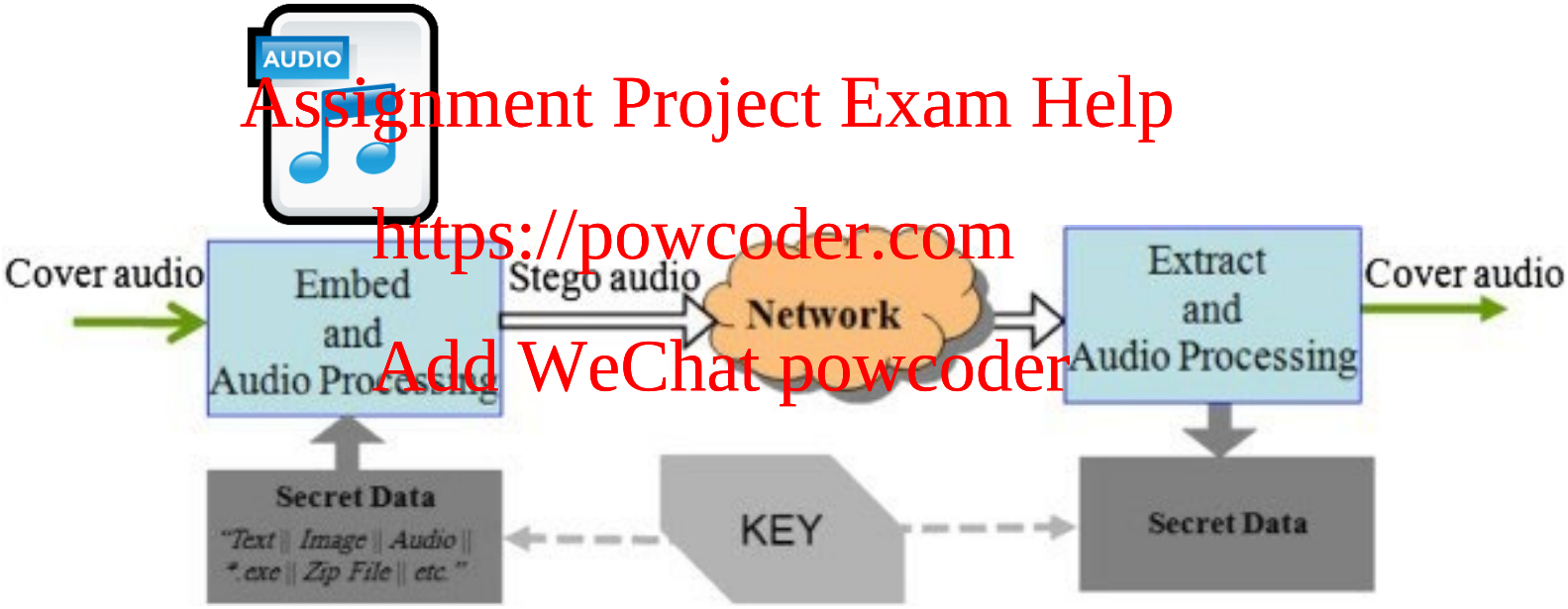
Audio Steganography



Audio Steganography (cont.)

