EECS 3482
Introduction to Computer Security

http://www.marw0rm.com/steganography-what-your-eyes-dont-see/

Instructor: N. Vlajic, Fall 2021

Learning Objectives

Upon completion of this material, you should be able to:

- Identify various motivations and implementation **approaches to information protection / hiding**.
- Describe the basic concepts and uses of digital steganography.
- Explain the key principles pertaining to four common types of digital steganography: plaintext, image, audio and datagram.
- Enlist the common uses of digital watermarking.
- Explain the difference between digital watermarking and digital fingerprinting.

Required Reading

Computer Security, Stallings: ???

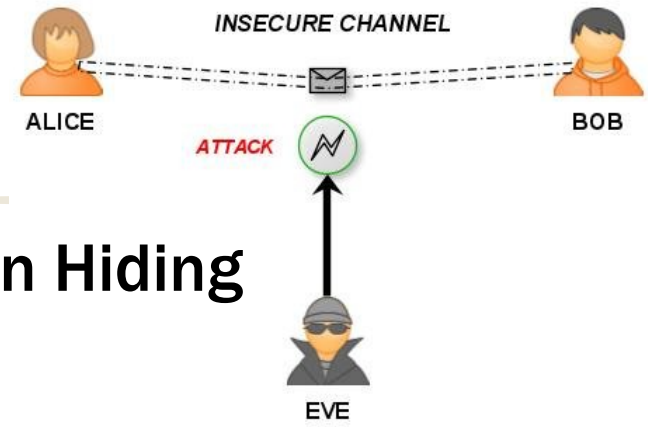
Introduction

- **WHO Protects Information in Digital Age & WHY?**
  - companies: trade secrets, intel. prop., customer records, …
  - governments: classified information, citizen records, …
  - individuals: personal & sensitive information (protect from hackers and/or authorities)

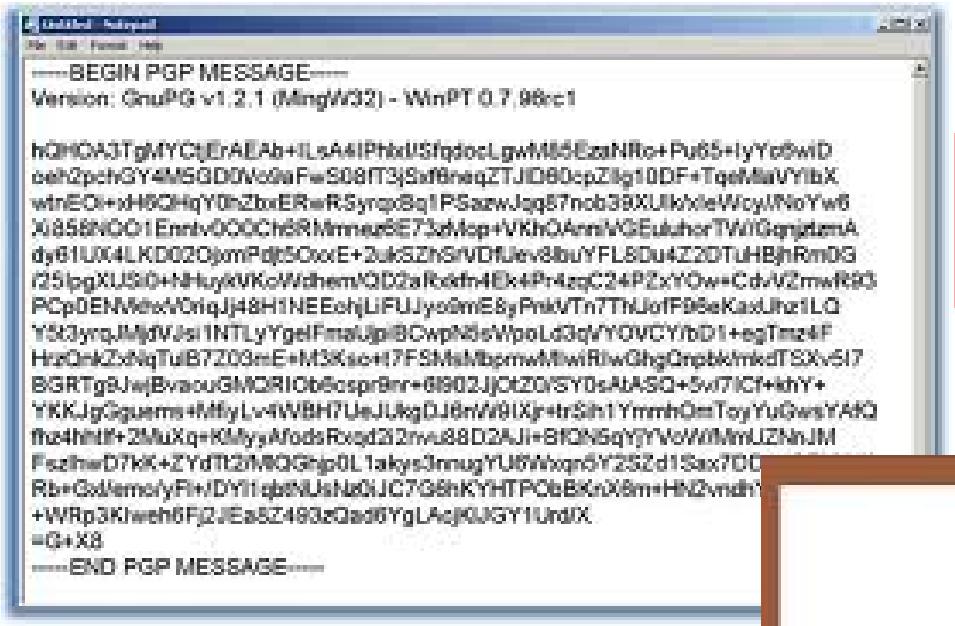
Introduction (cont.)

- **Information Protection in Digital Age** – techniques of digital information protection can be grouped in two major categories:
  - **Information Encryption**
    - the content is 'scrambled' using a crypto-key, so it becomes meaningless
    - however, the presence of information is 'obvious'
    - no matter how 'unbreakable', encrypted message will arose suspicion
  - **Information Hiding**
    - the goal is not just to prevent others from accessing hidden information, but to make others unaware of the very existence of the hidden information

Introduction (cont.)

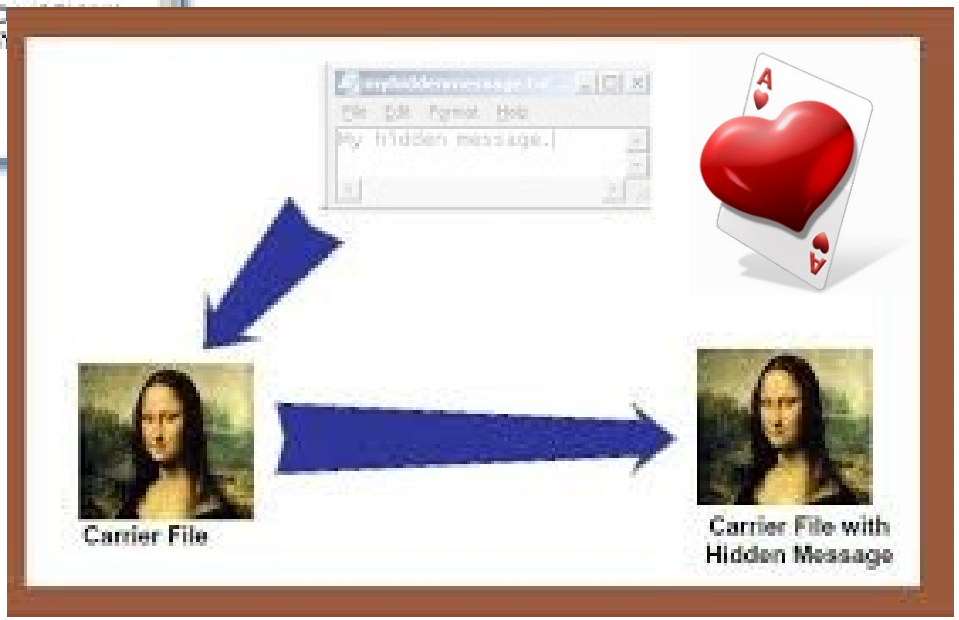


Example: Encryption vs. Information Hiding



unauthorized users will be aware of the existence of confidential data but will not be able to 'read' it

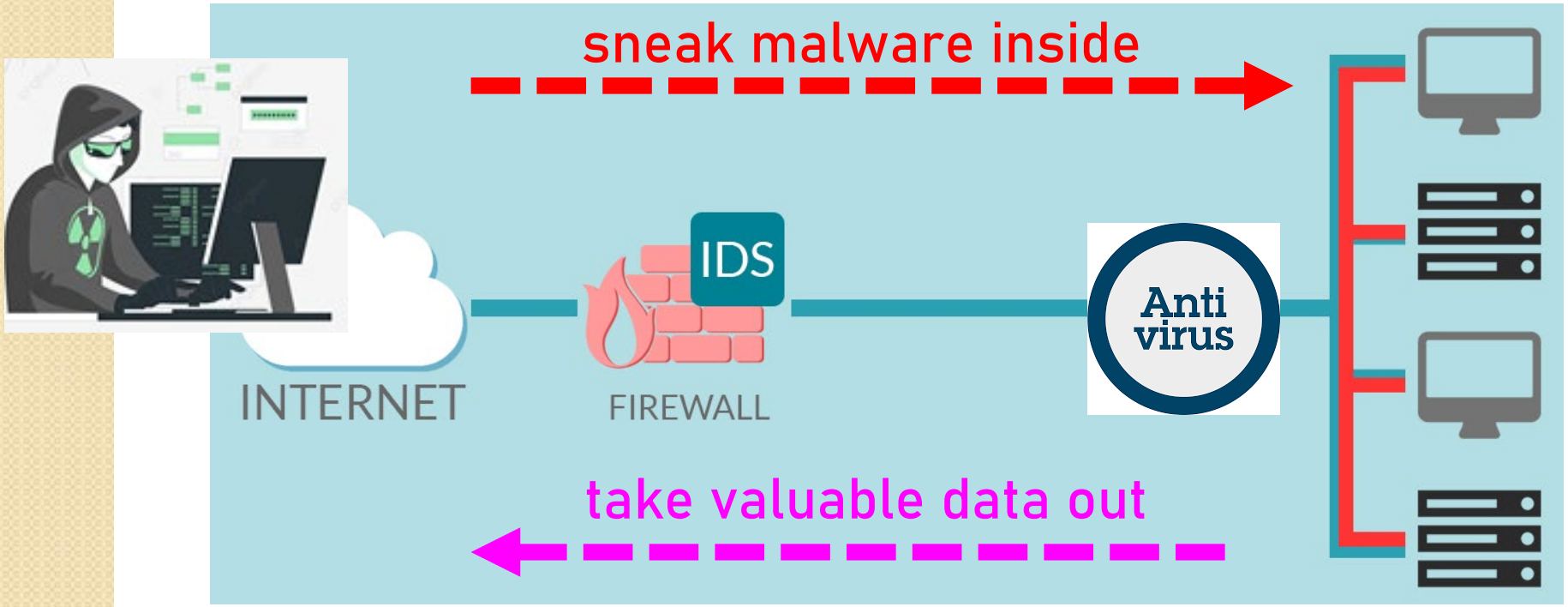
the actual existence of the confidential data is entirely obscured from unauthorized users



Can be used when protecting both – data 'at rest' and data 'in transit' !

Introduction (cont.)

Example: Use of Steganography by Hackers …



target system
(e.g., bank, hospital, industrial facility, …

MITRE | ATT&CK

Adversarial Tactics and Techniques

ID: T1027.003

Sub-technique of: T1027

Tactic: Defense Evasion

Platforms: Linux, Windows, macOS

CAPEC ID: CAPEC-636

TECHNIQUES

Modify System Image

Network Boundary Bridging

Obfuscated Files or Information

Binary Padding

Software Packing

Steganography

Home > Techniques > Enterprise > Obfuscated Files or Information > Steganography

Obfuscated Files or Information: Steganography

Other sub-techniques of Obfuscated Files or Information (6)

Adversaries may use steganography techniques in order to prevent the detection of hidden information. Steganographic techniques can be used to hide data in digital media such as images, audio tracks, video clips, or text files.

Duqu was an early example of malware that used steganography. It encrypted the gathered information from a victim's system and hid it within an image before exfiltrating the image to a C2 server.[1]

By the end of 2017, a threat group used `Invoke-PSImage` to hide PowerShell commands in an image file (.png) and execute the code on a victim's system. In this particular case the PowerShell code downloaded another obfuscated script to gather intelligence from the victim's machine and communicate it back to the adversary.[2]

https://attack.mitre.org/techniques/T1027/003/

Introduction (cont.)

Mimikatz is a leading post-exploitation tool that dumps passwords from memory, as well as hashes, PINs and Kerberos tickets.

Home › Latest News › Steganography used in attack on industrial enterprises

Latest News | Security

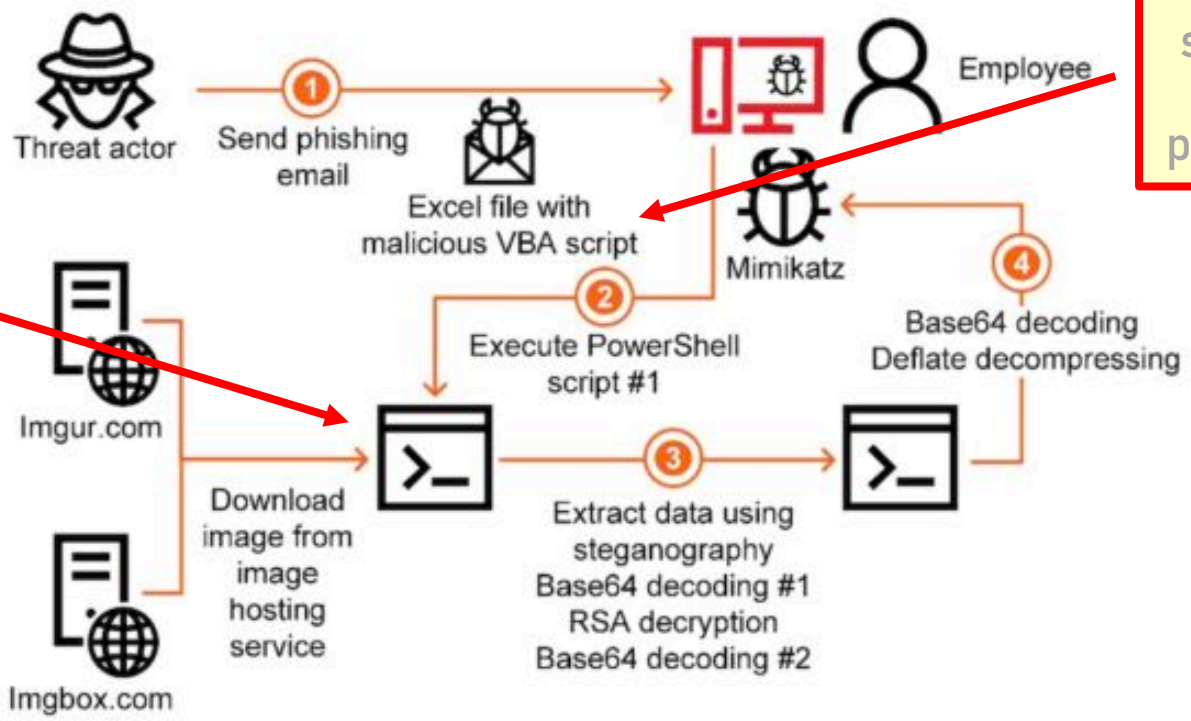
Steganography used in attack on industrial enterprises

By **Ian Murphy** - June 1, 2020

Mimikatz malware spread

Warhead - small hard-to-detect piece of code

Propagation Engine



Attack kill chain

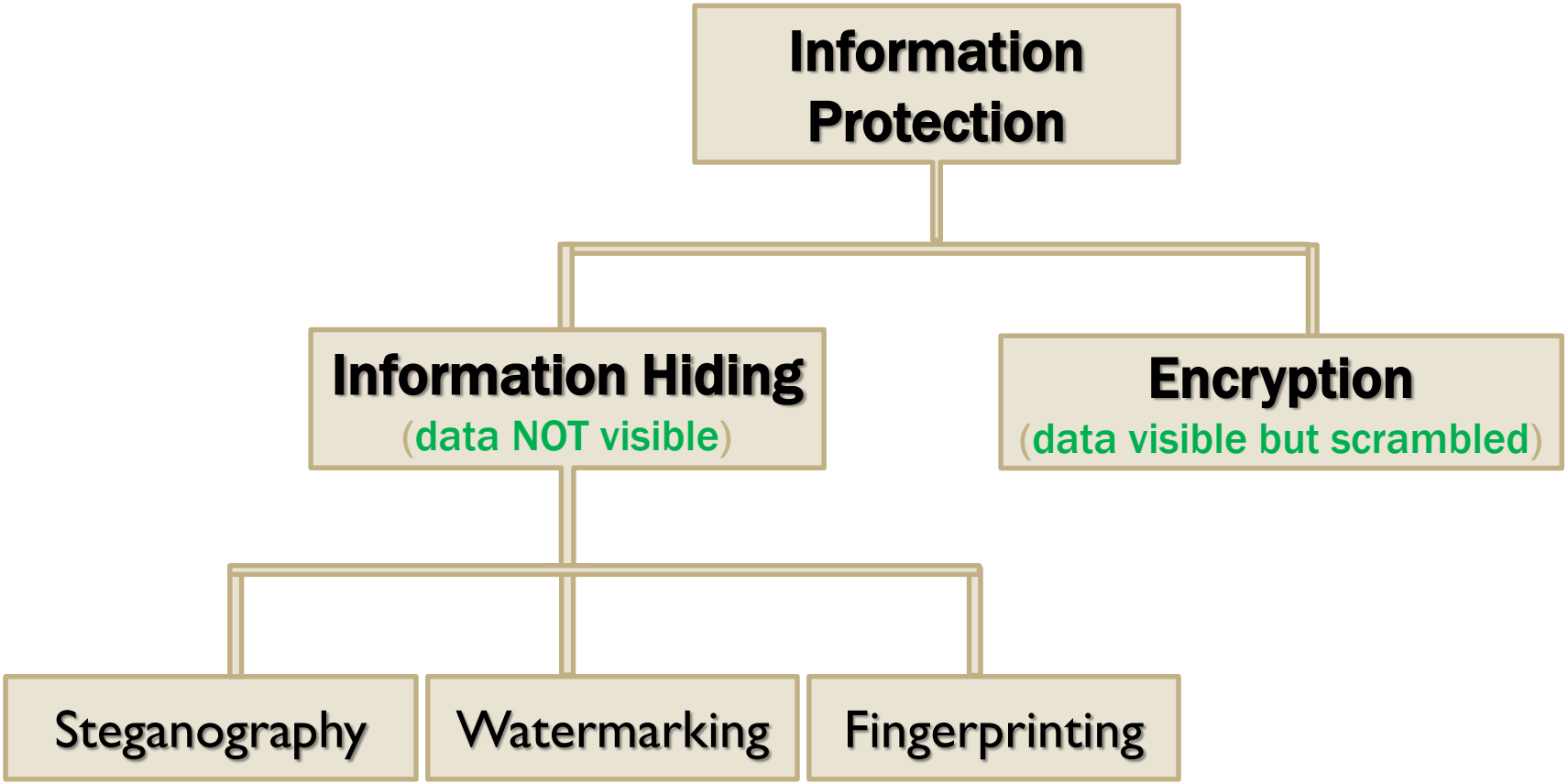
The images containing the code are located on public servers that are unlikely to be on any blacklist.

https://cisomag.eccouncil.org/hackers-using-steganography-to-target-industrial-enterprises-kaspersky/

https://arstechnica.com/information-technology/2020/05/an-advanced-and-unconventional-hack-is-targeting-industrial-firms/

Introduction (cont.)

- **Information Protection in Digital Age**



Introduction (cont.)

