

Steganography types

- **Image Steganography**
  The image steganography is the process in which we hide the data within an image so that there will not be any perceived visible change in the original image. There are different file formats that are available for digital images and for these file formats different algorithms exist such as least significant bit (LSB) insertion, Masking and filtering, Redundant Pattern Encoding, Encrypt and Scatter.
- **Audio Steganography**
  Secret message is embedded into digitized audio signal which result slender shifting of binary sequence of the equivalent audio file. There are a number of methods like LSB coding, Phase coding, spread spectrum, Echo hiding which are used for audio steganography.

Steganography types

- **Video Steganography**
  Video files consist of assortment of images and sounds, so most of the presented techniques on images and audio can be applied to video files too. An advantage of using video steganography is that large amount of data that can be hidden inside the cover file and it is the fact that it is flow of images and sounds.
- **Text Steganography**
  Steganography can be applied to text files as well. In text steganography formatting or by changing certain characteristics of textual elements can be changed. It consists of line-shift coding, word-shift coding and feature coding.
- **Protocol Steganography**
  Protocol steganography embeds the information using network control protocol like HTTP, FTP, TCP, SSH, UDP etc. Secret information is embedded in voice-over IP. Protocol steganography is an advance dimension of steganography and more secure than other dimensions.

Steganography and watermarking

- Even though watermarking and steganography share some fundamental similarities in that they both secretly hide information, they address very different applications.
- While in steganography the secret message has usually no relationship to the cover object, which plays the role of a mere decoy, watermarks usually carries supplemental information about the cover image or some other data related to the cover, such as labels identifying the sender or the receiver.
- Moreover, and most importantly, watermarks do not have to be embedded undetectably.

Digital images formats. Color representation

- Digital images are commonly represented in four basic formats - raster, palette, transform, and vector.
- According to the trichromatic theory of human perception, each color that humans can perceive is a linear combination of three basic colors (or color channels) - red, green, and blue - the **RGB** color model.
- The name of the model comes from the initials of the three additive primary colors, red, green, and blue.
- A color in the RGB color model is described by indicating how much of each of the red, green, and blue is included. The color is expressed as an RGB triplet (R, G, B). Each component of a triplet can vary from zero to a defined maximum value. If all the components are at zero the result is black; if all are at maximum, the result is the brightest representable white.

Digital images formats. Color representation

- Denoting the amount of each color as R, G, and B, where each number is from the interval $[0, 1]$, each color can be represented as a three-dimensional vector in the RGB color cube $(R, G, B) \in [0, 1]^3$.
- Since colors are usually defined by three components, then a three-dimensional volume is described by treating the component values as ordinary Cartesian coordinates in a Euclidean space. For the RGB model, this is represented by a cube using non-negative values within a $0 - 1$ range, assigning black to the origin at the vertex $(0, 0, 0)$, and with increasing intensity values running along the three axes up to white at the vertex $(1, 1, 1)$, diagonally opposite black.
- *Examples.* Old computer monitors with the Cathode-Ray Tube (CRT) screens create colors by combining three RGB phosphores on the screen. Liquid-Crystal Display (LCD) panels combine the light from three adjacent pixels.

Digital images formats. Color representation

- An RGB triplet (R, G, B) represents the three-dimensional coordinate of the point of the given color within the cube or its faces or along its edges. This approach allows computations of the color similarity of two given RGB colors by simply calculating the distance between them: the shorter the distance, the higher the similarity.
- The set of all colors can be arranged lexicographically as a set of triplets.
- The similarity of colors can be measured using the Euclidean norm

$$\|(R_1, G_1, B_1) - (R_2, G_2, B_2)\| = \sqrt{(R_1 - R_2)^2 + (G_1 - G_2)^2 + (B_1 - B_2)^2}.$$

Digital images formats. Color representation

- The CMY color model is related to the RGB color model.
- The subtractive color models is used for hardware devices that create colors by absorption of certain wavelenghts rather than emission of light. A good example of a substractive color device is a printer.
- Its base colors are
  - cyan (C)
  - magenta (M)
  - yellow (Y).
- These three colors are obtained by removing from white the colors red, green and blue, respectively.
- The CMY system is augmented with a fourth color, black (abbreviated as K) to improve the printing contrast and save on color toners.

Digital images formats. Color representation

Simple relation between RGB and CMY (Conversion between RGB and CMY.)