3.1) Audio Steganography: Least Significant Bit (LSB) Coding

- LSB of each audio sample is replaced with a secret bit

sample in time

quantize (round up) in value

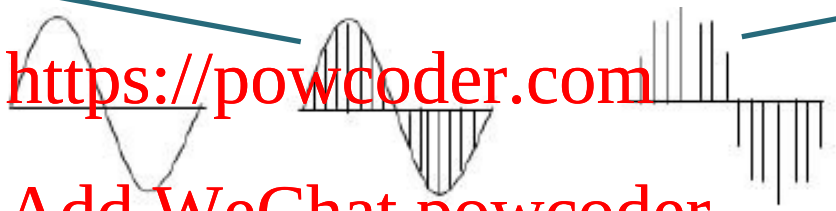
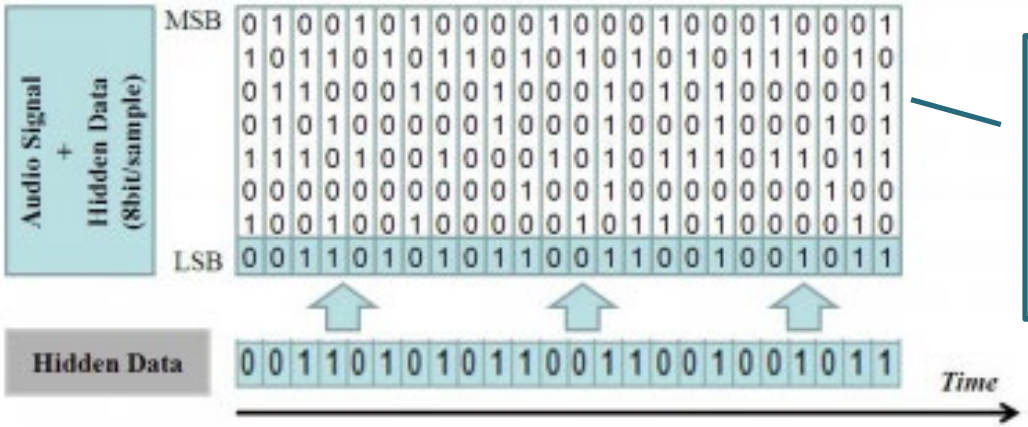
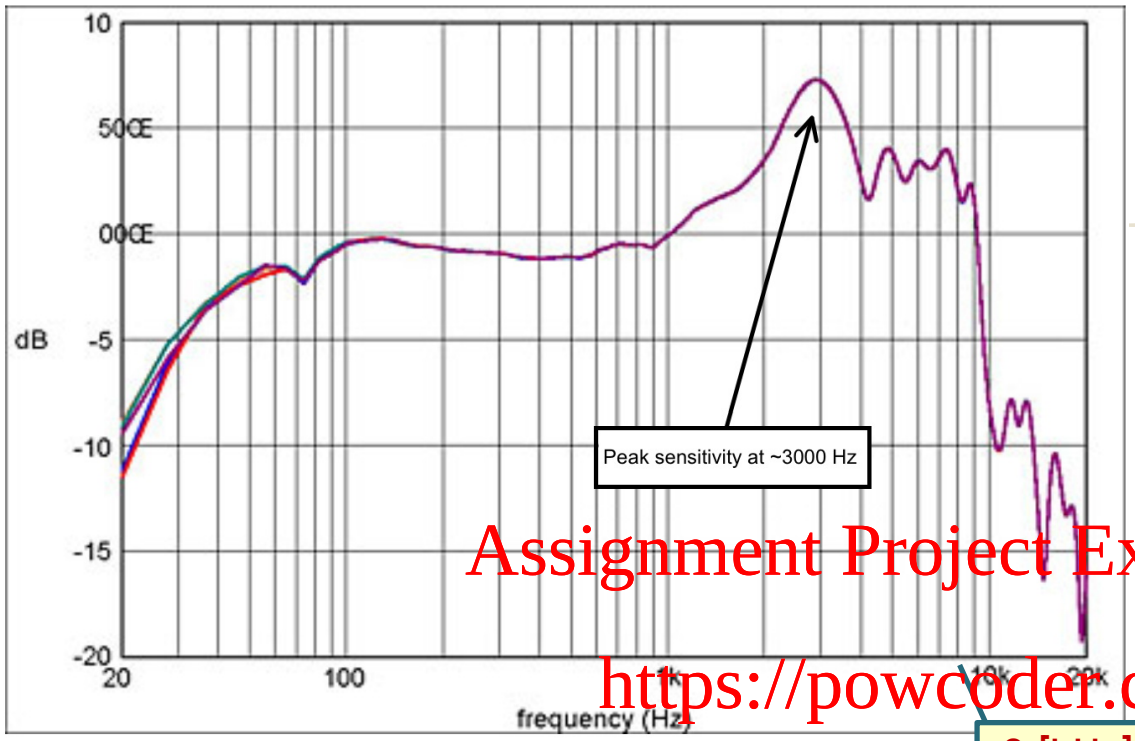


Figure 3: Sampling of the Sine Wave followed by Quantization process.



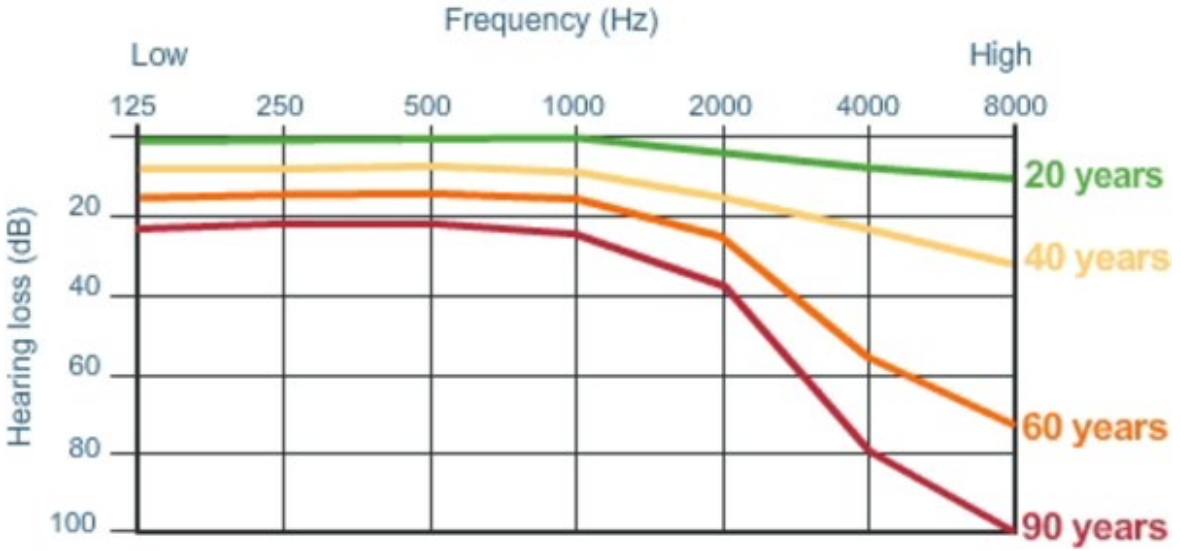
finite # of samples represented by a finite # of bits



sensitivity of a
normal human ear
to different frequencies

http://umdberg.pbworks.com/w/page/131541489/Frequency%20response%20of%20the%20human%20ear