- **Techniques of Information Hiding**

  - **Steganography**
    - steganography - Greek word for "*concealed writing*"
    - art and science of hiding information in some cover media for the purpose of protecting information confidentiality
    - digital steganography – cover media: image, text, audio, video

  - **Watermarking**
    - also aims to make information invisible, but for the purpose of protection of intellectual property

  - **Fingerprinting**
    - embedding user-unique marking to different copies of content for the purpose of tracking of intellectual property

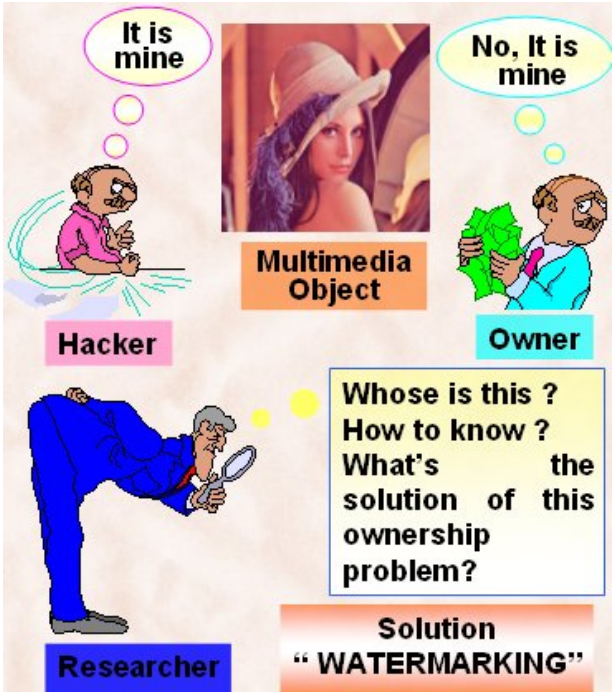
unauthorized users cannot find/read confidential info

unauthorized users cannot use or appropriate somebody's IP

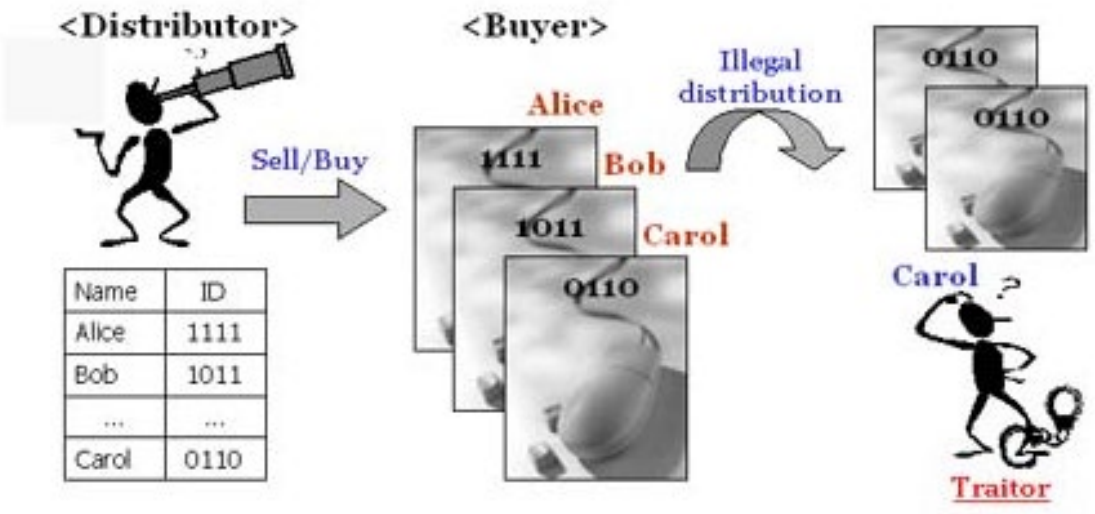
users can be tracked/identified

Introduction (cont.)

Example: Watermarking vs. Digital Fingerprinting



http://www.cse.unt.edu/~smohanty/Publications_Others/Mohanty_Masters_Thesis_Spring1999.html



http://itslab.inf.kyushu-u.ac.jp/research/fingerprint.html

The main difference between watermarking and fingerprinting is that the WM remains the same for all copies of the IP while the FP is unique for each copy. As such, FPs … enable tracking of IP misuse conducted by a specific user.

http://aceslab.org/sites/default/files/DeepMarks_ICMR.pdf

Information Hiding: Steganography

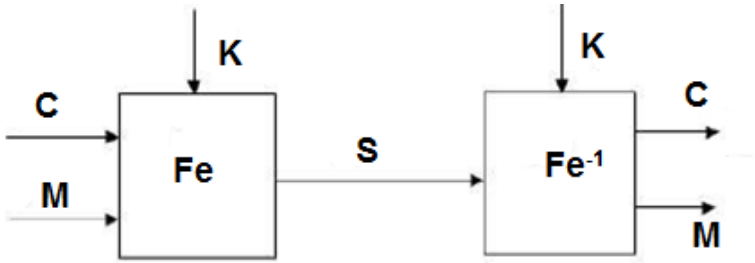
Classical Steganography

- **History of Steganography** – the need to protect information from unsolicited access, by making it obscure, precedes our digital age
  - in ancient Greece, a message would be tattooed on the shaved head of a messenger; the hair would be grown over
  - in era of printed press, different typefaces were used to 'encode' a message
  - in WW2, the French resistance used invisible ink (e.g., wax) to write messages on the back of regular currier

ahzemllyo

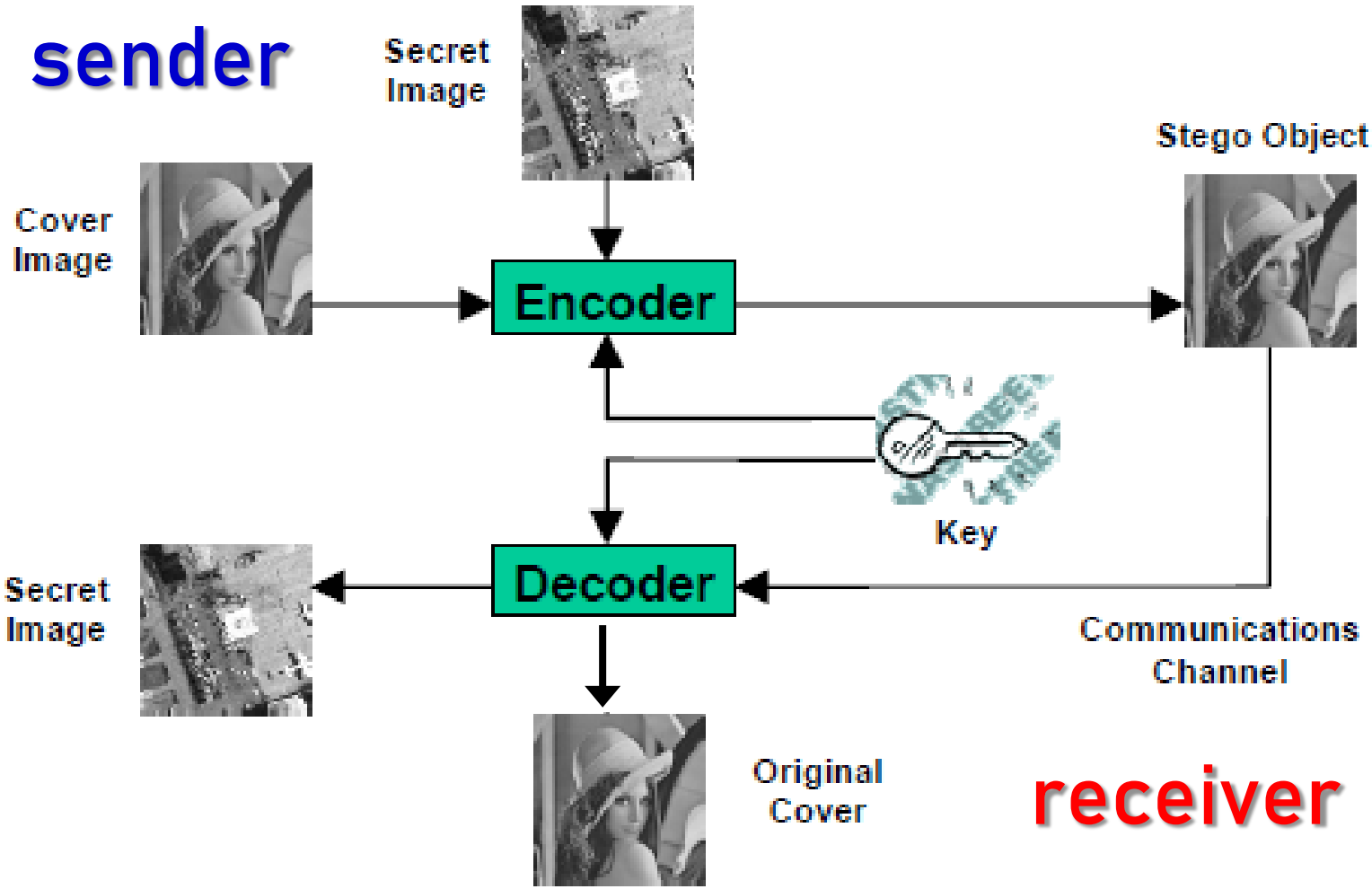
Digital Steganography

- **Digital Steganography**
  - process of hiding information in digital multimedia files and in network packets
  - elements of digital steganography system include
    - cover media (**C**) that will hold the hidden data
    - secret message (**M**) - may be plain text or any other type of data
    - stego function (**Fe**) and its inverse (Fe^{-1})
    - an optional stego-key (**K**) or password to hide and unhide the message
    - stego object (**S**) = cover media + secret message



Digital Steganography (cont.)

Example: Steganography of 'Image inside an Image'



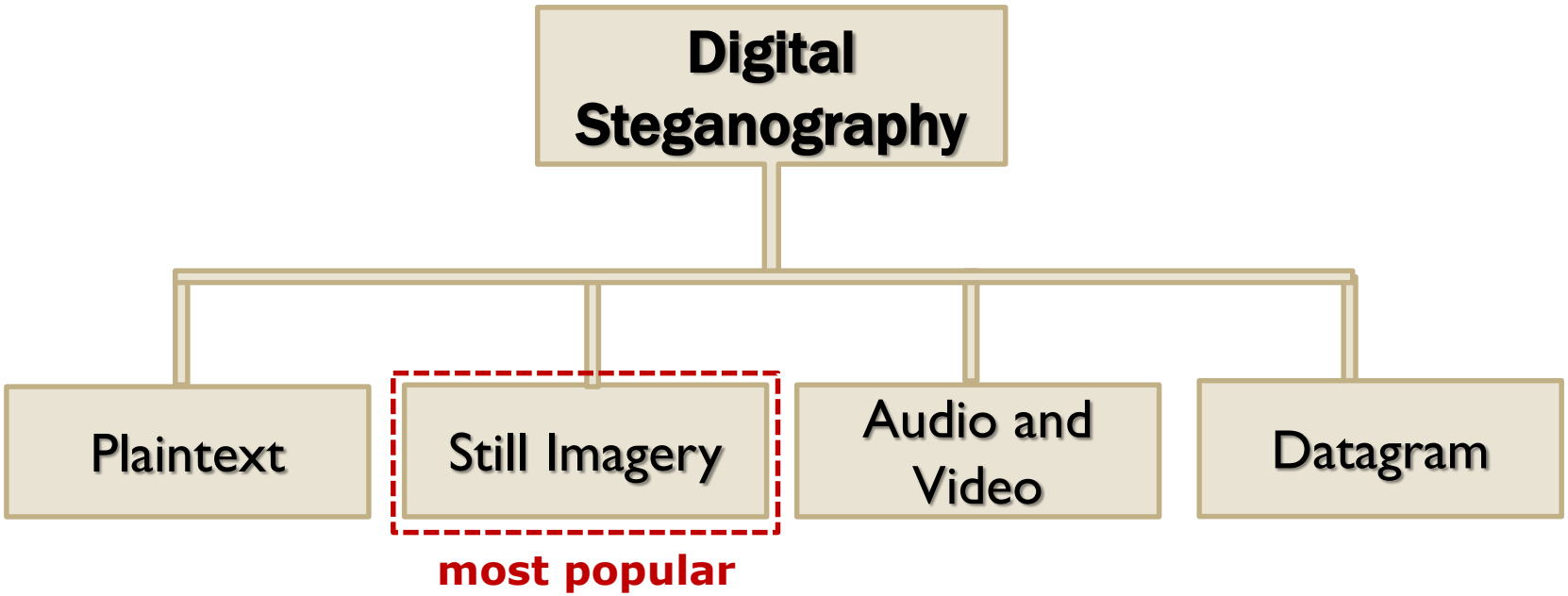
Digital Steganography (cont.)

- **What Makes Steganography Work?**

  - digital steganography takes advantage of
    1) space redundancy in cover media
    2) data redundancy in cover media in combination with inherent weaknesses of human perception
      - e.g., in computer/text file steganography, information can be hidden in unused areas of the file/text
      - e.g., in image steganography, information can be embedded in the Least Significant Bits (LSBs) of an image (introduced change is insignificant for human eye)
      - e.g., in audio steganography, information can be embedded in high frequencies of audio spectrum (human ear is insensitive to slight variations in high audio frequencies)

Digital Steganography (cont.)

- **Techniques of Digital Steganography**
  Based on Type of Cover Media



Plaintext Steganography

1.1) Plaintext Steganography: Use of Selected Characters in Cover Media

- sender sends
  1) text message / text file = stego object
  2) a series of integer number = key
- secret message is hidden within the respective positions of subsequent words in cover media

Example: Plaintext Steganography with Selected Characters

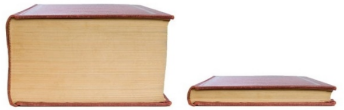
The weather is sunny and wonderful.
They have gone running at the beach.

2 2 1 1 2 2 1 1 4 1 0 0 2

character in each word (to extract)

He is not here.

Disadvantage?!



Plaintext Steganography (cont.)

1.2) Plaintext Steganography:

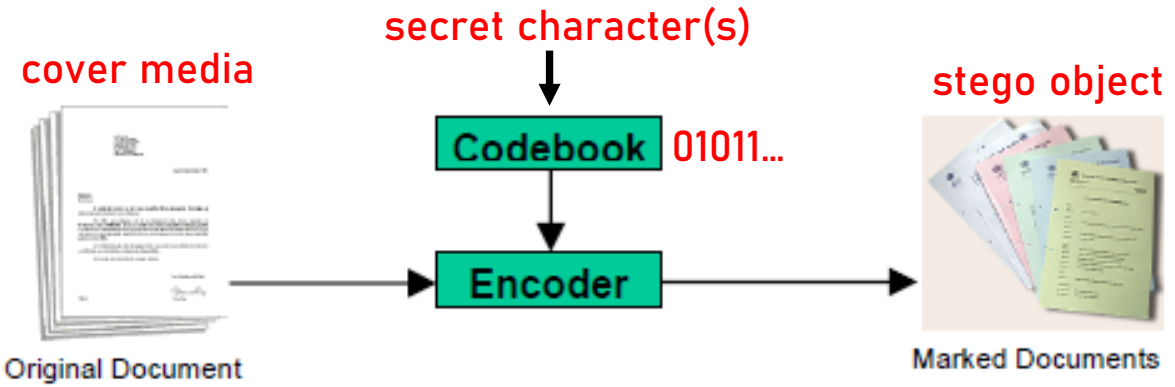
used to hide binary 0 and 1, not letters !

Line Shifting or Word Shifting in Cover Media

- e.g., lines are shifted down by a small fraction
  - shift present = 1, shift not present = 0
- e.g., words are shifted right by a small fraction
  - shift present = 1, shift not present = 0
- encoded bits are extracted and compared against a predefined **Codebook**

Codebook:

00000 – a	10010 – n
00001 – b	10011 – o
00010 – c	10100 – p
00011 – d	10101 – q
00100 – e	10110 – r
00101 – f	10111 – s
00111 – g	11000 – t
01000 – h	11001 – u
01001 – i	11010 – v
01011 – j	11011 – w
01111 – k	11100 – x
10000 – l	11101 – y
10001 – m	11110 – z



https://www.cs.bham.ac.uk/~mdr/teaching/modules03/security/students/SS5/Steganography.htm

Recipient's perspective!!! (message extraction)

Example: Steganography with Line Shifting

IF you can keep your head when all about you
Are losing theirs and blaming it on you,

If you can trust yourself when all men doubt you,
But make allowance for their doubting too;
If you can wait and not be tired by waiting,
Or being lied about, don't deal in lies,
Or being hated, don't give way to hating,
And yet don't look too good, nor talk too wise:

If you can dream - and not make dreams your master;
If you can think - and not make thoughts your aim;
If you can meet with Triumph and Disaster

And treat those two impostors just the same;
If you can bear to hear the truth you've spoken
Twisted by knaves to make a trap for fools,
Or watch the things you gave your life to, broken,
And stoop and build 'em up with worn-out tools:

If you can make one heap of all your winnings
And risk it on one turn of pitch-and-toss,
And lose, and start again at your beginnings
And never breathe a word about your loss;
If you can force your heart and nerve and sinew

To serve your turn long after they are gone,
And so hold on when there is nothing in you
Except the Will which says to them: 'Hold on!'

If you can talk with crowds and keep your virtue,

Or walk with Kings - nor lose the common touch,
If neither foes nor loving friends can hurt you,
If all men count with you, but none too much;
If you can fill the unforgiving minute
With sixty seconds' worth of distance run,
Yours is the Earth and everything that's in it,
And - which is more - you'll be a Man, my son!

extract

Codebook:

00000 – a	10010 – n
00001 – b	10011 – o
00010 – c	10100 – p
00011 – d	10101 – q
00100 – e	10110 – r
00101 – f	10111 – s
00111 – g	11000 – t
01000 – h	11001 – u
01001 – i	11010 – v
01011 – j	11011 – w
01111 – k	11100 – x
10000 – l	11101 – y
10001 – m	11110 – z

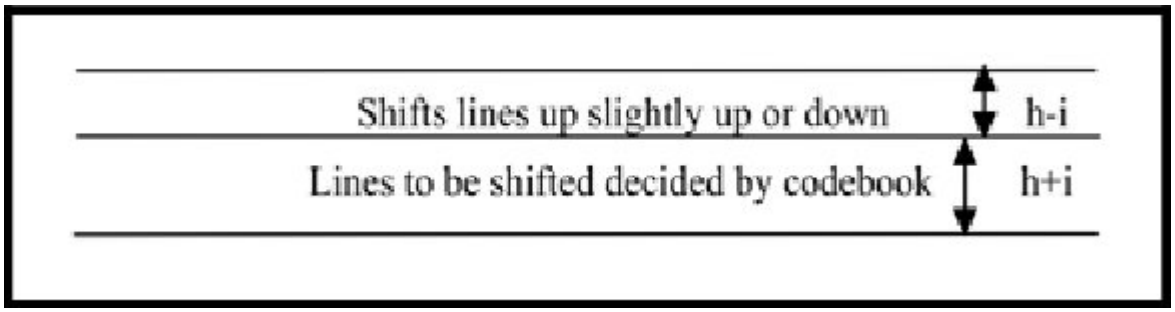
01000
00100
10000
10000
10011

decode

hello

Plaintext Steganography (cont.)

