Steganography

Dr. Shubhangi Sapkal

CLASSIFICATION OF STEGANOGRAPHY TECHNIQUES

1. Spatial Domain Techniques
2. Transform Domain Techniques
3. Spread Spectrum
4. Statistical Method
5. Distortion Technique

Spatial Domain

- These techniques use the pixel gray levels and their color values directly for encoding the message bits. These techniques are some of the simplest schemes in terms of embedding and extraction complexity.
- The major drawback of these methods is amount of additive noise that creeps in the image which directly affects the Peak Signal to Noise Ratio and the statistical properties of the image.
- Moreover these embedding algorithms are applicable mainly to lossless image compression schemes like TIFF images. For lossy compression scheme like JPEG, some of message bits get lost during compression step.

Transform Domain

- These techniques try to encode message bits in the transform domain coefficients of the image. Data embedding performed in transform domain is widely used for robust watermarking.
- Similar techniques can also realize large capacity embedding for Steganography. Candidate transforms include discrete cosine Transform (DCT), discrete wavelet transform (DWT), and discrete Fourier transform (DFT).
- By being embedded in the transform domain, the hidden data resides in more robust areas, spread across the entire image, and provides better resistance against signal processing. Eg: we can perform a block DCT and, depending on pay-load and robustness requirements, choose one or more components in each block to form a new data group that, in turn, is pseudo randomly scrambled and undergoes a second-layer transformation.
- Modification is then carried out on double transform domain coefficients using various schemes.
- These techniques have high embedding and extraction complexity. Because of robustness properties of transform domain embedding, these techniques are more applicable to “Watermarking” aspect of data hiding.

Spread Spectrum

- Spread spectrum transmission in radio communication transmit message below level of noise frequency.
- In Steganography it deals either with cover image as noise or tries to add as pseudo-noise in the cover image.
- Cover Image As Noise: A system that treats the cover image as noise can add a single value to that cover image. This value must be transmitted below that noise level. This means that the channel capacity of the image changes significantly. Thus, while this value can be a real number, in practice, the difficulty in recovering a real number decreases the value to a single bit.
- To permit the transmission of more than one bit, the cover image has to be broken into sub images. When these sub cover images are tiles, the technique is referred to as direct-sequence spread spectrum Steganography.
- When the sub cover images consist of separate points distributed over the cover image, the technique is referred to as frequency-hopping spread-spectrum Steganography. These techniques require searching the image for the carrier in order to then retrieve the data.
- These techniques are robust against gentle JPEG compression and can be made more robust through the pre-distortion of the carrier.

STATISTICAL METHODS

- Also known as model-based techniques, these techniques tend to modulate or modify the statistical properties of an image in addition to preserving them in the embedding process.
- This modification is typically small, and it is thereby able to take advantage of the human weakness in detecting luminance variation.
- Statistical Steganography techniques exploit the existence of a “1-bit”, where nearly a bit of data is embedded in a digital carrier.

STATISTICAL METHODS

- This process is done by simply modifying the cover image to make a sort of significant change in the statistical characteristics if “1” is transmitted, otherwise it is left unchanged.
- To send multiple bits, an image is broken into sub-images, each corresponding to a single bit of the message.

Distortion Technique

- It require original cover image during decoding process where decoder functions to check for differences between original cover image and distorted cover image in order to restore secret message.
- Encoder, adds a sequence of changes to cover image. So, information is described as being stored by signal distortion .
- Using this technique, a stego-object is created by applying sequence of modifications to cover image. This sequence of modifications is selected to match secret message required to transmit. Message is encoded at pseudo-randomly chosen pixels.
- If stego-image is different from cover image at given message pixel, then message bit is a “1.” Otherwise, message bit is a “0.”
- Encoder can modify “1” value pixels in such manner that statistical properties of image are not affected (which is different from many LSB methods).

Steganography Properties

- A few key properties that must be considered when creating a digital data hiding system are
  - Imperceptibility: Imperceptibility is the property in which a person should be unable to distinguish the original and the stego-image.
  - Embedding Capacity: Refers to the amount of secret information that can be embedded without degradation of the quality of the image.
  - Robustness: Refers to the degree of difficulty required to destroy embedded information without destroying the cover image.

Steganography techniques by file format

- There exist two types of materials in steganography: message and carrier. Message is the secret data that should be hidden and carrier is the material that takes the message in it. There are many types of steganography methods.
- Different categories of file formats that can be used for steganography techniques – Text, Image, Audio

TEXT STEGANOGRAPHY

- Text steganography can be achieved by altering the text formatting, or by altering certain characteristics of textual elements (e.g., characters).
- The goal in the design of coding methods is to develop alterations that are reliably decodable (even in the presence of noise) yet largely indiscernible to the reader.
- These criteria, reliable decoding and minimum visible change, are somewhat conflicting; herein lies the challenge in designing document marking techniques.
- The document format file is a computer file describing the document content and page layout (or formatting), using standard format description languages such as PostScript2, TeX, @off, etc. It is from this format file that the image - what the reader sees - is generated. The three coding techniques illustrate different approaches.