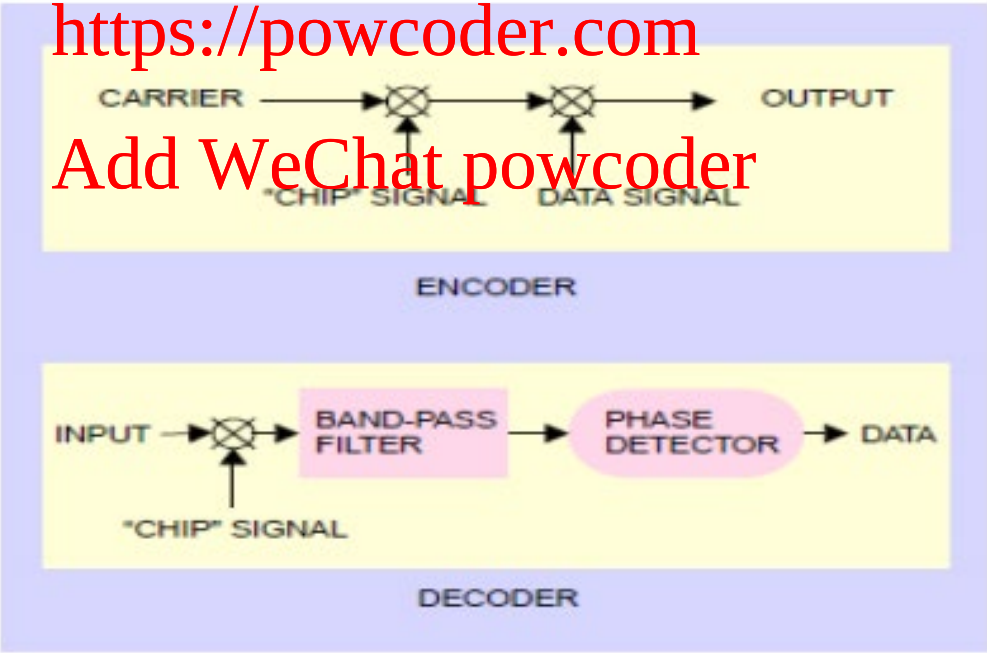
sensitivity of a
human ear
by age



Audio Steganography (cont.)

3.2) Audio Steganography: Spread Spectrum

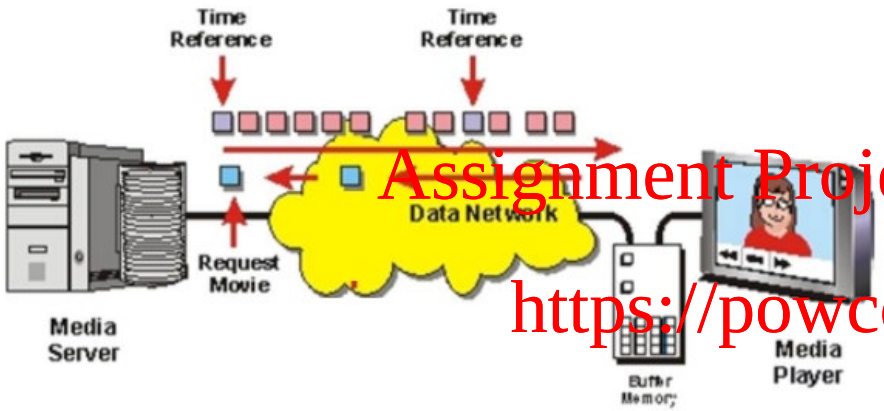
- secret bit is spread across cover audio in form of high frequency noise

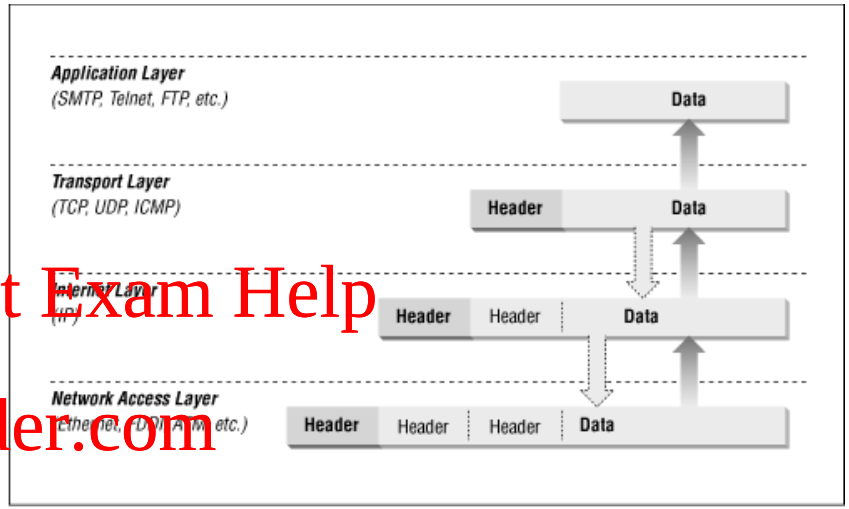


http://www.sersc.org/journals/IJDTA/vol2_no2/1.pdf

Datagram Steganography

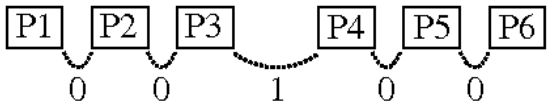
Datagram / Packet / Network Steganography