Example: More Subtle Forms of Line and Word Shifting



Text placed at the bottom vs. at the center of a row.

a)

Now	is	the	time	for	all	men/women	to ...
Now	is	the	time	for	all	men/women	to ...

b)

Now is the time for all men/women to ...

Now is the time for all men/women to ...

https://www.researchgate.net/publication/228672143_WhiteSteg_A_new_scheme_in_information_hiding_using_text_steganography/figures?lo=1

https://www.researchgate.net/publication/228672143_WhiteSteg_A_new_scheme_in_information_hiding_using_text_steganography/figures?lo=1

Image Steganography

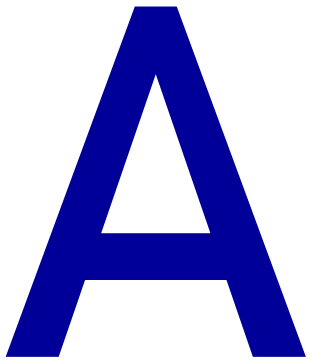
In each point, there could be an infinite number of possible color shades.
No two (adjacent) points could be of the same color.

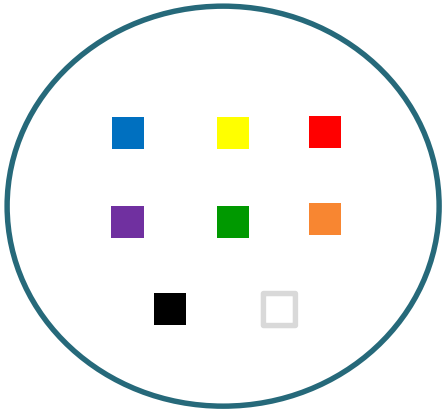
Image Steganography

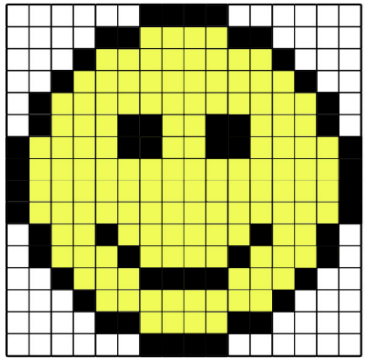
Image is broken into a finite number of areas that contain the same color/shade. There is finite number of colors/shades available.

Example: Digitized Image

- any image can be digitized – i.e., represented by a discrete (finite) set of display elements holding same-color content







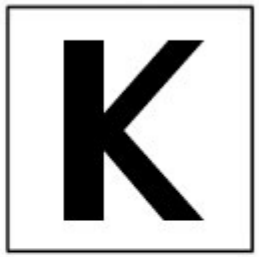
How can we improve the quality of digital images?

By decreasing the size of display elements (increase resolution).

96ppi

192ppi

384ppi



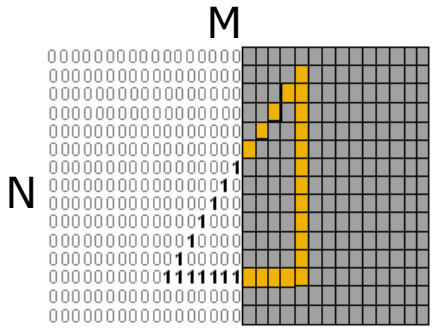
Phones with best screens 2018

Mobile Phone Name	Screen Size	Pixel Size	Aspect Ratio	Ppi
iPhone-8	4.7 inch	1334x750	16 by 9	326
iPhone-8 Plus	5.5 inch	1920x1080	16 by 9	401
iPhone-X	5.8 inch	2436x1125	16 by 9	458
Samsung Galaxy S8	5.8 inch	2960x1440	18.5 by 9	572
Samsung Galaxy S8 Plus	6.2 inch	2960x1440	18.5 by 9	529
Samsung Galaxy Note-8	6.3 inch	2960x1440	18.5 by 9	521
Google Pixel 2	5 inch	1920x1080	16 by 9	441
Google Pixel 2 Plus	6 inch	2560x1440	16 by 9	538
Sony Xperia XZ Premium	5.5 inch	3840x2160	16 by 9	801

https://www.phoneppi.com/screen-resolution-and-ppi-of-mobile-phones.php

Image Steganography (cont.)

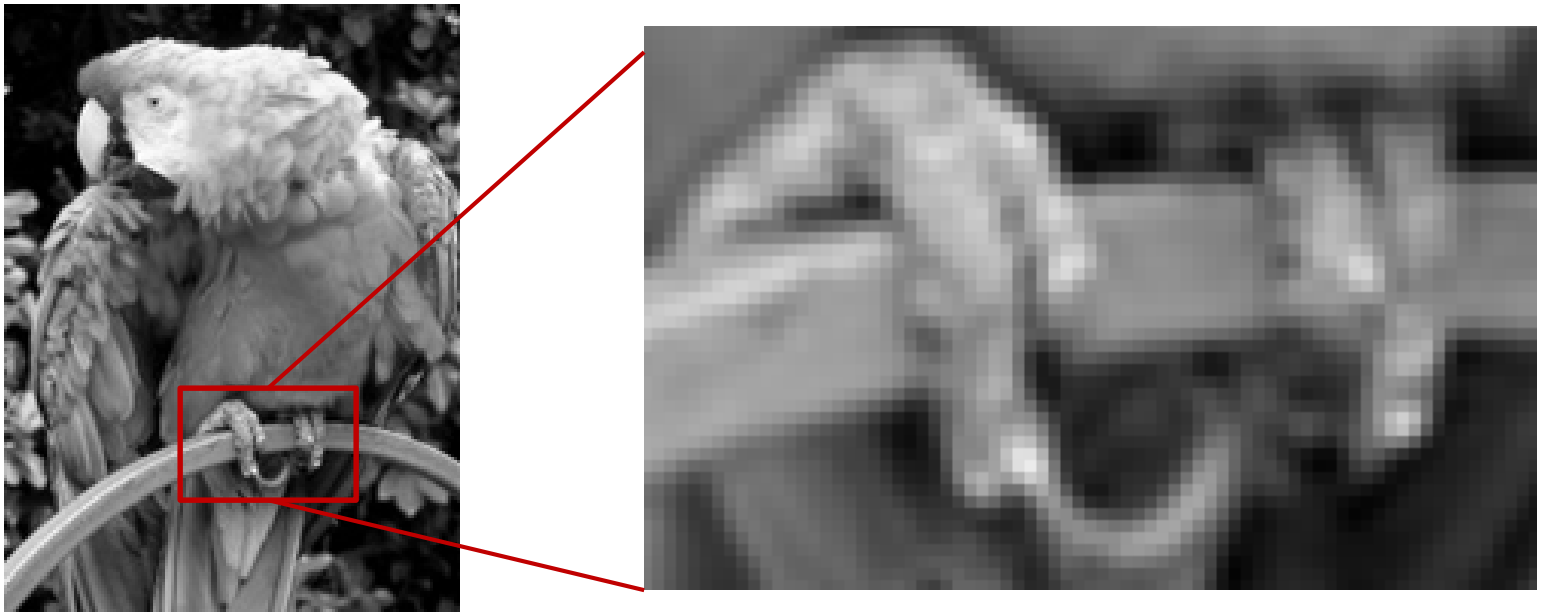
- **Digital Image** – a 2D (NxM) array/grid of m-bit pixels



- **Pixel** – fundamental same-color display element in a digital image
  - each pixel is made up of one or more bits
    - monochrome image: pixel = 1 bit => (black/white)
    - grayscale image: pixel = 8 bits => 256 shades of gray
    - RGB image: pixel = 24 bits => 8 bits for each – red, green, blue => **16777216** different color shades

Image Steganography (cont.)

Example: Pixels in Grayscale Image



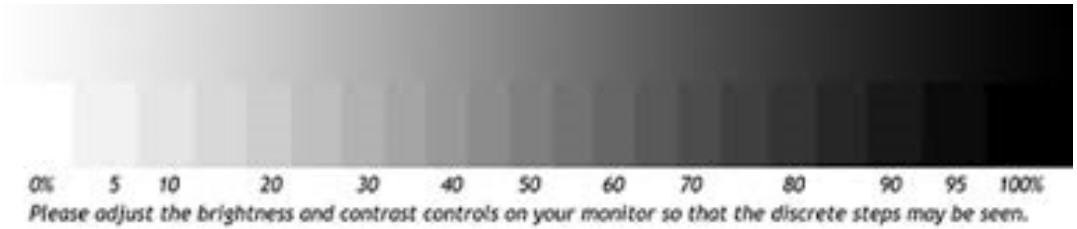
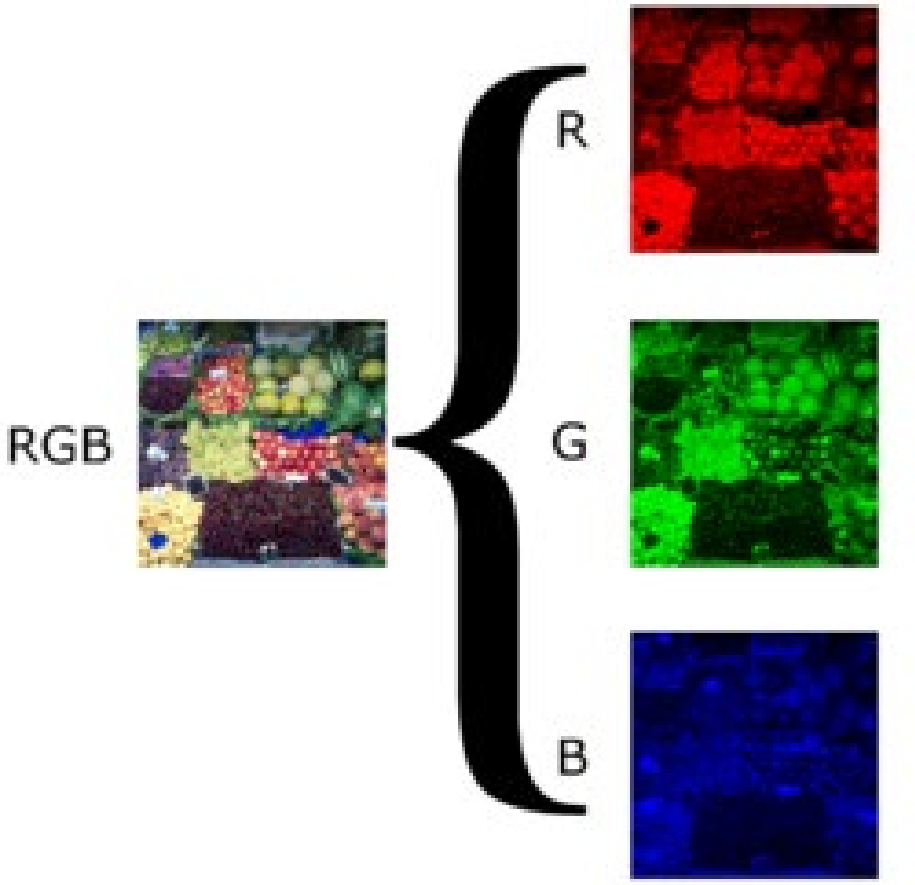


Image Steganography (cont.)

Example: RGB Image



http://www.freeonlinephotoeditor.com/

Image Steganography (cont.)

Example: Image Size

What is the size (in kbytes and KBytes) of a grayscale image comprising 200x300 pixels?

200 x 300 x 8 = 480,000 bits
= 60,000 bytes
= 60 kbytes
= 58.59 KBytes

kbyte = 10^3 bytes = 1000 bytes
KByte = 2^{10} bytes = 1024 bytes

http://jan.ucc.nau.edu/lrm22/pixels2bytes/calculator.htm

Image Steganography (cont.)

- **Bits in a Pixel** – relative importance of different pixels is different
  - LSB – least significant bit – last bit
  - MSB – most significant bit – 1st bit

(a) Original image

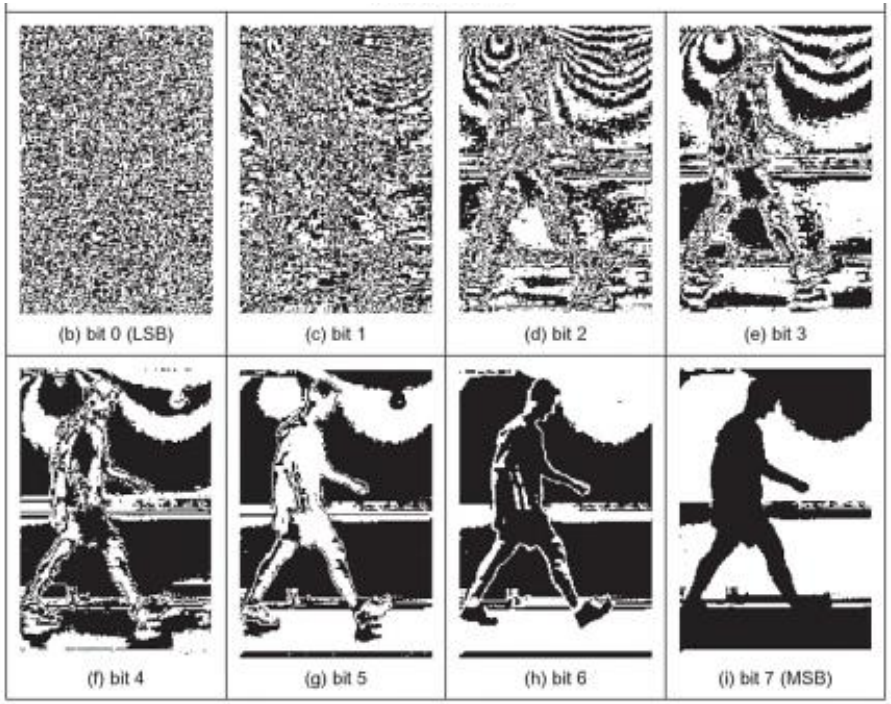
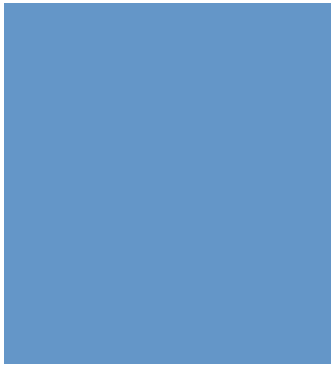


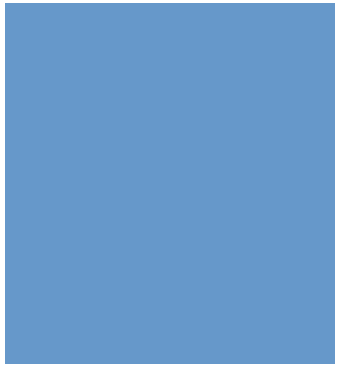
FIGURE 2.1
Decomposing an image into its bits.

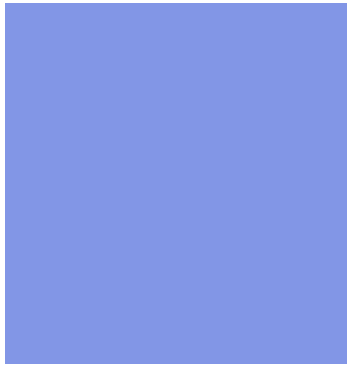
- LSB carries the least information – it changes most rapidly
- MSB carries the most information – it changes least rapidly

Image Steganography (cont.)

Example: LSB(s) and Human Eye







$R = 100_{10} = 01100100$
$G = 150_{10} = 10010110$
$B = 200_{10} = 11001000$

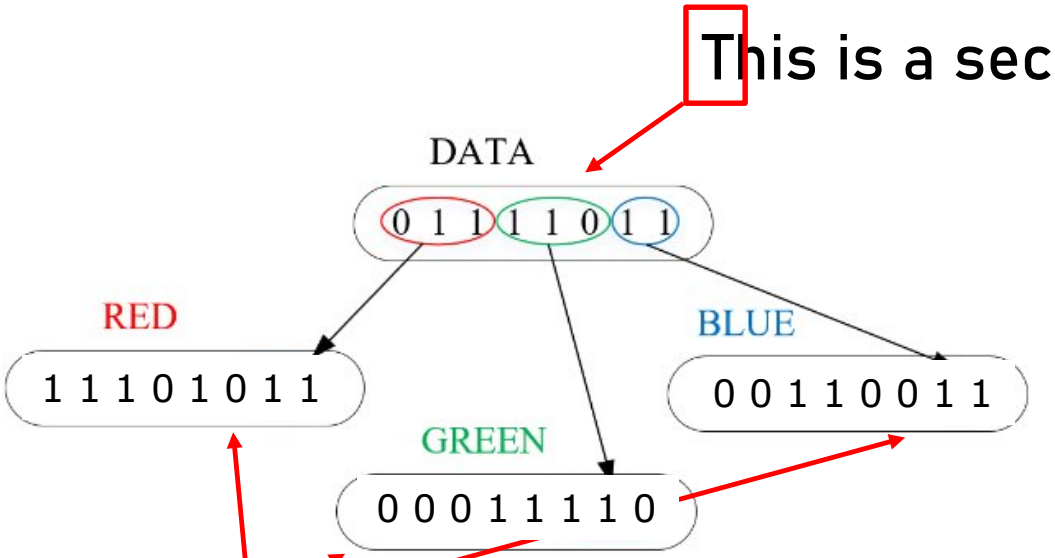
$R = 102_{10} = 01100110$
$G = 152_{10} = 10011000$
$B = 202_{10} = 11001010$

$R = 130_{10} = 01111000$
$G = 150_{10} = 10010110$
$B = 230_{10} = 11100110$

http://jumk.de/color-calculator/

Image Steganography (cont.)