TEXT STEGANOGRAPHY-Line-Shift Coding

Line-Shift Coding

- This is a method of altering a document by vertically shifting the locations of text lines to encode the document uniquely. This encoding may be applied either to the format file or to the bitmap of a page image.
- The embedded codeword may be extracted from the format file or bitmap. In certain cases this decoding can be accomplished without need of the original image, since the original is known to have uniform line spacing between adjacent lines within a paragraph.

TEXT STEGANOGRAPHY- Word-Shift Coding

Word-Shift Coding

- This is a method of altering a document by horizontally shifting the locations of words within text lines to encode the document uniquely.
- This encoding can be applied to either the format file or to the bitmap of a page image. Decoding may be performed from the format file or bitmap.
- The method is applicable only to documents with variable spacing between adjacent words. Variable spacing in text documents is commonly used to distribute white space when justifying text. Because of this variable spacing, decoding requires the original image - or more specifically, the spacing between words in the un-encoded document.

TEXT STEGANOGRAPHY- **Feature Coding**

Feature Coding

- This is a coding method that is applied either to a format file or to a bitmap image of a document. The image is examined for chosen text features, and those features are altered, or not altered, depending on the codeword.
- Decoding requires the original image, or more specifically, a specification of the change in pixels at a feature. There are many possible choices of text features; for example, alter upward, vertical endlines - that is the tops of letters, b, d, h, etc. These endlines are altered by extending or shortening their lengths by one (or more) pixels, but otherwise not changing the endline feature.

IMAGE STEGANOGRAPHY

- Hiding information inside images is a popular technique nowadays. An image with a secret message inside can easily be spread over the World Wide Web or in newsgroups.
- To hide a message inside an image without changing its visible properties, the cover source can be altered in ”noisy” areas with many color variations, so less attention will be drawn to the modifications.
- The most common methods to make these alterations involve the usage of the least-significant bit or LSB, masking, filtering and transformations on the cover image. These techniques can be used with varying degrees of success on different types of image files.

IMAGE STEGANOGRAPHY- Least Significant Bits

Least Significant Bits

- A simple approach for embedding information in cover image is using Least Significant Bits (LSB). The simplest steganography techniques embed the bits of the message directly into least significant bit plane of the cover image in a deterministic sequence. Modulating the least significant bit does not result in human-perceptible difference because the amplitude of the change is small.
- To hide a secret message inside an image, a proper cover image is needed. Because this method uses bits of each pixel in the image, it is necessary to use a lossless compression format, otherwise the hidden information will get lost in the transformations of a lossy compression algorithm.
- When using a 24-bit color image, a bit of each of the red, green and blue color components can be used, so a total of 3 bits can be stored in each pixel. For example, the following grid can be considered as 3 pixels of a 24-bit color image, using 9 bytes of memory:

IMAGE STEGANOGRAPHY- **Least Significant Bits**

(00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)

When the character A, which binary value equals 10000001, is inserted, the following grid results:

(00100111 11101000 11001000)
(00100110 11001000 11101000)
(11001000 00100111 11101001)

- In this case, only three bits needed to be changed to insert the character successfully. On average, only half of the bits in an image will need to be modified to hide a secret message using the maximal cover size.
- The result changes that are made to the least significant bits are too small to be recognized by the human visual system, so the message is effectively hidden.
- As you see, the least significant bit of third color is remained without any changes. It can be used for checking the correctness of 8 bits which are embedded in these 3 pixels. In other words, it could be used as “parity bit”.

IMAGE STEGANOGRAPHY- *Masking and filtering*

Masking and filtering

- Masking and filtering techniques, usually restricted to 24 bits or grayscale images, take a different approach to hiding a message. These methods are effectively similar to paper watermarks, creating markings in an image.
- This can be achieved for example by modifying the luminance of parts of the image. While masking does change the visible properties of an image, it can be done in such a way that the human eye will not notice the anomalies. Since masking uses visible aspects of the image, it is more robust than LSB modification with respect to compression, cropping and different kinds of image processing.
- The information is not hidden at the ”noise” level but is inside the visible part of the image, which makes it more suitable than LSB modifications in case a lossy compression algorithm like JPEG is being used.