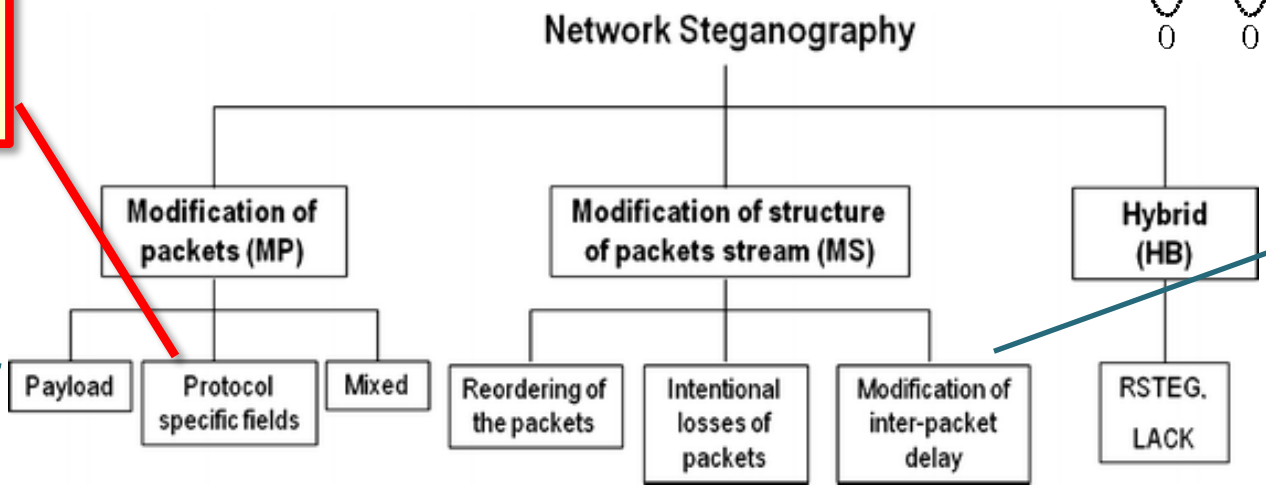




(e.g.) place secret bits into packet header(s)

(e.g.) break secret message into 1-byte packets



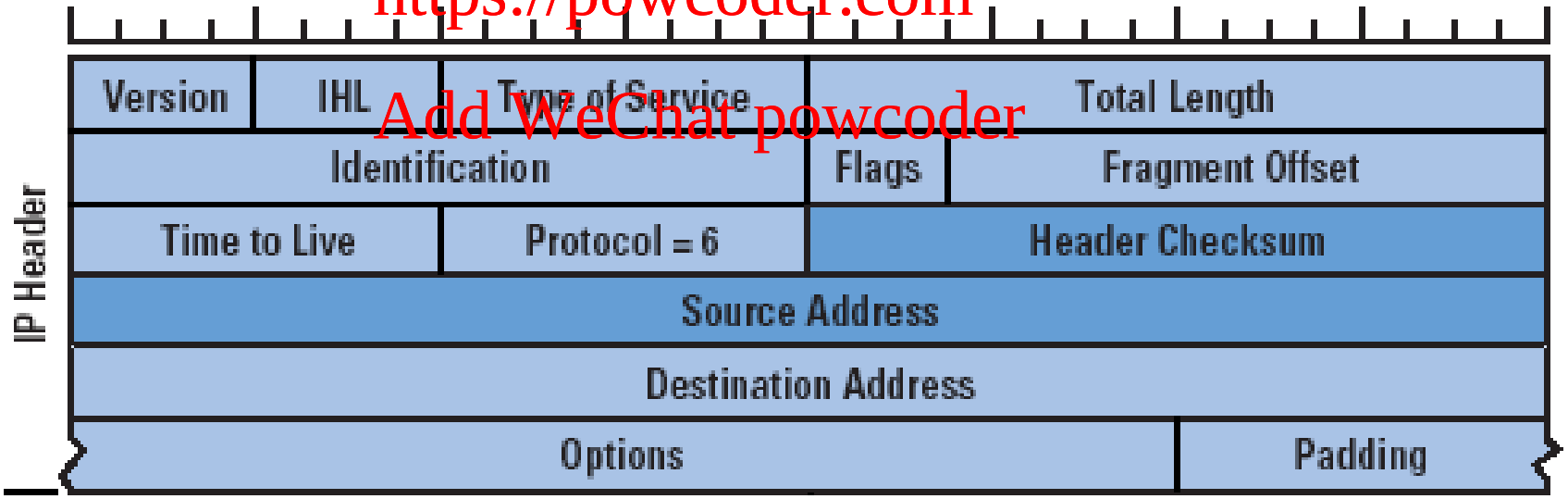


(e.g.) control the timing of individual packet transmission

Datagram Steganography (cont.)