Example: '**text in image**' using LSB



cover image

https://www.researchgate.net/publication/321183782_FPGA_implementation_of_LSB-based_steganography/figures?lo=1

Image Steganography (cont.)

2.1) Image Steganography: Use of LSB to hide 'image in image'

- easiest and surprisingly effective way of hiding information in an image
- LSB(s) of each pixel in cover object/image are used to hide the most significant bits of another image
- algorithm:

  (1) load up host image and image to hide

  (2) choose the number of LSBs you whish to hide the secret image in

  more bits used { => better quality of hidden image ☺
  => more distortion in cover image ☹

  (3) to get original image back, pick out the LSBs according to the number used in (2)

Image Steganography

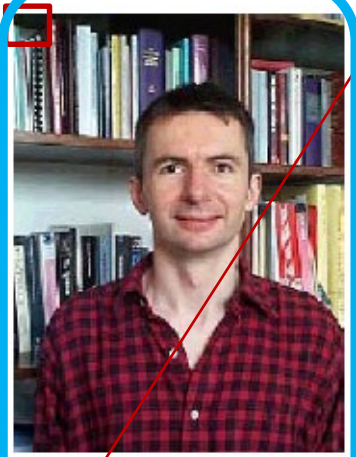
Cover and secret image of the same size (# of pixels).
One secret pixel has to be 'encoded' in one cover pixel.

Example: 'image in image' using LSB

Number of LSB used = 4

Cover

Secret



Stego Image

Recovered Image

Encoding:

Host Pixel: 10110001
Secret Pixel: 00111111
New Image Pixel: **10110011**

Decoding:

Host Pixel: 10110011
Bits used: 4
New Image: **00110000**

Image Steganography (cont.)

Example: 'image in image' using LSB

Number of LSB used = 1

Cover

Secret

Stego Image

Recovered Image

fewer LSB bits used => 'hiding' capacity low –
better stego-image ☺
worse recovered image ☹

Image Steganography (cont.)

Example: 'image in image' using LSB

Number of LSB used = 7

Cover

Secret

Stego Image

Recovered Image

more LSB bits used => 'hiding' capacity high –
worse stego-image ☹
better recovered-image ☺

Image Steganography (cont.)

What if we do not need all the pixels of the cover image to hide our secret message??

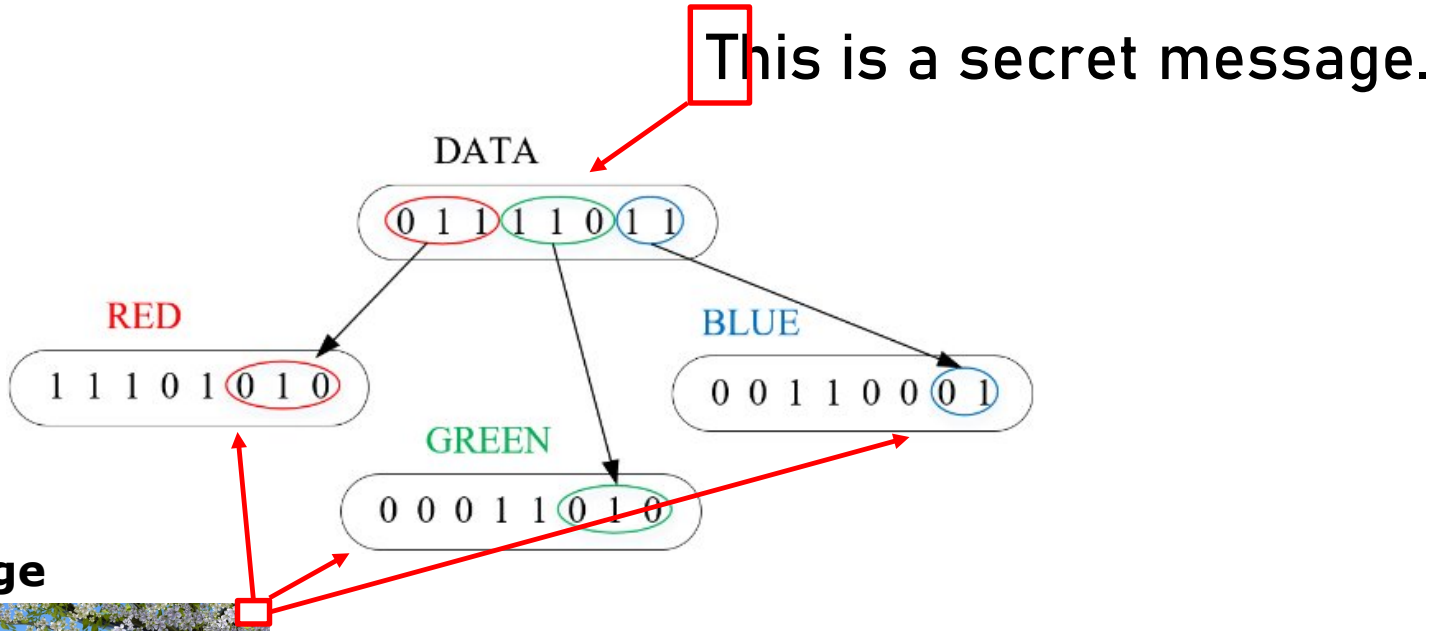
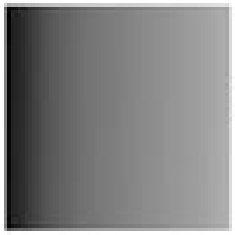
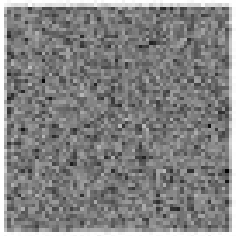


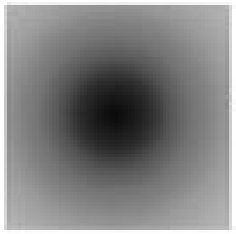
Image Steganography (cont.)

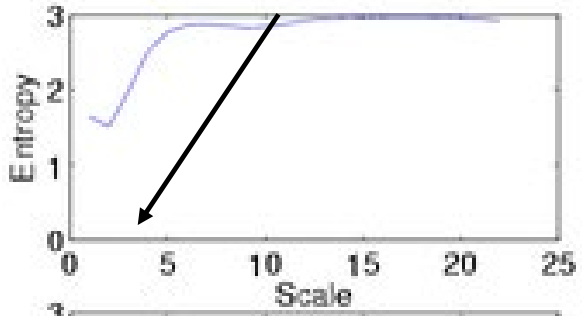
given a specific pixel, how similar are the 'color values' n-pixels away

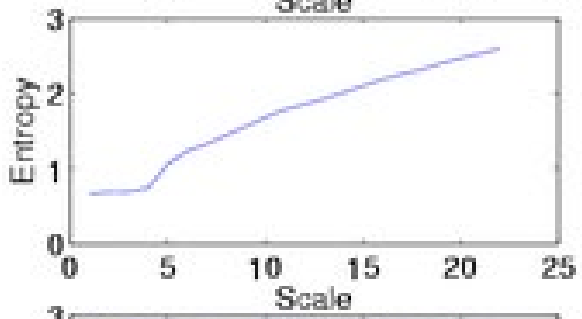
The entropy of local attributes measures the (un)predictability of a region with respect to an assumed model of simplicity.

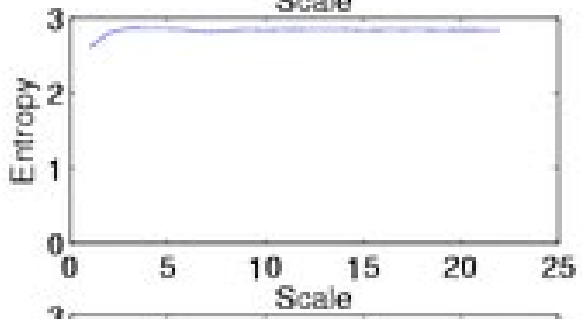


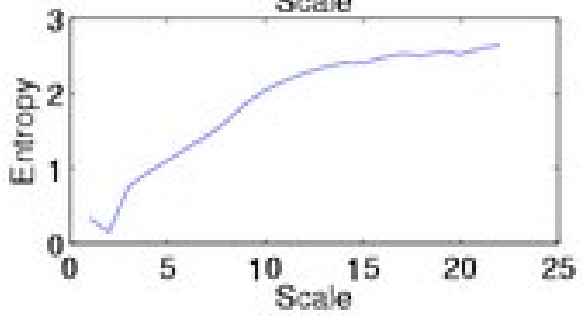








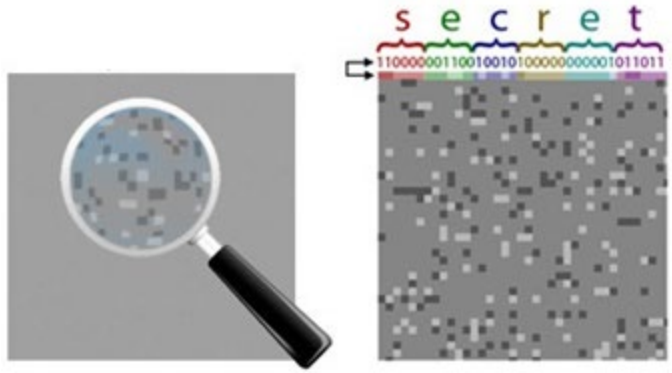




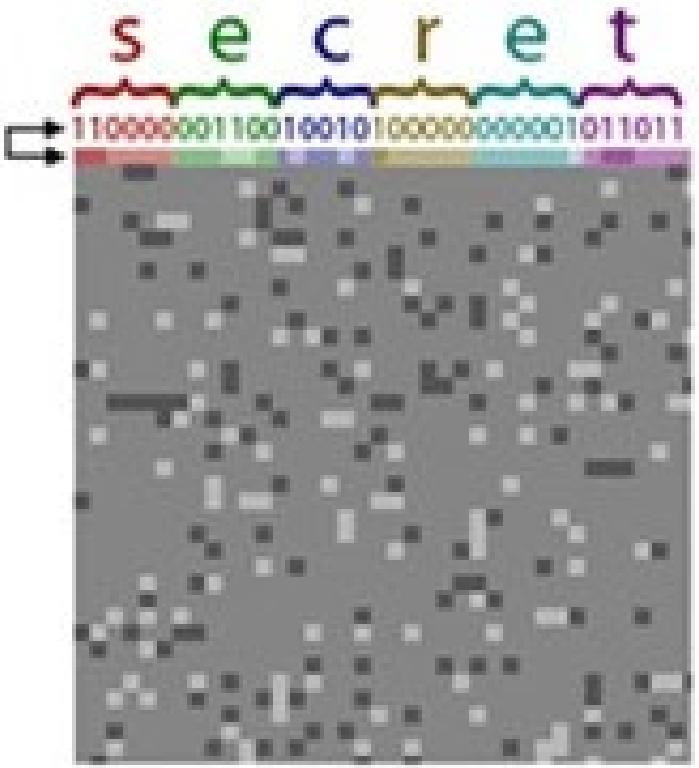
https://www.robots.ox.ac.uk/~timork/Saliency/background.html

Image Steganography (cont.)

- **Pattern of LSB Embedding** – secret bits can be embedded in LSBs of cover image in two ways:
  - sequentially
    - ➢ simple embedding & extraction of secret bits ☺
    - ➢ statistics of cover image abruptly changed - easy to detect ☹
  - randomly
    - ➢ the key to generate pseudorandom numbers must be sent ☹
    - ➢ secret bits scattered throughout cover image - hard to detect ☺



Is ‘random’ choice of pixels an ideal approach to information hiding in an image ???



Should not ‘mess up’ pixel values in areas of ‘low entropy’.

What is a better place to hide secret bits:

- same-color background
- part of image with lots of detail ???

Image Steganography (cont.)

2.2) Image Steganography: Use of Discrete Cosine Transform (DCT)

- DCT is one of key components of JPEG compression
- JPEG algorithm:

  (1) algorithm is split in 8x8 pixel squares

  (2) each square is transformed via DCT to 64 frequency components

  (3) each DCT coefficient is quantized against a reference table – many bits get removed

  - more bits are used for low-freq. and fewer for high-freq. components
    (human eye is more sensitive to low-freq. info)

  (4) many coefficients are (now) close in value => run/variable length coding can be used

Image Steganography (cont.)

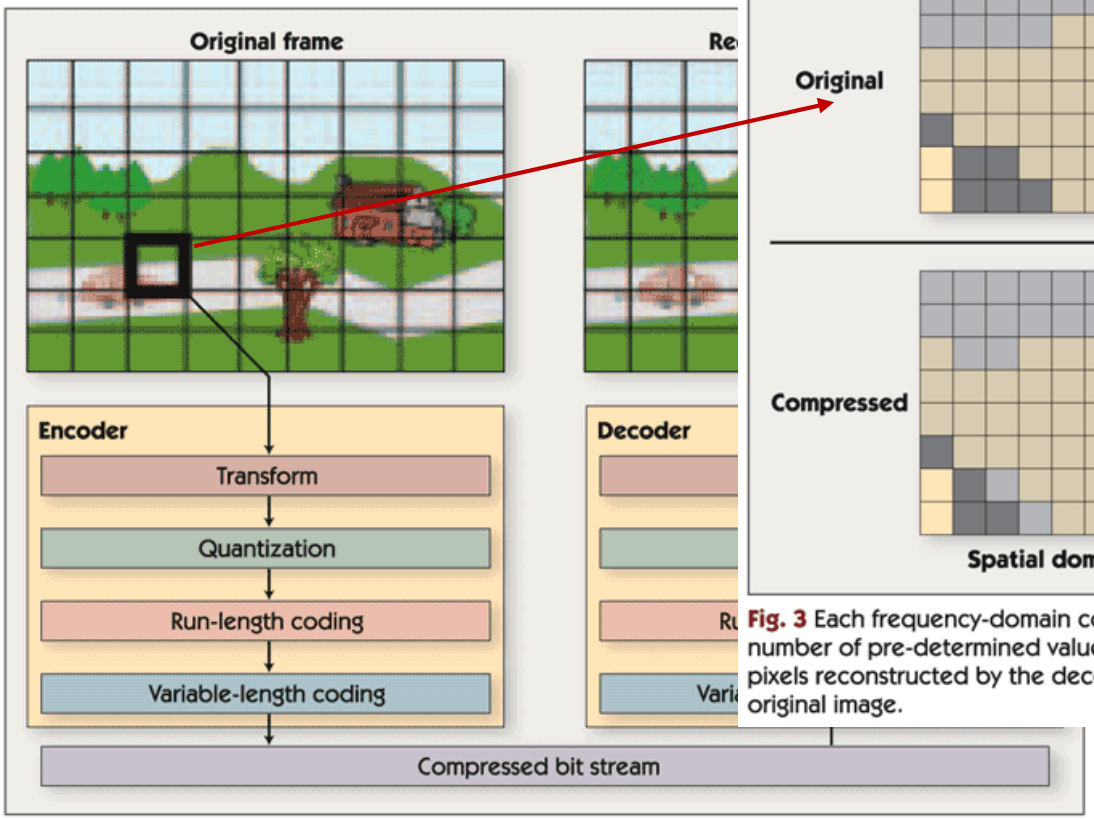


Fig. 1 Still image compression begins by dividing the image into 8-pixel by 8-pixel blocks. The main processing steps that follow are transformation to the frequency domain, quantization of the frequency domain coefficients, run-length coding of the coefficients, and variable-length coding. Still image decompression reverses these steps: variable-length decoding, run-length decoding, and dequantization restore the frequency domain coefficients (with some quantization error) and an inverse transform reconstructs the pixels in each image block from those coefficients.

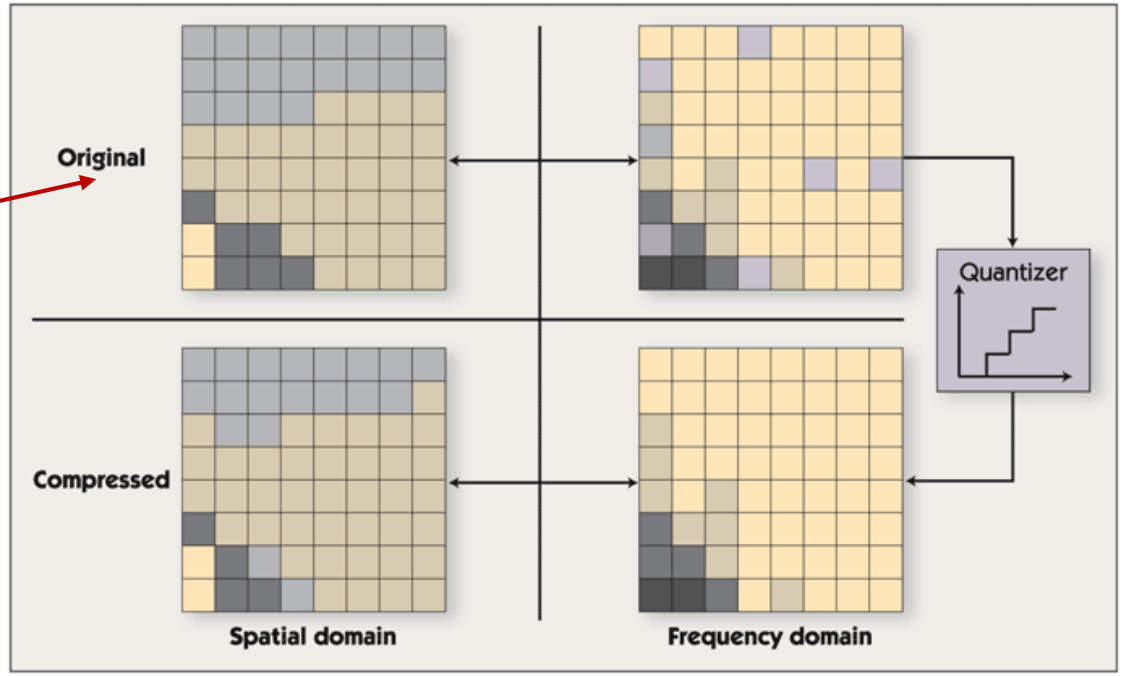


Fig. 3 Each frequency-domain coefficient is quantized in the encoder by rounding to the nearest of a number of pre-determined values. Because this rounding discards some information, the 8x8 block of pixels reconstructed by the decoder is close—but not identical—to the corresponding block in the original image.

http://www.eetimes.com/document.asp?doc_id=1275437

Image Steganography (cont.)