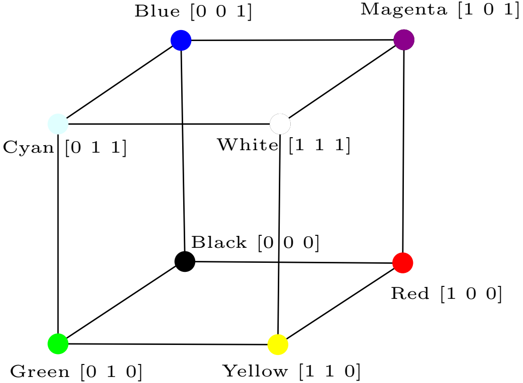
- RGB $\Longrightarrow$ CMY

$$\begin{pmatrix} C \\ M \\ Y \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} - \begin{pmatrix} R \\ G \\ B \end{pmatrix} \tag{1}$$

- CMY $\Longrightarrow$ RGB

$$\begin{pmatrix} R \\ G \\ B \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} - \begin{pmatrix} C \\ M \\ Y \end{pmatrix} \tag{2}$$

Digital images formats. Color representation



Digital images formats

- There are four main types of image formats: raster, palette (indexed), transform, and vector formats.
- Raster formats represent a digital image as a rectangular array of integers sampled using a fixed number of bits.
- The most common formats that allow raster image representation are BMP, TIFF, and PNG.
- Images in raster formats are often large despite the fact that the formats use lossless compression to decrease the amount of data that needs to be stored.
- TIFF (Tagged Image File Format) files have many formats: Black and white, greyscale, 4- and 8-bit color, full color (24-bit) images. TIFF files support the use of data compression using LZW (Lempel–Ziv–Welch) algorithm and other compression standards.

Digital images formats. BMP

- Bitmap (BMP) is monochrome and the color table contains two entries. Each bit in the bitmap array represents a pixel. If the bit is clear, the pixel is displayed with the color of the first entry in the color table. If the bit is set, the pixel has the color of the second entry in the table.
- Today's color display devices represent color using the RGB color model.
- The 4-bit per pixel (4bpp) format supports 16 distinct colors and stores. Each pixel value is a 4-bit index into a table of up to 16 colors.
- The 8-bit per pixel (8bpp) format supports 256 distinct colors and stores 1 pixel per 1 byte. Each byte is an index into a table of up to 256 colors.
- The 24-bit pixel (24bpp) format supports 16 777 216 distinct colors and each pixel is a 3-byte sequence in the bitmap array represents the relative intensities of red, green, and blue.

Digital images formats

- Palette images consist of two parts - a color palette and an array of indices to the palette. Typical palette formats are GIF and PNG. Palette images are convenient for representing charts, computer art, and other images with low color depth.
- Images in transform formats are represented through transform coefficients that are quantized by a fixed number of bits rather than using pixels directly. The most popular transform format is JPEG, which uses the discrete cosine transform (DCT).
- Vector formats, such as WMF, EPS, and PS, can represent objects in the image using parametric description.

Steganography by cover modification

- Alice starts with a cover image and makes modifications to it in order to embed secret data.
- Alice and Bob work with the set of all possible covers and the sets of keys and messages that may, in the most general case depend on each cover:
  - $\mathcal{C} \ldots$ set of cover objects $x \in \mathcal{C}$
  - $\mathcal{K}(x) \ldots$ set of all stego keys for x
  - $\mathcal{M}(x) \ldots$ set of all messages that can be communicated in x.
- A steganographic scheme is a pair of embedding (Emb) and extraction (Ext) functions,
  - Emb : $\mathcal{C} \times \mathcal{K} \times \mathcal{M} \to \mathcal{C}$
  - Ext : $\mathcal{C} \times \mathcal{K} \to \mathcal{M}$

  such that for all $x \in \mathcal{C}$, and all $k \in \mathcal{K}(x), m \in \mathcal{M}(x)$,

$$\mathrm{Ext}(\mathrm{Emb}(x, k, m), k) = m. \tag{3}$$

Steganography by cover modification

- Alice can take any cover $x \in \mathcal{C}$ and embed in it any message $m \in \mathcal{M}(x)$ using any key $k \in \mathcal{K}(x)$, obtaining the stego image $y = \text{Emb}(x, k, m)$.
- The number of messages that can be communicated in a specific cover x depends on the steganographic scheme and it may also depend on the cover itself.
- *Example.* If $\mathcal{C}$ is the set of all 512×512 grayscale images and Alice embeds one message bit per pixel, then $\mathcal{M} = \{0, 1\}^{512 \times 512}$ and $| \mathcal{M} | = 2^{512 \times 512}$ for all $x \in \mathcal{C}$.