4.1) IP Datagram Steganography: Using Identification Field in IP Packet

- IP Identification Field = 16 bits long - used to uniquely identify an IP packet - useful in case of fragmentation



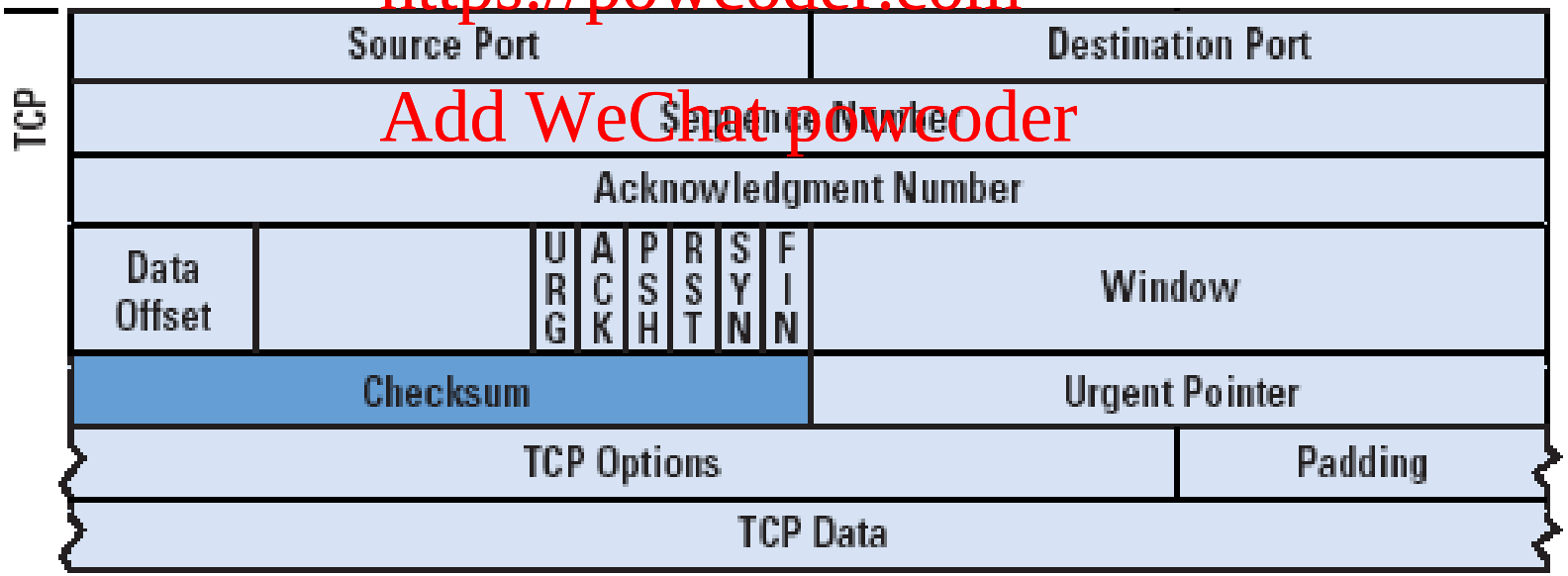
Could Source & Destination Address be used to hide data?!

How about Options field?

Datagram Steganography (cont.)

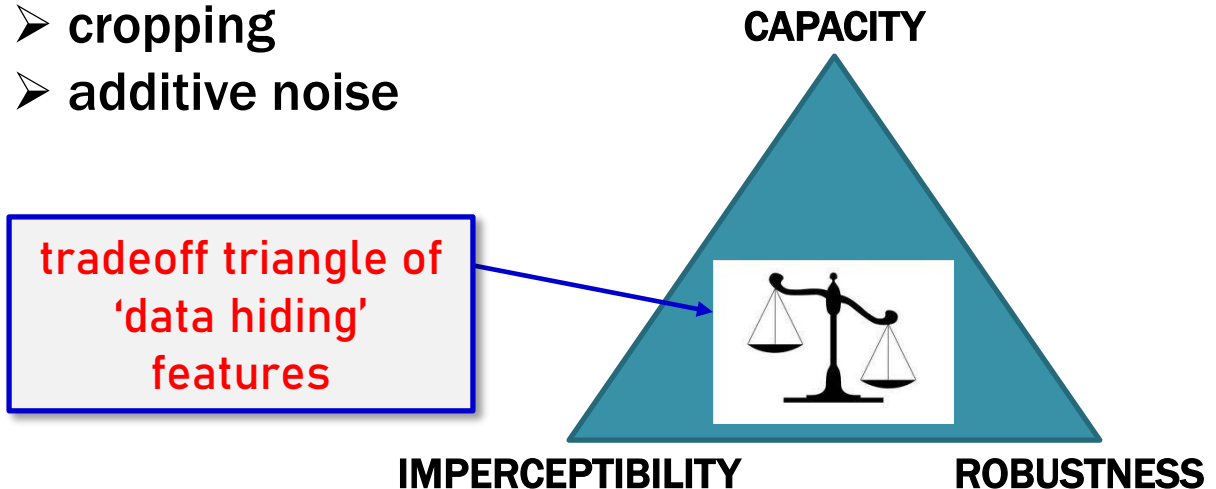
4.2) Datagram Steganography: Using Sequence Number in TCP Packets

- TCP Sequence Number = 32 bits - keeps track of byte order in payload - useful in payload reassembly