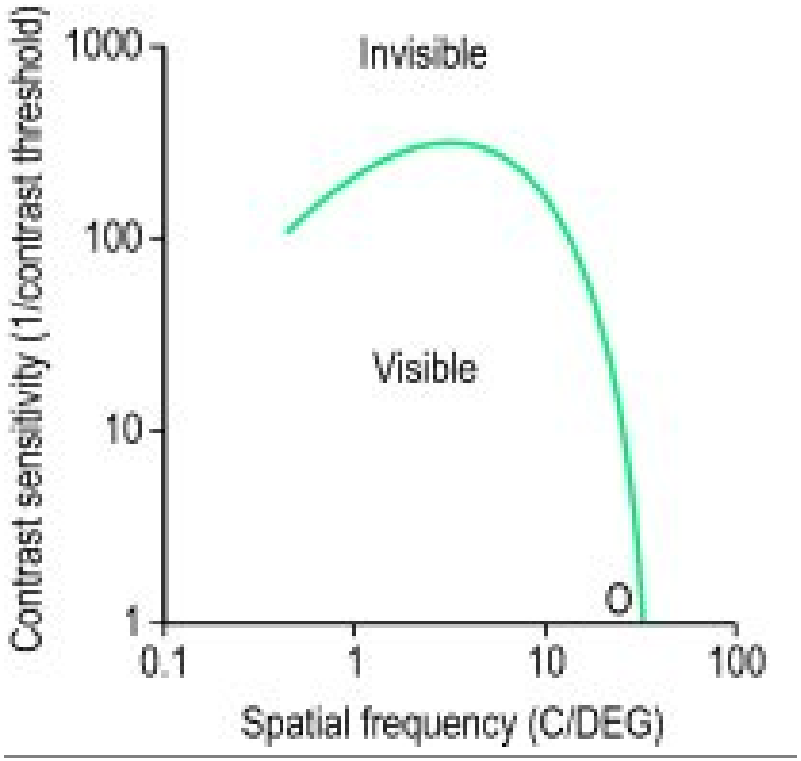
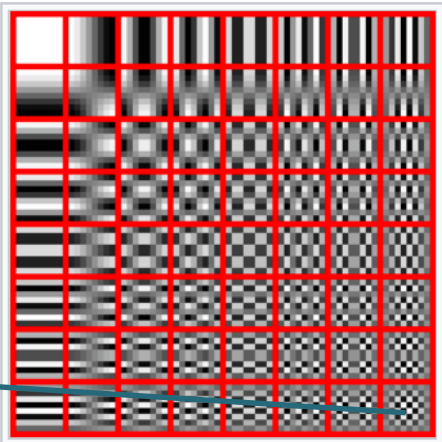


Fig. F10 Typical contrast sensitivity function of an adult human eye (O, cut-off frequency) (both scales are logarithmic)

http://medical-dictionary.thefreedictionary.com/Function+(disambiguation)

Low Frequency (intensity)

High Frequency (intensity)



The DCT transforms an 8×8 block of input values to a linear combination of these 64 patterns. The patterns are referred to as the two-dimensional DCT *basis functions*, and the output values are referred to as *transform coefficients*. The horizontal index is u and the vertical index is v.

a. Original image

b. With 10:1 compression

c. With 45:1 compression

FIGURE 27-15
Example of JPEG distortion. Figure (a) shows the original image, while (b) and (c) shows restored images using compression ratios of 10:1 and 45:1, respectively. The high compression ratio used in (c) results in each 8×8 pixel group being represented by less than 12 bits.

https://www.dspguide.com/ch27/6.htm

https://www.mathworks.com/help/images/jpeg-image-deblocking-using-deep-learning.html

Image Steganography (cont.)

2.2) Image Steganography: Use of Discrete Cosine Transform (DCT) - cont.

- Possible Approaches to Hiding Data in DCT

  (A) hide secret data in LSBs of selected or non-significant DCT coefficients (high. frequencies)

  (B) hide secret data in LSBs of DCT coefficients

  (C) hide one bit of data in each 8x8 block of DCT:
  0 => all coefficients even
  1 => all coefficients odd

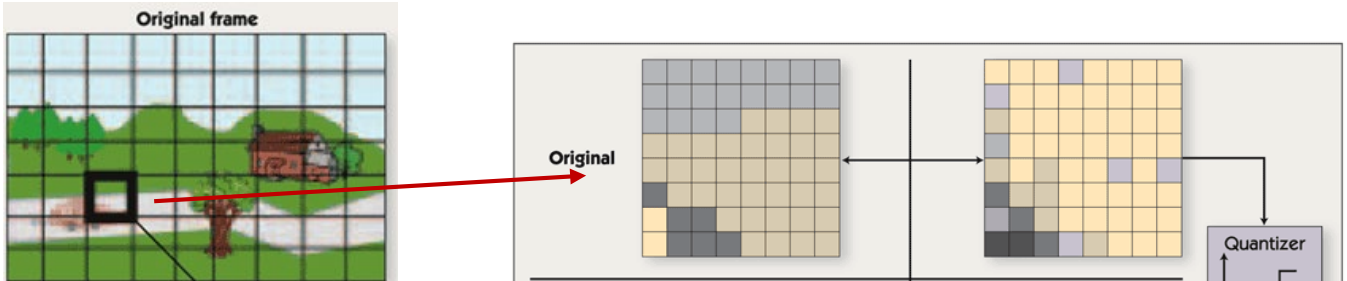
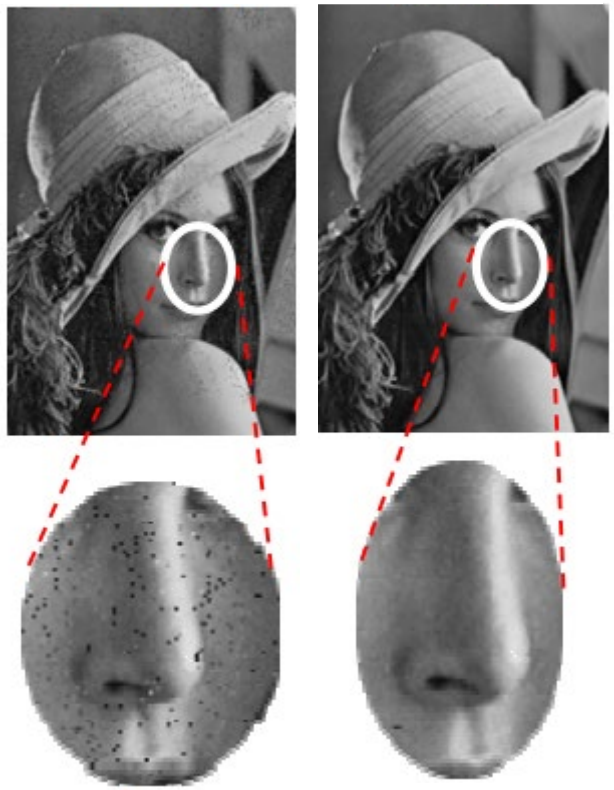


Image Steganography (cont.)

Example: Comparison of Spatial (LSB) vs. DCT Based Steganography

Method	Descriptions
Spatial domain techniques	▪ Large payload but often offset the statistical properties of the image ▪ Not robust against lossy compression and image filters ▪ Not robust against rotation, cropping and translation ▪ Not robust against noise ▪ Many work only on the BMP format
DCT based domain techniques	▪ Less prone to attacks than the former methods at the expense of capacity ▪ Breach of second order statistics ▪ Breach of DCT coefficients distribution ▪ Work only on the JPEG format ▪ Double compression of the file ▪ Not robust against rotation, cropping and translation ▪ Not robust against noise ▪ Modification of quantization table



http://www.abbascheddad.net/Survey.pdf

Image Steganography (cont.)

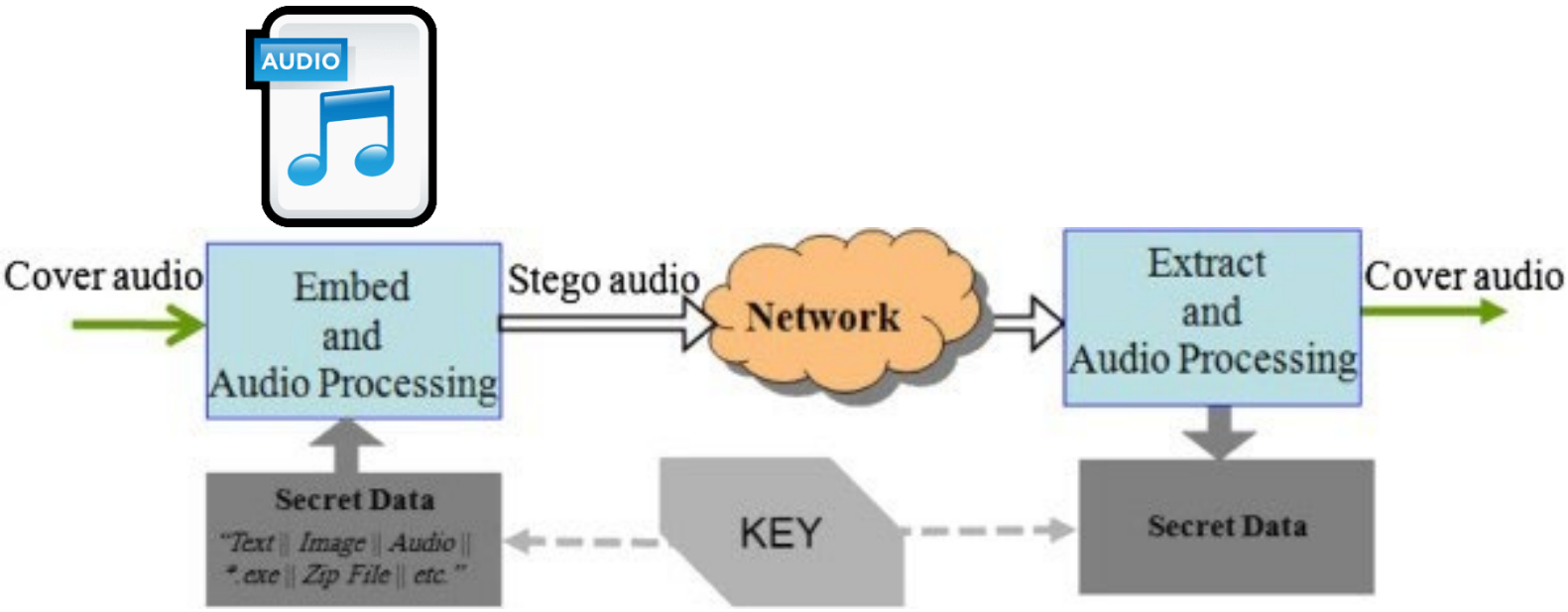
Example: Comparison of Different Tools for Image Steganography

Name	Creator	Year	Spatial domain	Frequency domain	Image format	Encryption support	Detected by
S-Tools	Andrew Brown	1996	✓	×	BMP,		
Outguess version 0.13b	Provos and Honeyman	1999	×	✓ DCT	JPE		
Outguess version 0.2	Provos and Honeyman	2001	×	✓ DCT	JPE		
F5	Andreas Westfeld	2001	×	✓ DCT	JPEG, B		
JPEG-JSteg	Derek Upham	2002	×	✓ DCT	JPE		
StegJasper	Su and Kuo	2003	×	✓ DWT	JPEG		method
MB	Phil Sallee	2003	×	✓ DCT	JPEG	-	First-order statistics
Info Stego	Antiy labs	2006	-	-	JPEG, BMP, GIF	✓	-
YASS	Kaushal Solanki	2007	×	✓ DCT	JPEG	-	Bin Li's method
StegMark	DataMark technologies	2007	×	✓	JPEG, BMP, GIF	-	-
Steganoflage	Abbas Cheddad	2009	×	✓ DWT	JPEG, BMP, GIF, PNG	✓ 2D SHA-2	-

S.No	Name of Image Steganography Tool	Format
1	Blind slide	BMP
2	Camera Shy	JPEG
3	Hide4PGP	BMP
4	JP Hide and Seek	JPEG
5	Jsteg Jpeg	JPEG
6	Mandelsteg	GIF
7	Steghide	BMP
8	wbStego	BMP

https://www.semanticscholar.org/paper/Stego-Image-Generator-(SIG)-Building-Steganography-Thiyagarajan-Aghila/05bbe26098eb27be54a0fa9993f671105e84cbf3

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

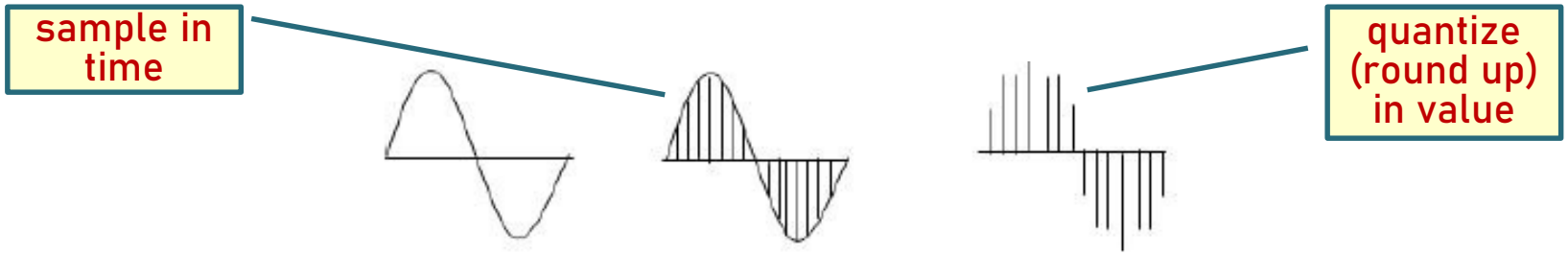
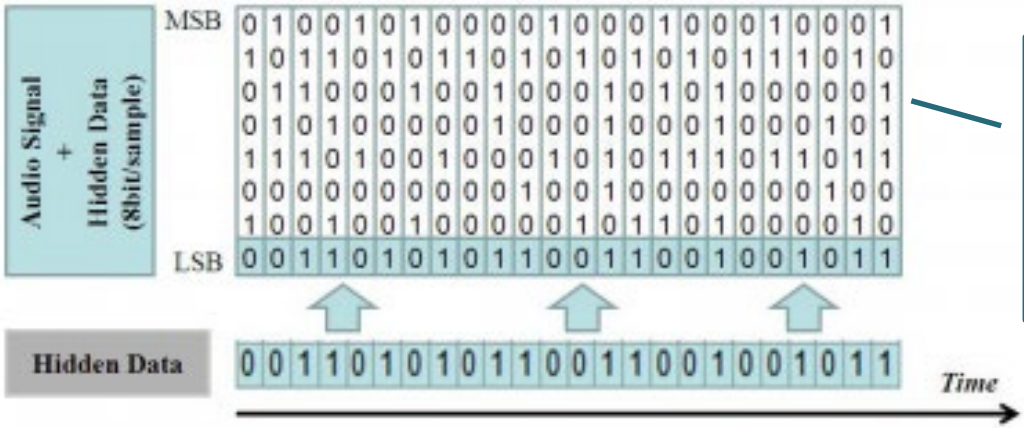
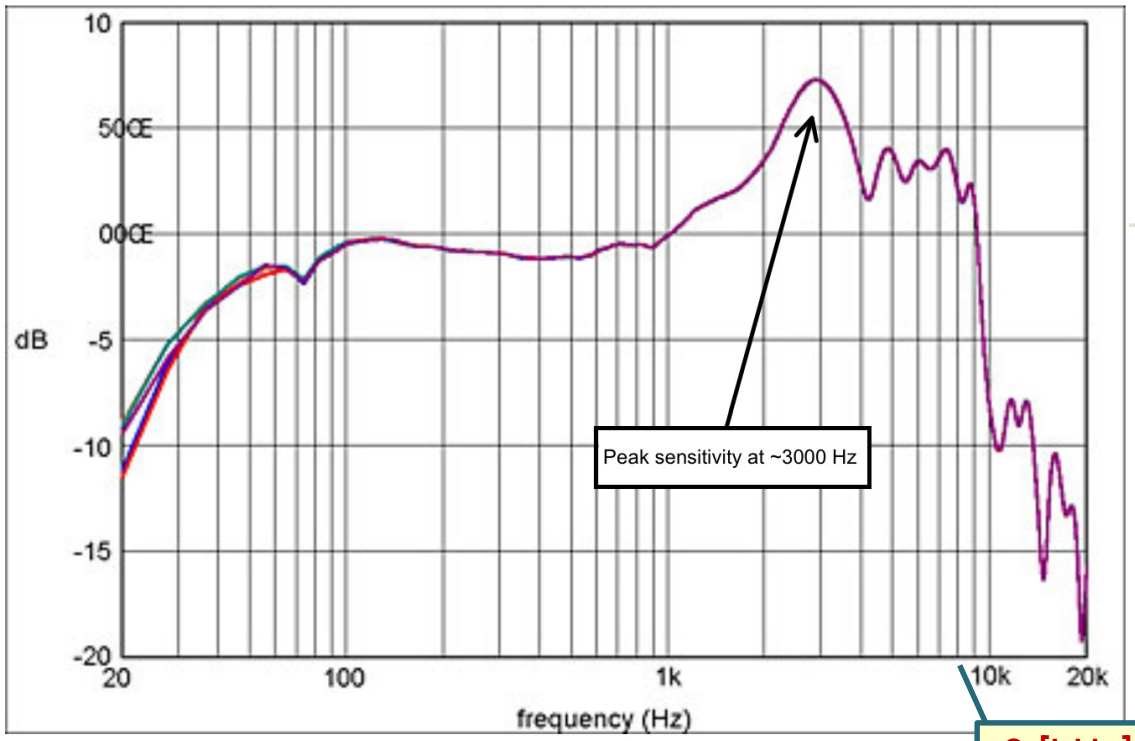


Figure 3: Sampling of the Sine Wave followed by Quantization process.