IMAGE STEGANOGRAPHY- *Transformations*

Transformations

- A more complex way of hiding a secret inside an image comes with the use and modifications of discrete cosine transformations.
- Discrete cosine transformations (DCT)), are used by the JPEG compression algorithm to transform successive 8 x 8 pixel blocks of the image, into 64 DCT coefficients each. Each DCT coefficient *F(u, v)* of an 8 x 8 block of image pixels *f(x, y)* is given by:

IMAGE STEGANOGRAPHY- *Transformations*

$$F(u,v) = \frac{1}{4}C(u)C(v)\left[\sum_{x=0}^{7}\sum_{y=0}^{7} f(x,y) * \cos\frac{(2x+1)u\pi}{16}\cos\frac{(2y+1)v\pi}{16}\right], \; C(x) = \begin{cases} \frac{1}{\sqrt{2}} & x = 0 \\ 1 & else. \end{cases}$$

After calculating the coefficients, the following quantizing operation is performed:

$$F^{Q}(u,v) = \left\lfloor \frac{F(u,v)}{Q(u,v)} \right\rfloor$$

Where *Q(u, v)* is a 64-element quantization table.

AUDIO STEGANOGRAPHY

- In audio steganography, secret message is embedded into digitized audio signal which result slight altering of binary sequence of the corresponding audio file. There are several methods available for audio steganography. We are going to have a brief introduction on some of them.

AUDIO STEGANOGRAPHY- *LSB Coding*

LSB Coding

- Sampling technique followed by Quantization converts analog audio signal to digital binary sequence.
- In this technique LSB of binary sequence of each sample of digitized audio file is replaced with binary equivalent of secret message.

AUDIO STEGANOGRAPHY-*Phase Coding*

Phase Coding

- Human Auditory System (HAS) can't recognize the phase change in audio signal as easy it can recognize noise in the signal.
- The phase coding method exploits this fact. This technique encodes the secret message bits as phase shifts in the phase spectrum of a digital signal, achieving an inaudible encoding in terms of signal-to-noise ratio.

AUDIO STEGANOGRAPHY-*Spread Spectrum*

Spread Spectrum

- There are two approaches used in this technique: the direct sequence spread spectrum (DSSS) and frequency hopping spread spectrum (FHSS). Direct-sequence spread spectrum (DSSS) is a modulation technique used in telecommunication. As with other spread spectrum technologies, the transmitted signal takes up more bandwidth than the information signal that is being modulated. Direct-sequence spread-spectrum transmissions multiply the data being transmitted by a "noise" signal.
- This noise signal is a pseudorandom sequence of 1 and −1 values, at a frequency much higher than that of the original signal, thereby spreading the energy of the original signal into a much wider band. The resulting signal resembles white noise.

AUDIO STEGANOGRAPHY-*Spread Spectrum*

- However, this noise-like signal can be used to exactly reconstruct the original data at the receiving end, by multiplying it by the same pseudorandom sequence (because 1 × 1 = 1, and −1 × −1= 1).
- This process, known as "de-spreading", mathematically constitutes a correlation of the transmitted Pseudorandom Noise (PN) sequence with the receiver's assumed sequence. For de-spreading to work correctly, transmit and receive sequences must be synchronized.
- This requires the receiver to synchronize its sequence with the transmitter's sequence via some sort of timing search process.
- In contrast, frequency-hopping spread spectrum pseudo-randomly retunes the carrier, instead of adding pseudo-random noise to the data, which results in a uniform frequency distribution whose width is determined by the output range of the pseudo-random number generator.

AUDIO STEGANOGRAPHY-*Echo Hiding*

Echo Hiding

- In this method the secret message is embedded into cover audio signal as an echo. Three parameters of the echo of the cover signal namely amplitude, decay rate and offset from original signal are varied to represent encoded secret binary message. They are set below to the threshold of Human Auditory System (HAS) so that echo can’t be easily resolved.
- Video files are generally consists of images and sounds, so most of the relevant techniques for hiding data into images and audio are also applicable to video media.

- In the case of Video steganography sender sends the secret message to the recipient using a video sequence as cover media. Optional secret key ‘K’ can also be used during embedding the secret message to the cover media to produce ‘stego-video’.
- After that the stego-video is communicated over public channel to the receiver. At the receiving end, receiver uses the secret key along with the extracting algorithm to extract the secret message from the stego-object.

AUDIO STEGANOGRAPHY-*Echo Hiding*

- The original cover video consists of frames represented by Ck(m,n) where 1 £ k £ N. ‘N’ is the total number of frame and m,n are the row and column indices of the pixels, respectively.
- The binary secret message denoted by Mk(m, n) is embedded into the cover video media by modulating it into a signal. Mk(m, n) is defined over the same domain as the host Ck(m,n).The stego-video signal is represented by the equation

$$Sk(m, n) = Ck(m, n) + ak(m, n)\, Mk(m, n)\ ,\ k = 1, 2, 3 \ldots N$$

Where ak (m, n) is a scaling factor. For simplicity ak (m, n) can be considered to be constant over all the pixels and frames. So the equation becomes

$$Sk(m, n) = Ck(m, n) + a(m, n)\, Mk(m, n)\ ,\ k = 1, 2, 3 \ldots N$$

References

- Masoud Nosrati, Ronak Karimi, Mehdi Hariri, “An introduction to steganography methods”, *World Applied Programming, Vol (1), No (3), August 2011. 191-195.*