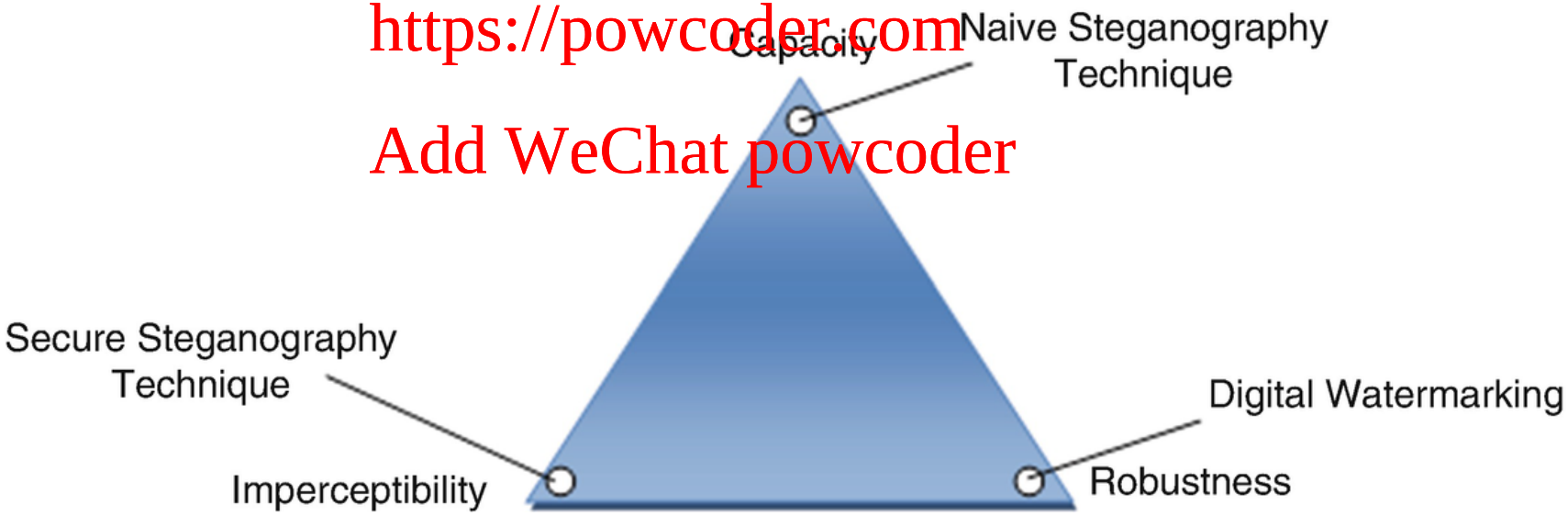
Data Hiding Tech.: Evaluation

- **Magic Triangle of Data Hiding Techniques** – outlines different goals / trade-off of digital steganography
  - **capacity**: how much bits can be hidden in a cover image
  - **imperceptibility**: how easy it is to spot hidden data (invisibility / secrecy)
  - **robustness**: hidden message in stego-object unaffected by
    - rotation
    - compression
    - cropping
    - additive noise



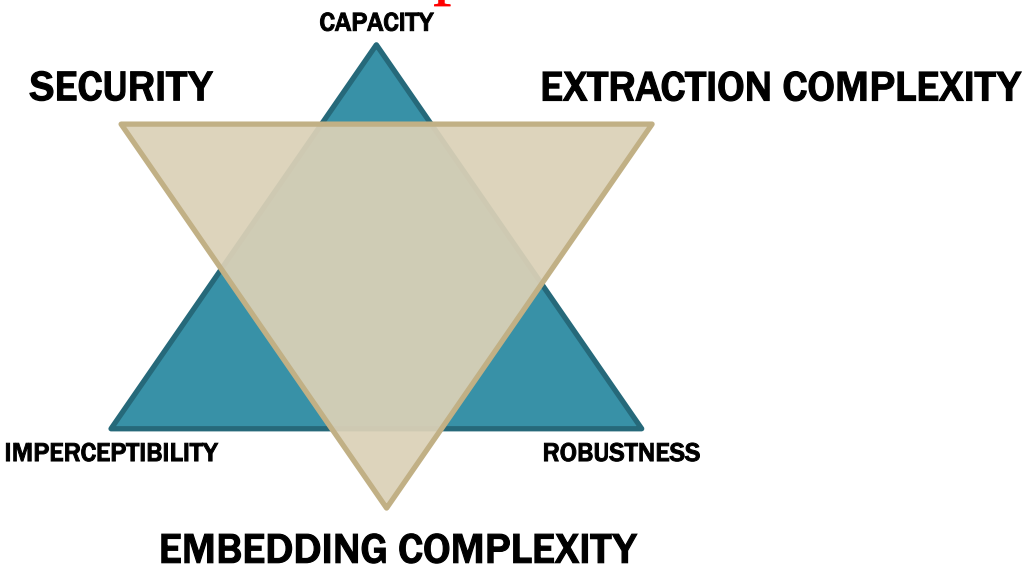
Data Hiding Tech.: Evaluation (cont.)