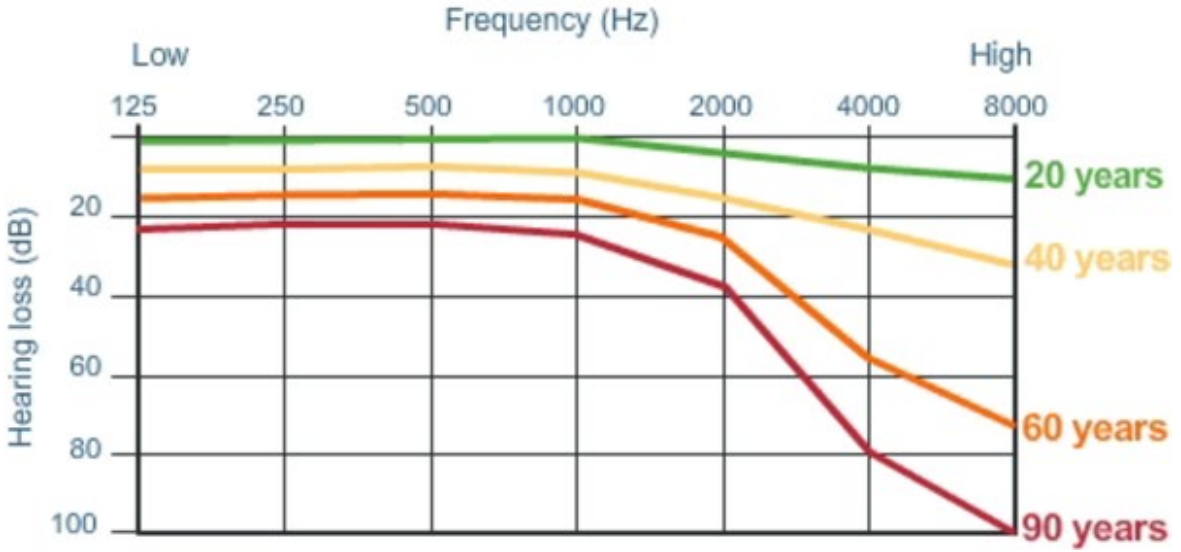




sensitivity of a normal human ear to different frequencies

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

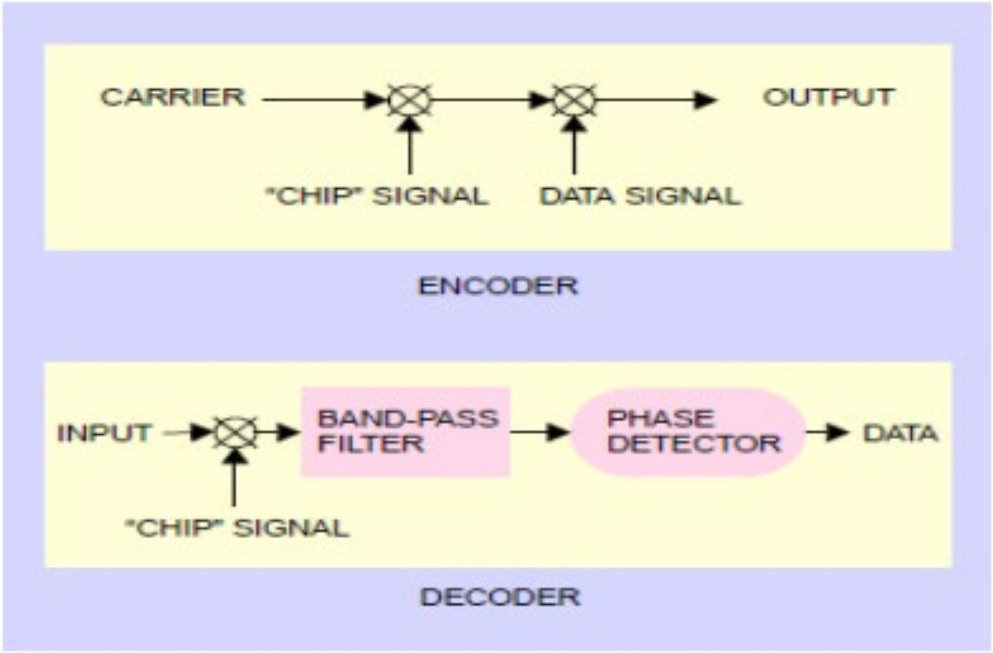
sensitivity of a human ear by age



Audio Steganography (cont.)

3.2) Audio Steganography: Spread Spectrum

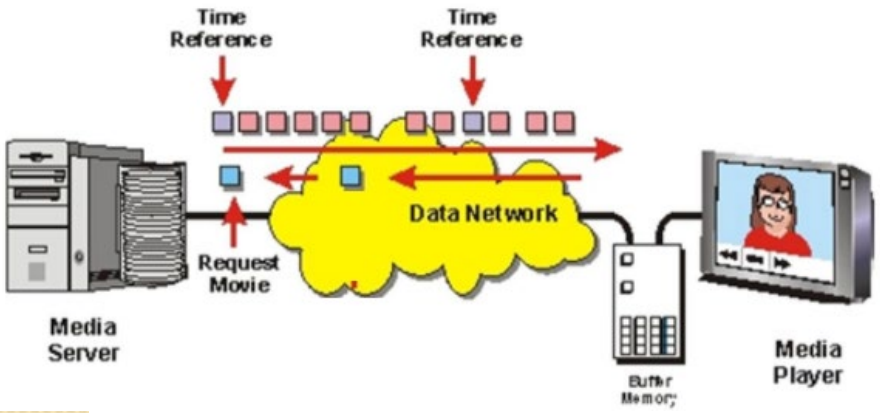
- secret bit is spread across cover audio in form of high-frequency noise

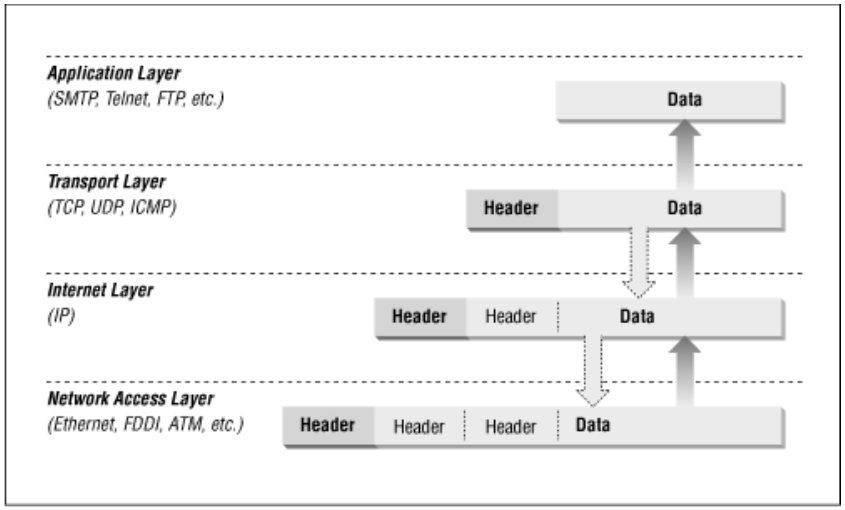


http://www.sersc.org/journals/IJDTA/vol2_no2/1.pdf

Datagram Steganography

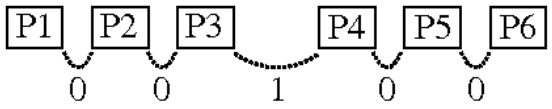
Datagram / Packet / Network Steganography



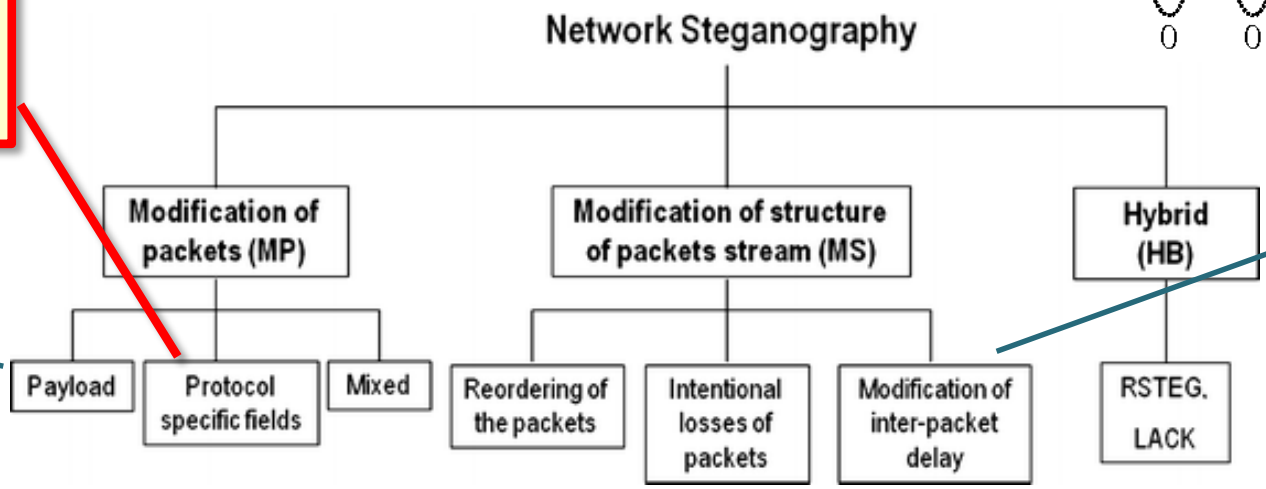


(e.g.) place secret bits into packet header(s)

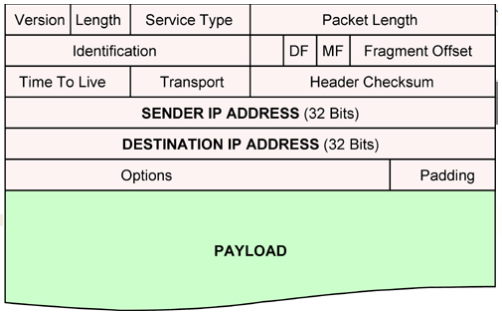
(e.g.) break secret message into 1-byte packets



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

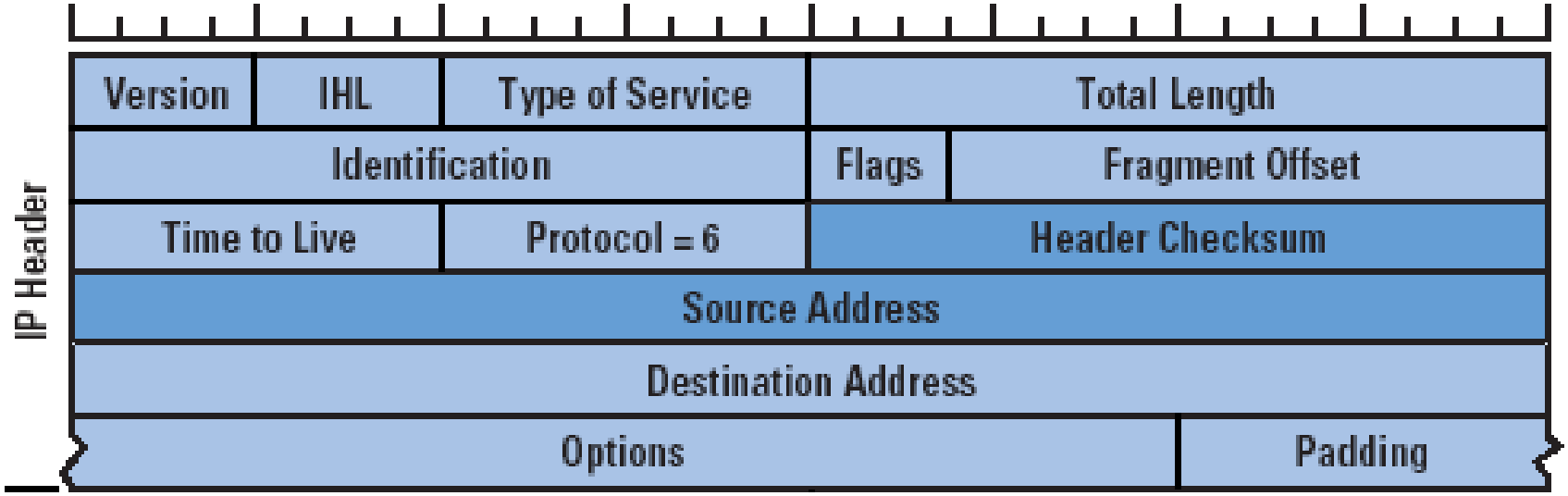


Datagram Steganography



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



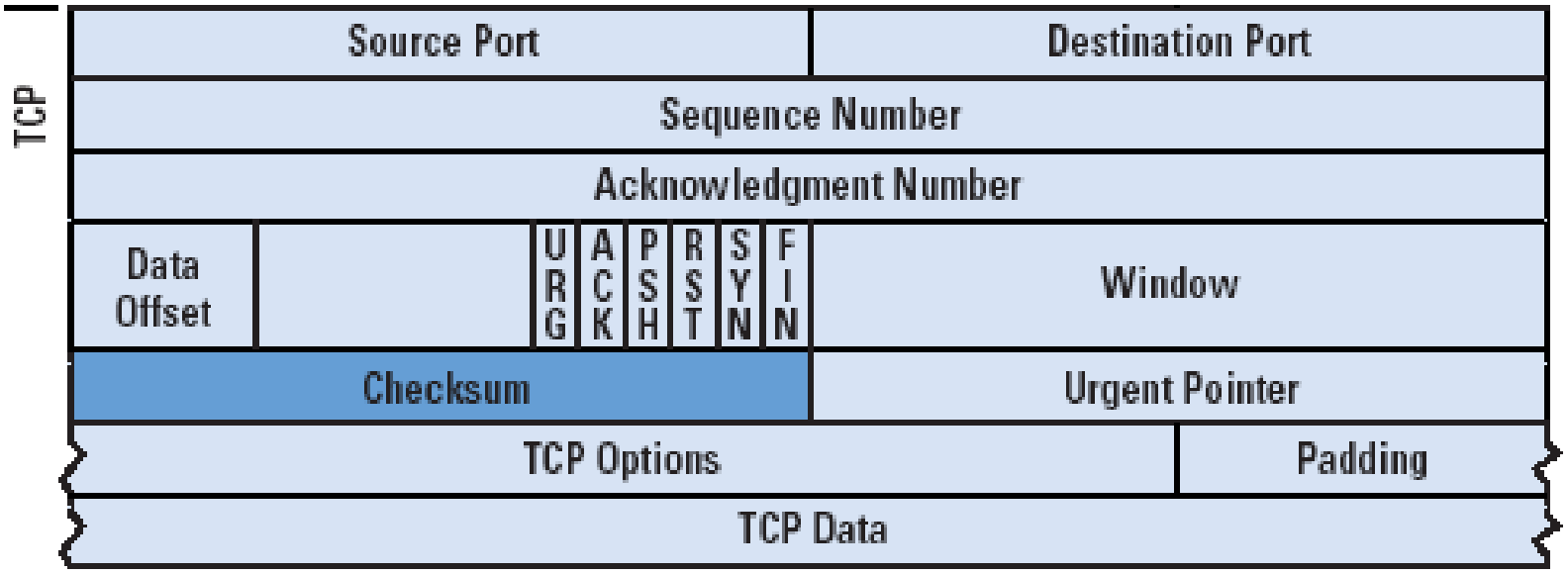
Could Source & Destination Address be used to hide data?!

How about Options field?

Datagram Steganography (cont.)