Steganography by cover modification

- Embedding algorithms for many steganographic schemes require a representation of cover and stego images using bits or, more generally, symbols from some alphabet $\mathcal{A}$ using a symbol-assigment function π,

$$\pi : \mathcal{X} \to \mathcal{A}, \tag{4}$$

  where $\mathcal{X}$ is the range of individual cover elements, such as pixels or DCT coeficients.

- One frequently used bit-assigment (parity) function is the least significiant bit

$$\mathsf{LSB}(x) = x \bmod 2. \tag{5}$$

Image steganography methods

- Image steganography methods can be divided in two groups, spatial domain methods and frequency domain methods.
- In the spatial domain, the secret message is directly embedded inside the least significant bit of the image.
- In the frequency domain, images are first transformed, and then the secret message is embedded in the image.

Image steganography methods

The spatial domain techniques involve:

- *Substitution system techniques.* Replace redundant or unneeded bits with secret message, such as: Least Significant Bit (LSB) and palette base image techniques.
- *Statistical system techniques.* Embeds one bit of information only in a carrier and creates statistical change, such as Pseudorandom Permutation (PP), patch work technique.
- *Spread spectrum techniques.* The stream of information to be transmitted is divided into small pieces, such as spread spectrum (SS).

Frequency domain techniques hide message data in the transform space of a signal such as Discrete Cosine Transform (DCT), Discrete Walvet Transform (DWT). Some techniques are common in two categories involve patch work technique and spread spectrum.

LSB algorithm

- The most frequently used steganography method is the technique of LSB substitution.
- This technique works best when the file is longer than the secret message file and if image is grayscale.
- In a gray-level image, every pixel consists of 8 bits. One pixel can hence display $2^8 = 256$ variations.
- The basic concept of LSB substitution is to embed the confidential data at the rightmost bits (bits with the smallest weighting) so that the embedding procedure does not affect the original pixel value greatly.
- LSB embedding can be applied to any collection of numerical data represented in digital form.

LSB algorithm

- Let us assume that secret message is $M \in \{0,1\}^m$ and cover image is $x \in \mathcal{X}^n$. Then $x[i] \in \mathcal{X} = \{0, \ldots, 2^{n_c} - 1\}$ is a sequence of integers.
  Example. $x[i]$ could be the light intensity at the ith pixel in an 8-bit grayscale image $(n_c = 8)$.
- Depending on the image format and the bit depth chosen for representing the individual values, each $x[i]$ can be represented using n_c bits $b[i,1], \ldots, b[i,n_c]$,

$$x[i] = \sum_{k=1}^{n_c} b[i,k] 2^{n_c - k.} \tag{6}$$

- We can think of the sequence $(b[i,1], \ldots, b[i,n_c])$ as the binary representation of $x[i]$ in big-endian form (the most significiant bit $b[i,1]$ is first.) The LSB is the last bit $b[i,n_c]$.

LSB algorithm

- LSB embedding replaces the LSBs of $x[i]$ with the message bits $m[i]$ and in the process we obtain the stego image $y[i]$.
- Note that in a color image the number of elements in the cover, n, is three times larger than for a grayscale image.
- The amplitude of changes in LSB embedding is 1, i.e. $\max_i [x[i] - y[i]] = 1$, which is the smallest possible change for any embedding operation.
- Under typical conditions, the embedding changes in an 8-bit grayscale or true-color image are not visually perceptible.

Algorithm of LSB Based Steganography

Algorithm 1 Algorithm to embed text message

```
1. Inputs: cover file and text message which need to be hidden
   in the cover file.
2. Convert text message into binary.
3. Calculate LSB of the each pixel of cover image.
4. Replace LSB of cover image with each bit of secret message
   one by one.
5. Return stego image.
```

Algorithm of LSB Based Steganography

Algorithm 2 Algorithm to retrieve text message

```
1. Input: the stego image.
2. Calculate LSB of each pixel of stego image.
3. Retrieve bits and convert each 8 bit into character.
```