Example: tradeoff triangle – steganography vs. watermarking



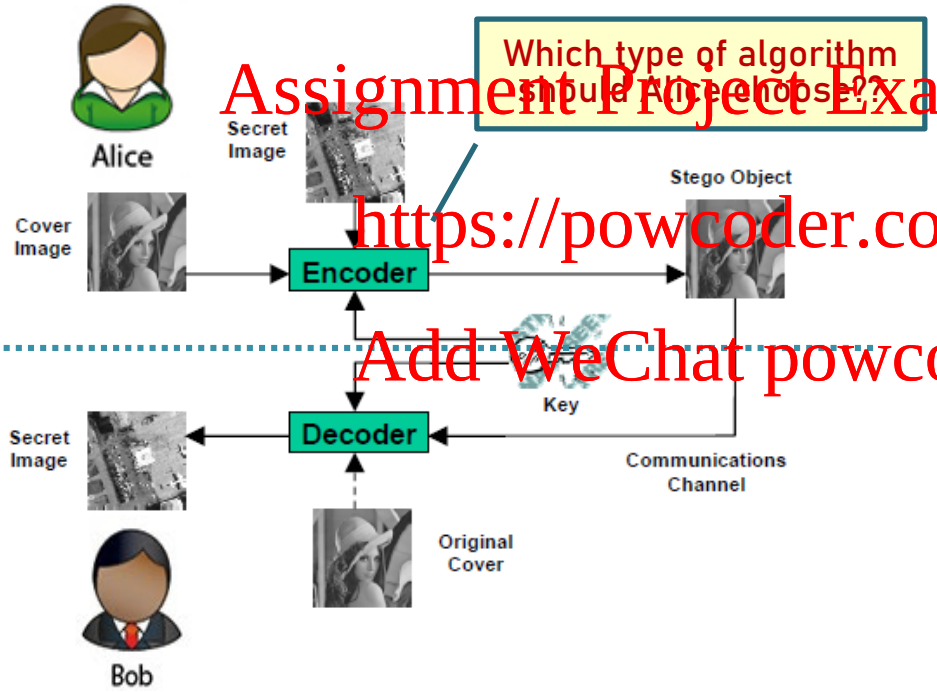
Data Hiding Tech.: Evaluation (cont.)

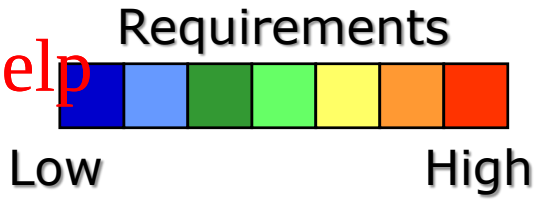
- **Additional Requirements on Data Hiding Techniq.**
  - **security**: embedded info. cannot be removed unless attacker has the full knowledge of algorithm and/or secret key
  - **extraction complexity**: computational effort/time to extract hidden information
  - **embedding complexity**: computational effort/time to embed hidden information

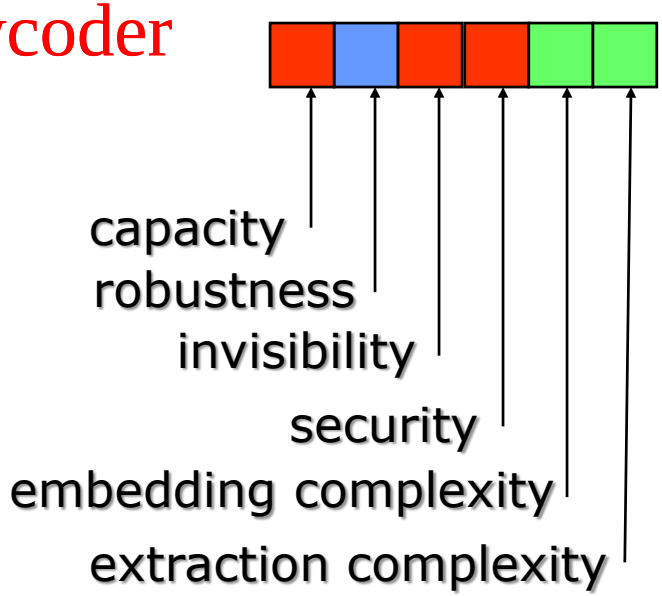


Data Hiding Tech.: Evaluation (cont.)

- **Comprehensive Look at Requirements of Digital 'Image-in-Image' Steganography**



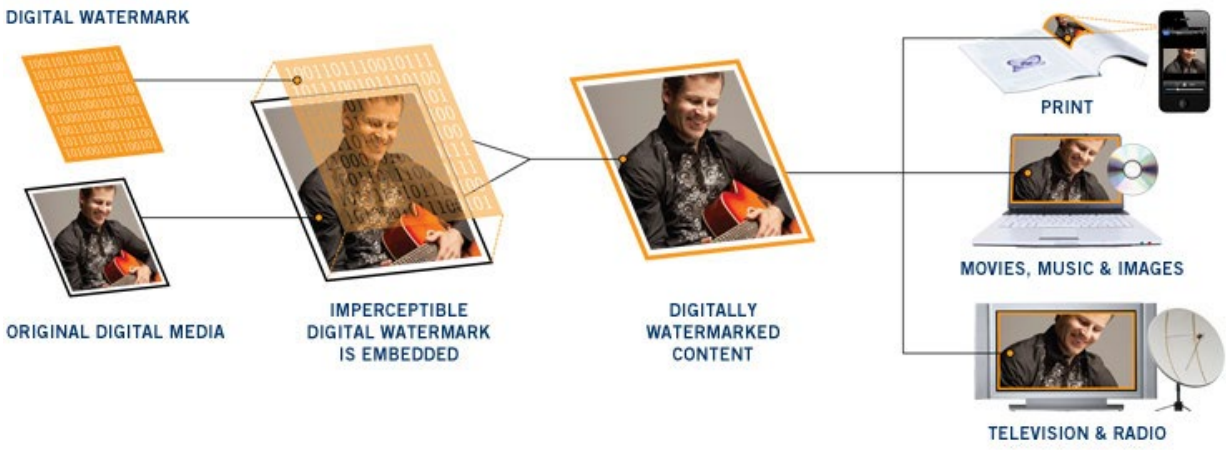




Alice is sending the stego image to Bob as an email attachment. The packet(s) carrying Alice's email travel through intermediate routers.