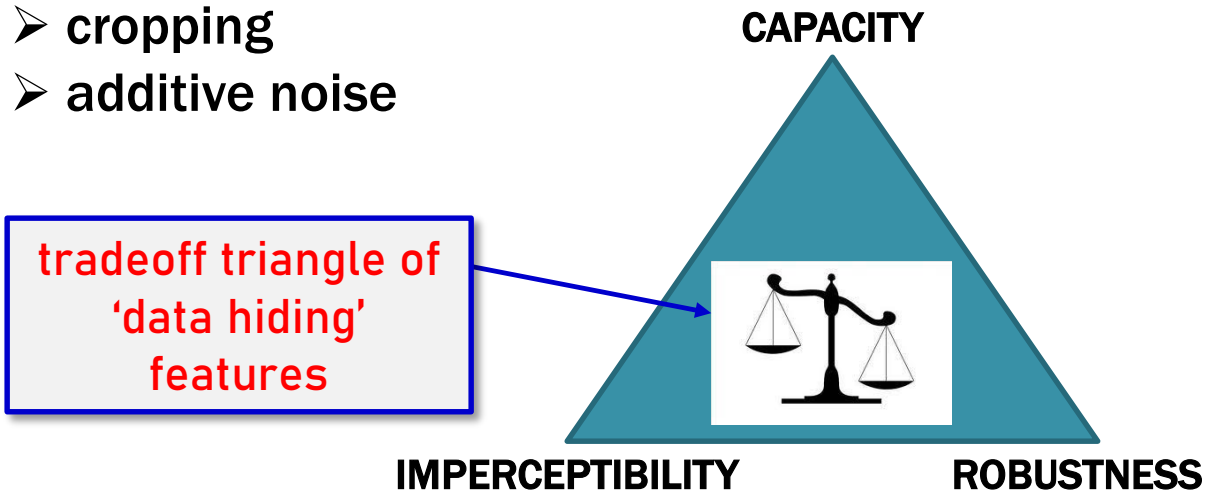
4.2) Datagram Steganography: Using Sequence Number in TCP Packets

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



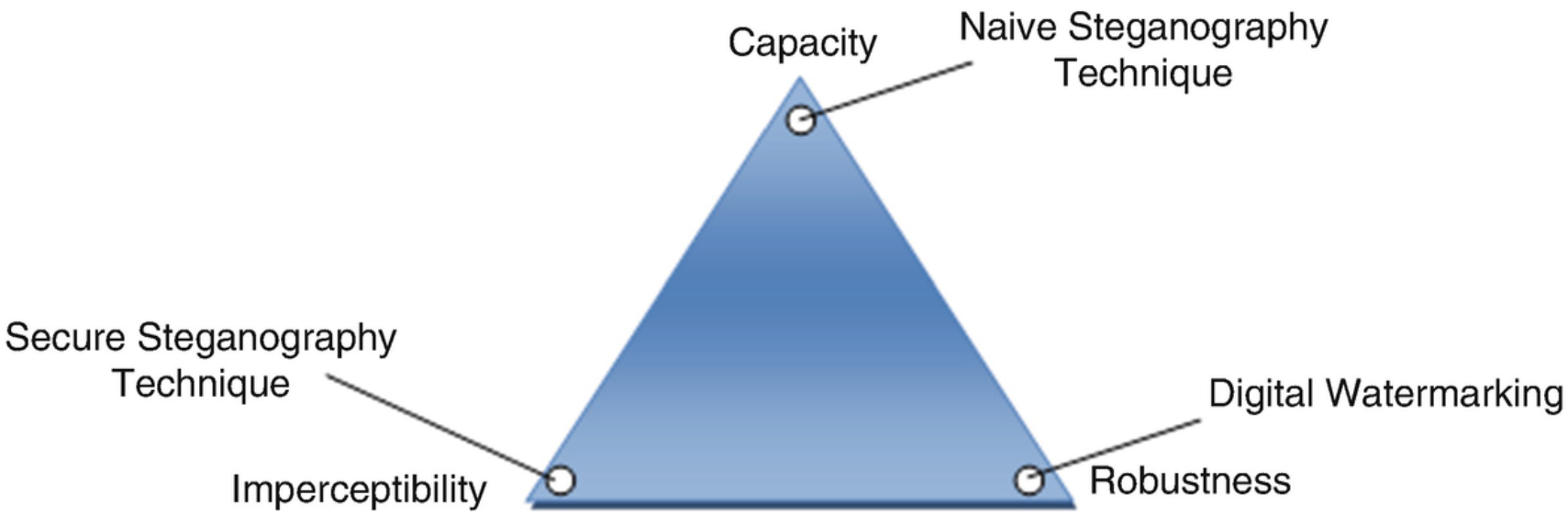
Data Hiding Tech.: Evaluation

- **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



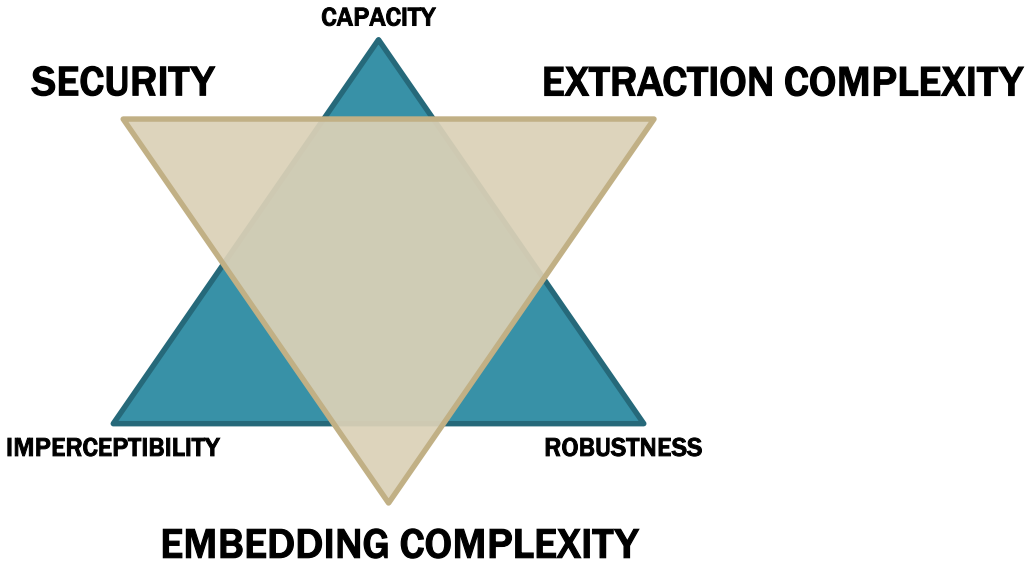
Data Hiding Tech.: Evaluation (cont.)

Example: tradeoff triangle –
steganography vs. watermarking



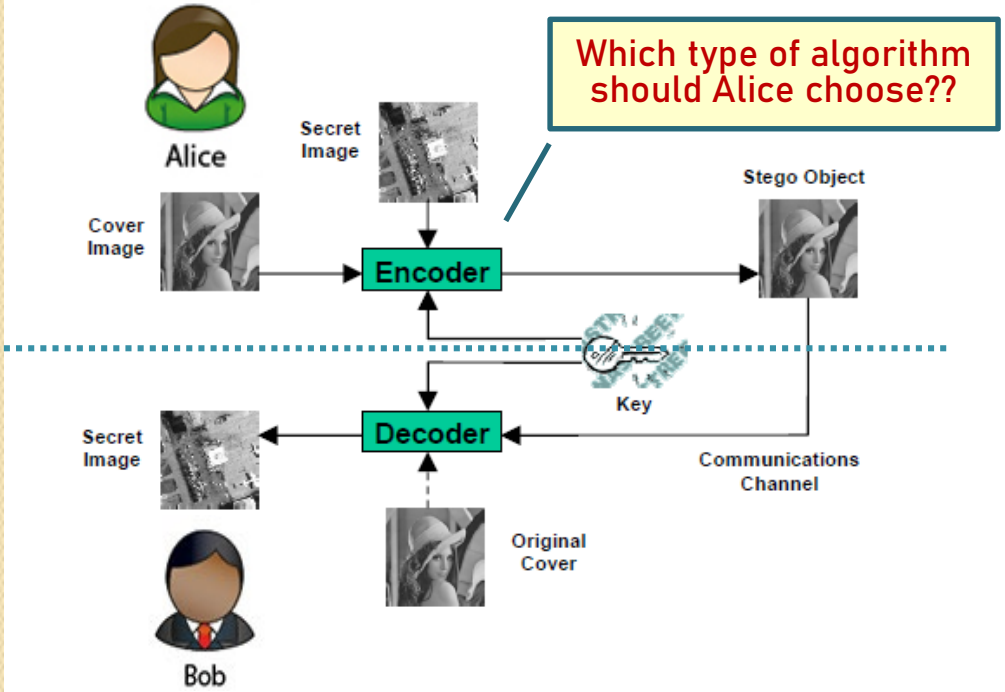
Data Hiding Tech.: Evaluation (cont.)

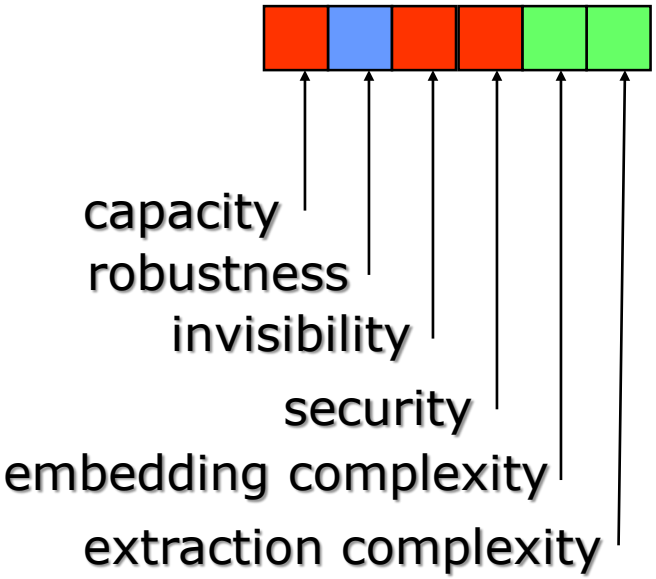
- **Additional Requirements on Data Hiding Techniq.**
  - **security**: embedded info. cannot be removed unless attacker has the full knowledge of algorithm and/or secret key
  - **extraction complexity**: computational effort/time to extract hidden information
  - **embedding complexity**: computational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



Data Hiding Tech.: Evaluation (cont.)

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

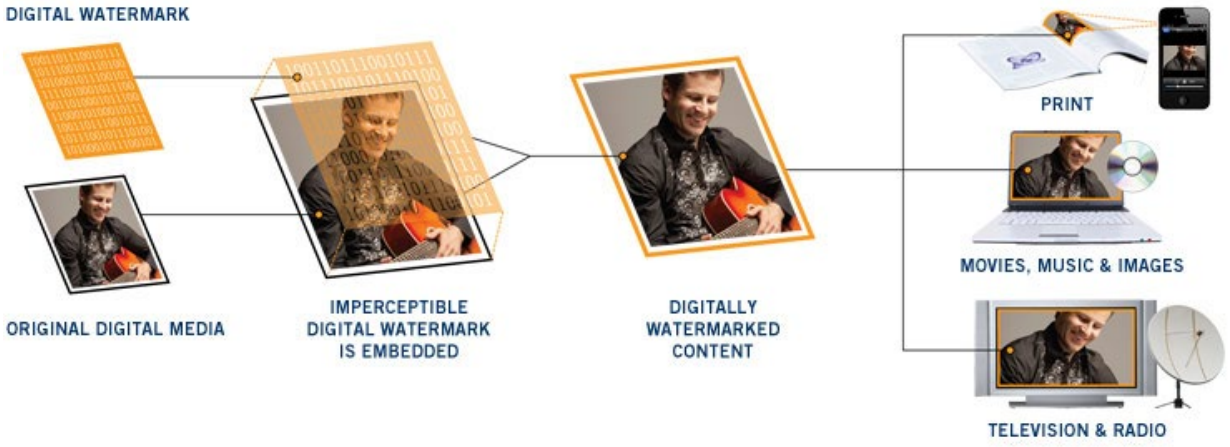




Alice is sending the stego image to Bob as an email attachment.
Packet(s) carrying Alice's email travel through intermediate routers/AS/ISPs.

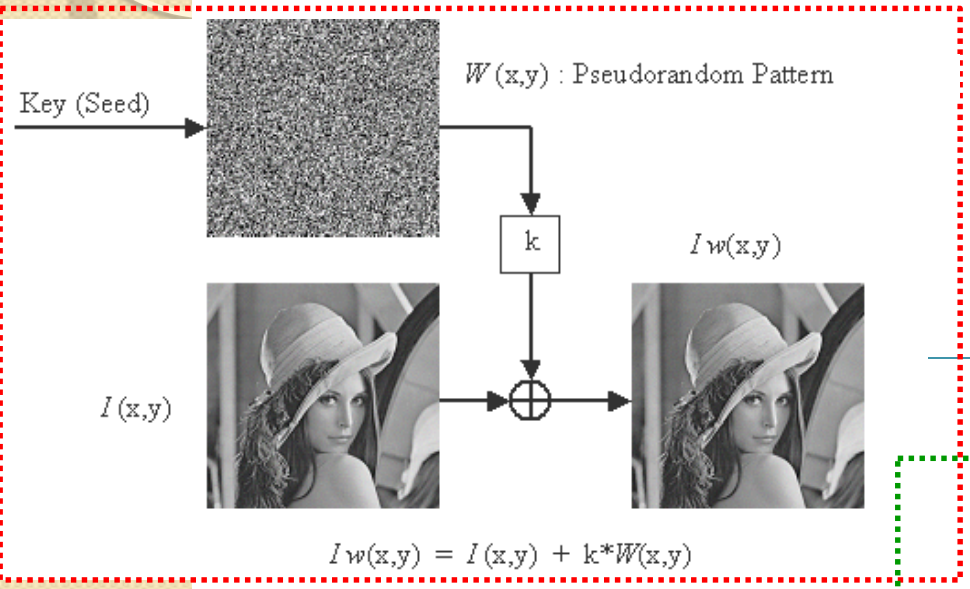
Watermarking

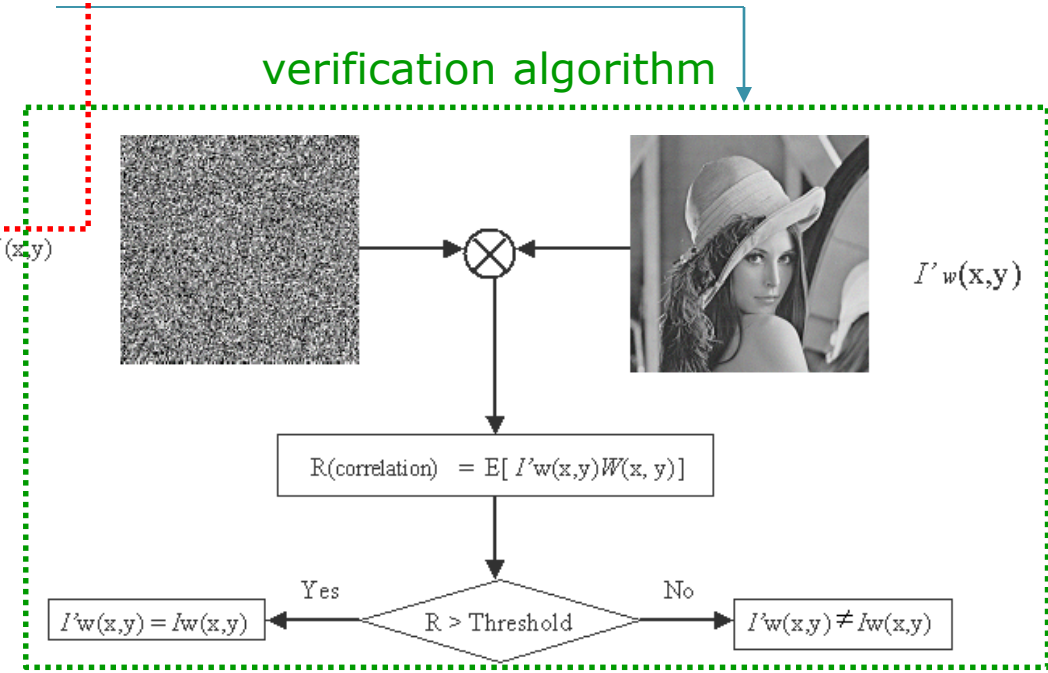
- **Watermarking - Process Components / Terminology**
  - **Watermark (W)**
    - each owner has a unique watermark (e.g., 'layer' of 1 bit/pixel)
  - **Marking Algorithm**
    - incorporates the watermark into the image
  - **Verification Algorithm**
    - determines the integrity/ownership of the image



Watermarking (cont.)

Example: Watermarking in Space Domain

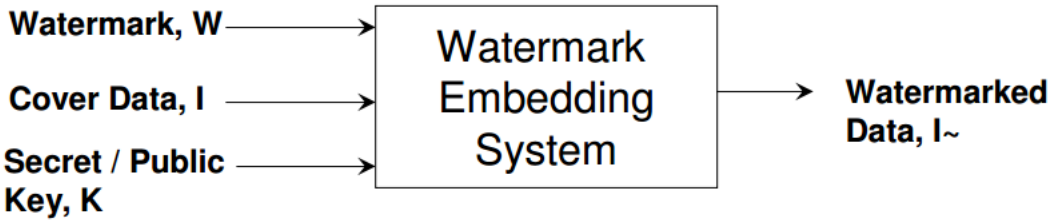




http://scien.stanford.edu/pages/labsite/2001/ee368/projects2001/dropbox/project06/

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 – key is not a 'secret'
      (can be used to actually discover all illicit uses – e.g., by providing the watermark key to search crawlers)



Watermarking (cont.)

E.g., course material vs. selling of digital art online

- **Watermarking vs. Steganography**

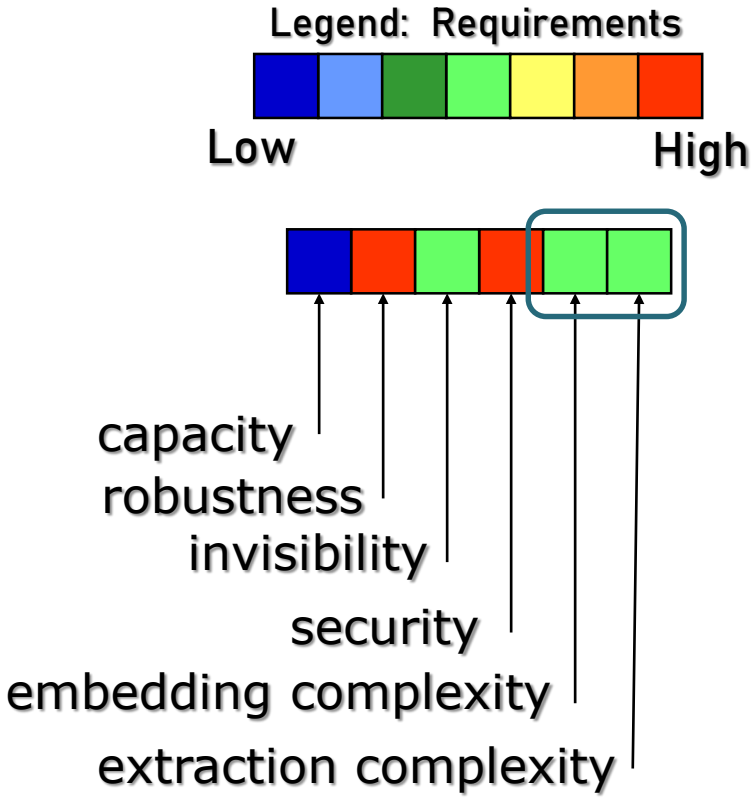
	Requirements	Watermarking		Steganography
		Private	Public	
Goal	Protection of intellectual property rights	++++		–
	Transmission of secret message without raising suspicion	–		++++
Specifications	Perceptual invisibility	++++		+++++
	Statistical or algorithmic invisibility (keep entropy low)	+		+++++
	Robustness against hostile removal, destruction, or counterfeiting	+++++		–
	Resistance against normal signal processing	++++		+
	Capable of surviving common compression coding	++++		++
	Large payload	++		++++
Detection/ Extraction	Extractability/detectability without key	–	++++	++++
	Extractability only with presence of key	++++	–	–
	Requirement of low complexity in extraction/detection	++		+++

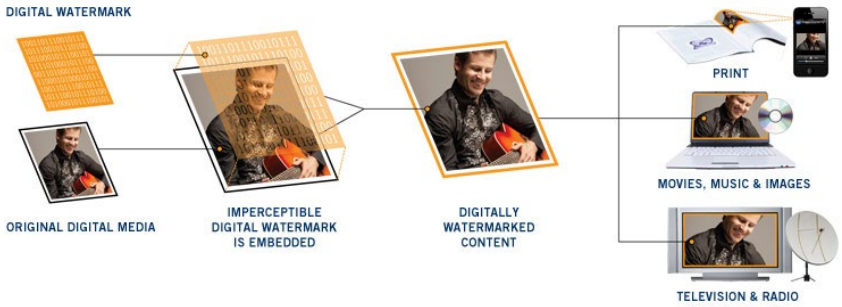
Note: Crucial: +++++ Necessary: ++++ Important: +++ Desirable: ++ Useful: + Unnecessary or irrelevant:: –
Public watermarking schemes do not need the host signal in detection/extraction; private schemes require the presence of the host.

http://cgi.csc.liv.ac.uk/~leszek/COMP526/week4/comp526-3.pdf

Watermarking (cont.)

