Digital Watermarking and Steganography

Han Tao (htao@cise.ufl.edu)

Digital Watermarking

- Definition: Insertion of information into data through slight modification of the data
- Applications: copyright protection; traitor tracing; tamper proofing; copy control
- Requirements: Imperceptible or visible; robust or fragile, depending on application; public or private watermarking; redundant; secure
- Techniques:
  - ➢ Spatial
    - Fast and easy to embed; fragile

    - ***Patchwork algorithm*****:** a pseudorandom statistical process.
      Two patches A and B are chosen pseudorandomly and repeatedly so they are scattered throughout the image. The image data in patch A are lightened and those in patch B are darkened. The change to the original data indicates a presence or absence of watermark.

    - ***Shuffling*****:** based on the concept of texture in an image.
      Embeddable and unembeddable coefficients of the data are separated. All the coefficients are concatenated into a string and shuffled. The shuffled string is divided into segments of equal length and watermark is embedded into these segments. One bit of watermark is encoded into an embeddable coefficient using a lookup table. The string is reshuffled inversely.

  - ➢ Simple spectral
    - Modification of last bit of DCT coefficients
    - Useful for formats that store data in the frequency domain
    - Relatively easy to implement; easy to detect and destroy

  - ➢ Spread spectrum
    - Allows narrow band watermark to be spread to all the frequency bands
    - The most robust of existing techniques

- Robustness
  - ➢ Signal processing attacks
    - Signal diminishment – noise addition; over-marking; compression;

- Enhancement techniques - low pass filtering; sharpening; histogram modifications; gamma correction; color quantisation

➢ Geometric attacks – cropping; transformations

➢ Synchronization problems

<u>Steganography</u>

- Definition: The hiding of secret messages within another seemingly innocuous message, or carrier.
- Requirements
  - Imperceptible; statistically undetectable
  - Unverifiable without the stego-key
  - Large capacity
- Applications: Confidential communication
- Techniques
  - *Substitution system*s: substitute redundant parts of a cover with a secret message
  - *Transform domain technique*s: embed secret in the frequency domain
  - *Spread spectrum techniques*: adopt ideas from spread spectrum communication
  - *Statistical methods*: encode information by changing several statistical properties of a cover and use hypothesis testing in the extraction process
  - *Distortion techniques*: store information by signal distortion and measure the deviation from the original cover in the decoding step
  - *Cover generation methods*: encode information in the way a cover for secret communication is created
- Attacks
  - Stego-only; Known cover; Known message; Chosen stego; Chosen message; Known stego
  - To extract or disable hidden information
  - Lossy compression; Image processing attacks: rotating; cropping; blurring

<u>Bibliography</u>

- Stefan Katzenbeisser. Fabien A. P. Petitcolas (Eds). “Information Hiding Techniques for Steganography and Digital Watermarking.” Artech House Books, January 2000.
- Helen Wollan. “Digital Watermarking in Still Images.”
  http://mrs.umn.edu/~lopezdr/seminar/spring2000/wollan.pdf