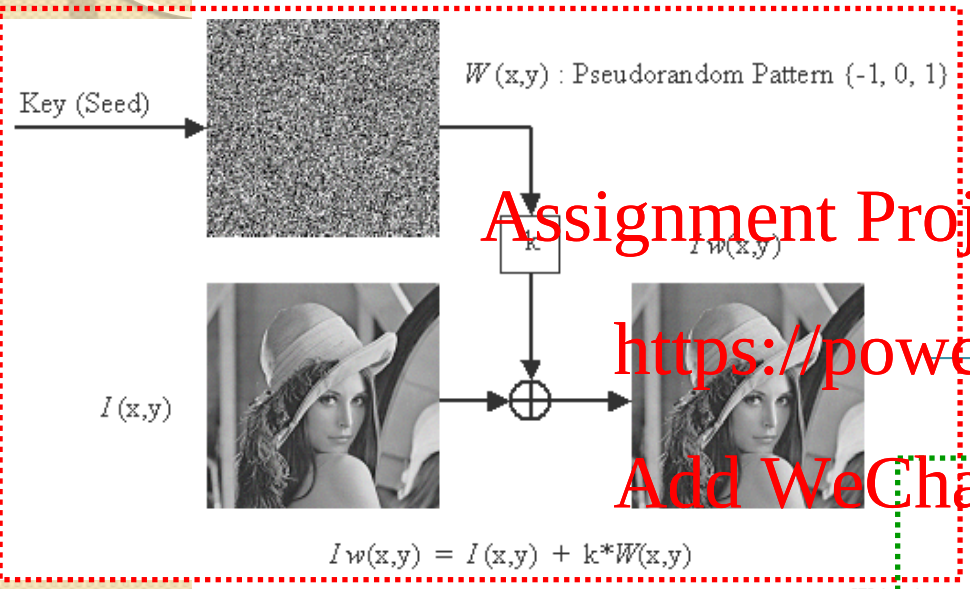
Watermarking

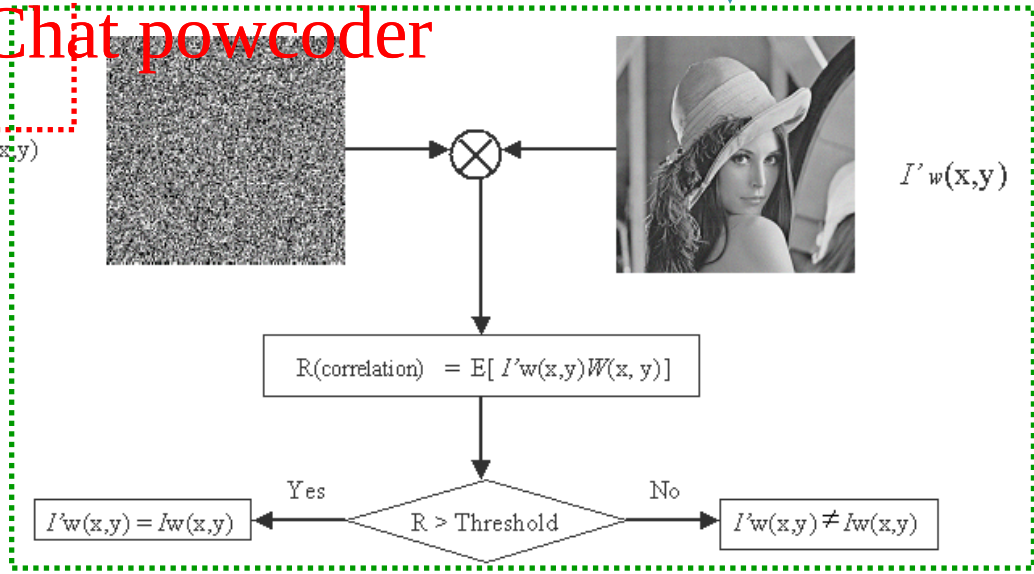
- **Watermarking - Process Components / Terminology**
  - **Watermark (W)**
    - each owner has a unique watermark (e.g., 'layer' of 1 bit/pixel)
  - **Marking Algorithm**
    - incorporates the watermark into the image
  - **Verification Algorithm**
    - determines the integrity/ownership of the image



Watermarking (cont.)

Example: Watermarking in Space Domain





http://scien.stanford.edu/pages/labsite/2001/ee368/projects2001/dropbox/project06/

Watermarking (cont.)

- **Watermarking - Categories**
  - **Private vs. Public**
    - Private – a secret key was used in watermarking process
      => only authorized users can recover it
      (can be used by owner to demonstrate ownership once he discovers illicit use)
    - Public – anyone can read watermark – 'secret' key not needed
      (can be used to actually discover all illicit uses – e.g., by providing the watermark key to search crawlers)