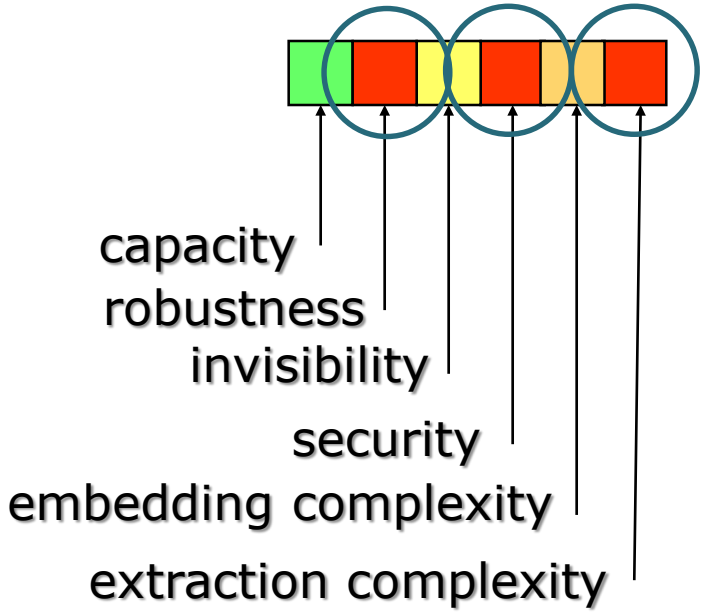
- **Watermarking - Common Applications**
  - **verify the owner of a digital object - copyright protection**
    - placing a (unique) watermark = placing a (unique) signature

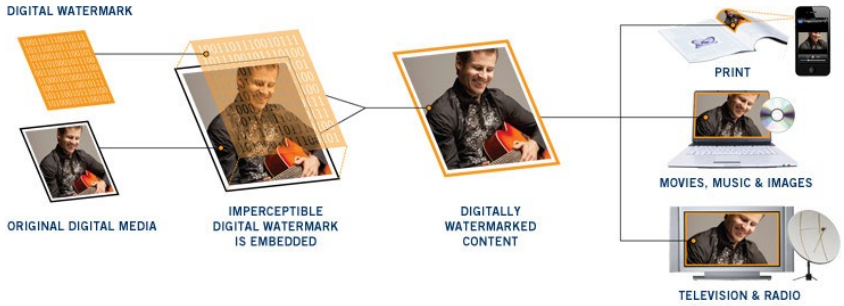




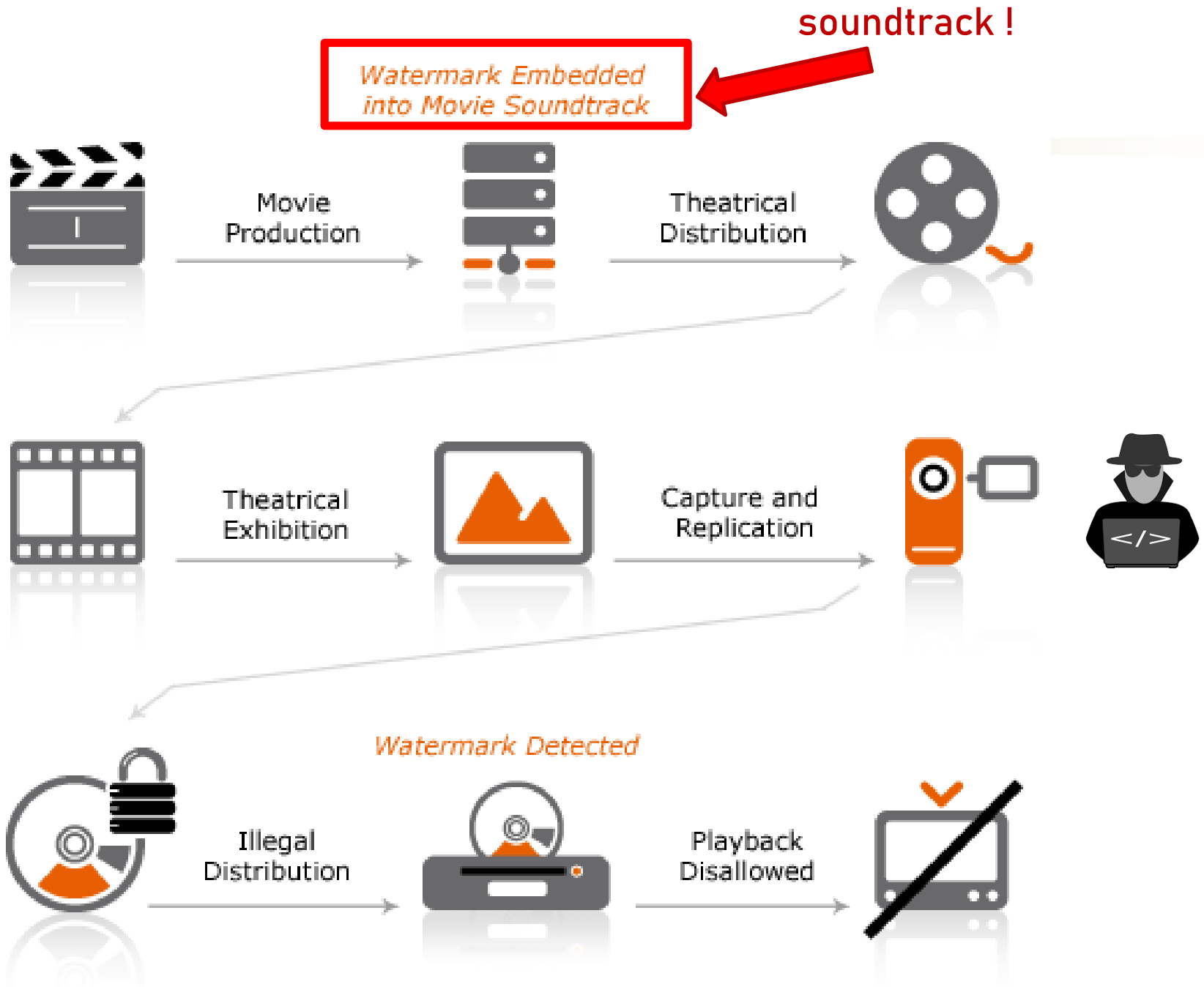
Watermarking (cont.)

- **Watermarking - Common Applications**
  - identify illegal '*theatrical release*' copies of a movie: watermark prior to release to prevent **movie piracy**
    - copy control in DVD and Blu-ray player





http://digitalwatermarkingalliance.org/digital-watermarking-applications/content-protection-audio-video-content/



http://digitalwatermarkingalliance.org/digital-watermarking-applications/content-protection-audio-video-content/

https://randocity.com/2014/02/23/cinavia-annoying/

What is Cinavia and how does it work?

Cinavia is an audio watermarking technology created by the company Verance where an audio subcode is embedded within digital audio soundtracks at humanly imperceptible levels, but at a level where a DSP or other included hardware chip can read and decode its presence. Don't be fooled by the ad with smiling children on the Verance site, this has nothing to do with helping make audio better for the consumer. No, it is solely created for industry media protection.

This Cinavia watermark audio subcode seems to be embedded at a phase and frequency that can be easily isolated and extracted from an audio soundtrack, then processed and determined if it's valid for the movie title being played back. Likely, it's also an analog audio-based digital carrier subcode (like a modem tone) that contains data about the title being played.

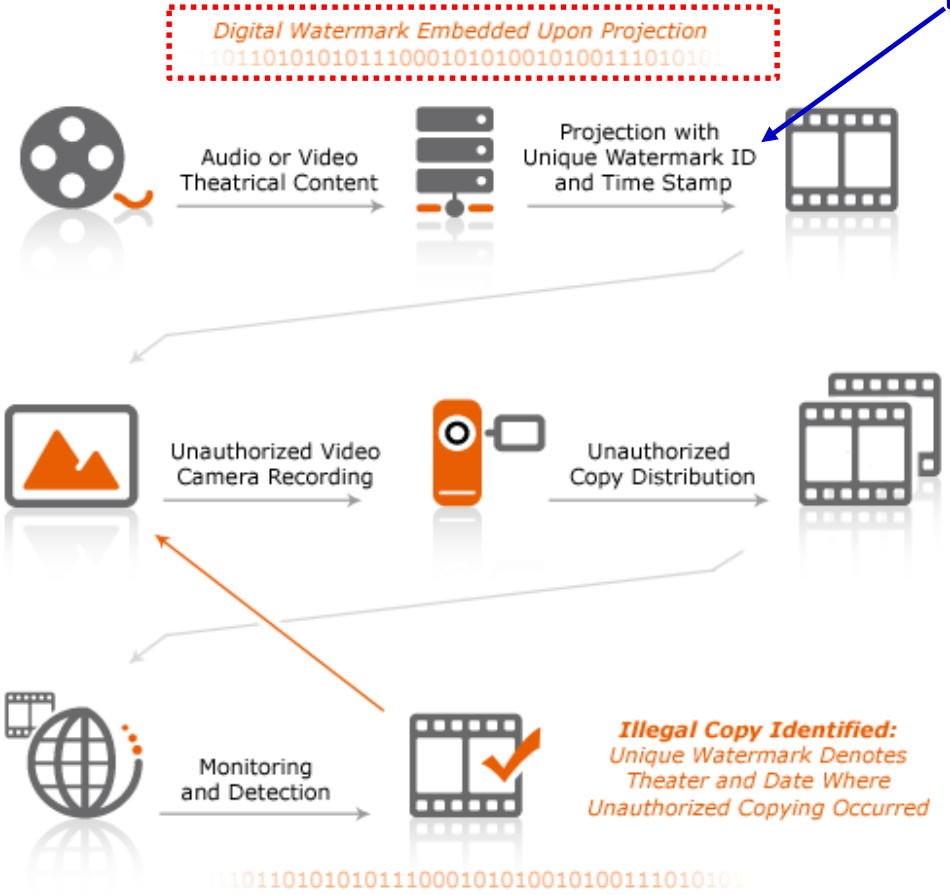
How would I be affected by this?

All consumer Blu-ray players manufactured after 2012-2013 are required to support Cinavia. If the Cinavia subcode is present, the player will blank the audio track if the AACS key is mismatched. This means hardware Blu-ray players from pretty much any manufacturer will be affected by Cinavia protection if the title supports it. CAM copies of theatrical releases will never play because the audio subcode is entirely different for theatrical films and the Blu-ray player will recognize that theatrical subcode and stop audio playback.

Watermarking (cont.)

- **Watermarking - Other Applications**
  - forensics and piracy deterrence

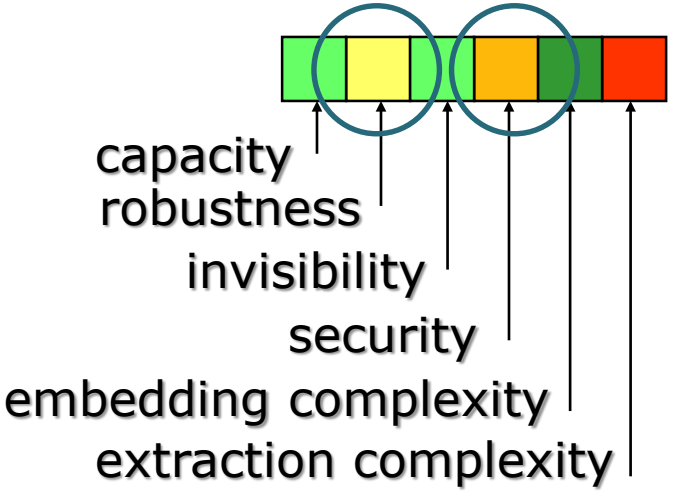
each showing of the movie has a unique watermark

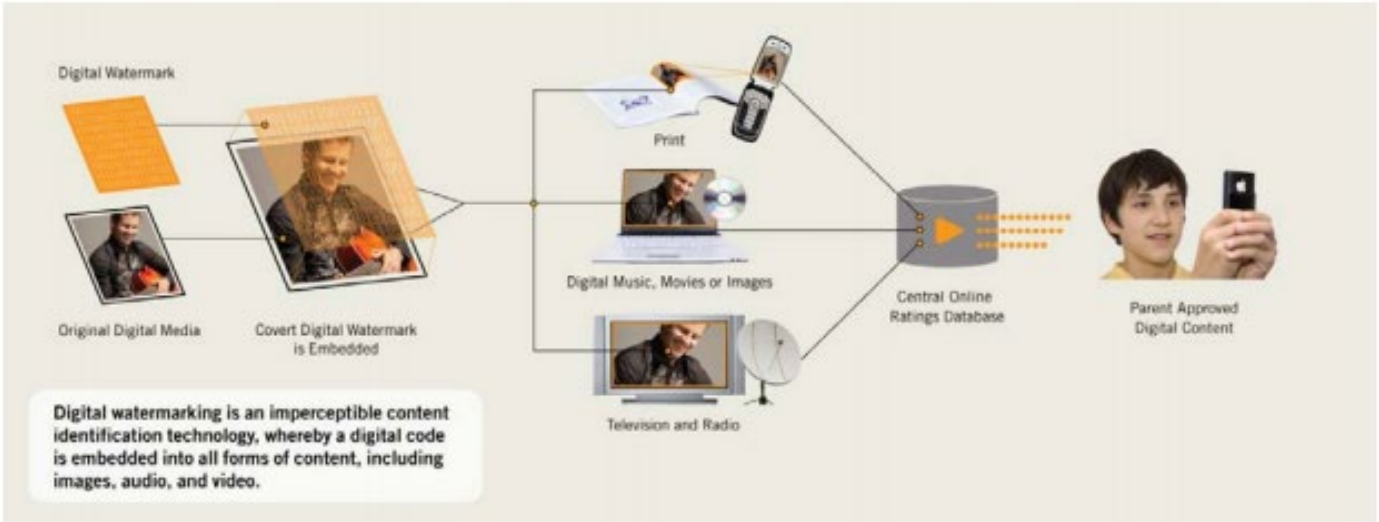


http://digitalwatermarkingalliance.org/digital-watermarking-applications/forensics-and-piracy-deterrence/

Watermarking (cont.)

- **Watermarking - Other Applications**
  - **content filtering**

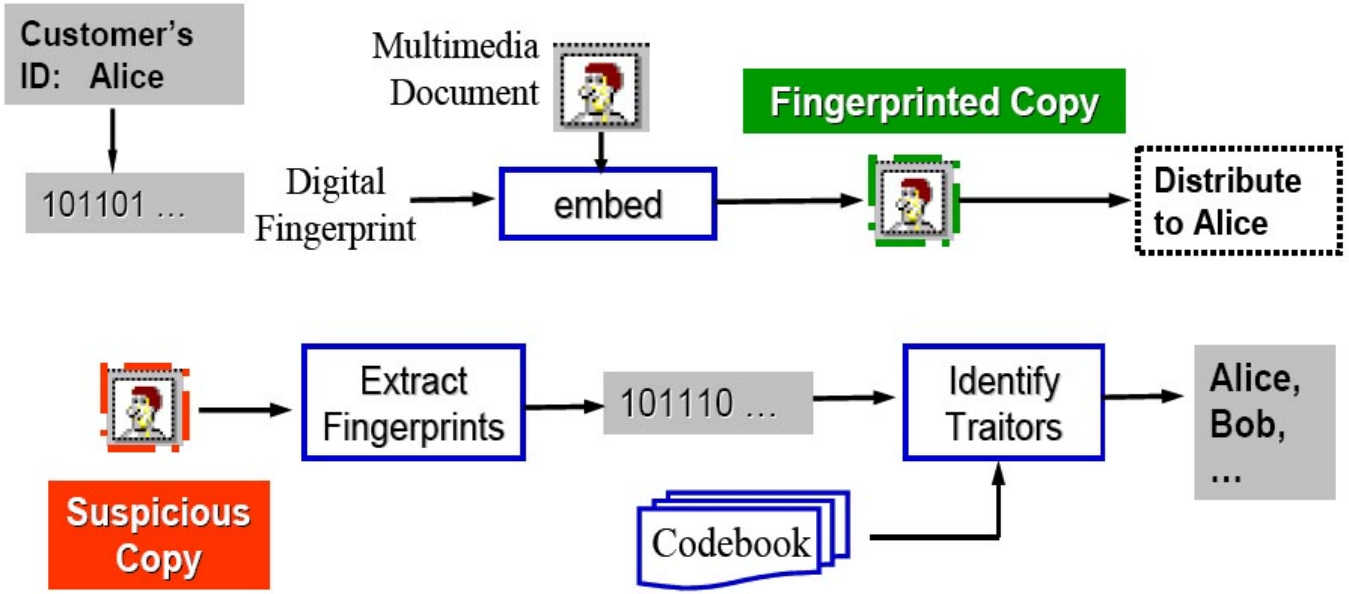




http://digitalwatermarkingalliance.org/digital-watermarking-applications/content-filtering/

Digital Fingerprinting

- **Digital Fingerprinting**
  - process of embedding unique information for each user--copy of a digital object in order to be able to identify entities involved in illegal distribution of the digital object
    - if object with Alice's ID is found on Bob's computer => copy is illegal AND likely provided by Alice



Digital Fingerprinting (cont.)

- requirements of digital fingerprinting