# Media Protection

- Media Protection
- Media Encryption
- Media Watermark

# What is Media Protection?

- New technologies bring with them new issues:
  - Advances in compression techniques make it possible to create high-quality digital content (audio, video, still pictures, etc.)
  - Advances in the network protocols and infrastructure makes it possible to store, stream and distribute this content in a very large scale.
- Media protection or Digital Rights Management (DRM) is the set of techniques used to:
  - Control access to content:
    - Viewing rights
    - Reproduction (copying) rights
- Essentially, media protection is the management of the author's and publisher's intellectual property (IP) in the digital world.

# Media Protection Principles

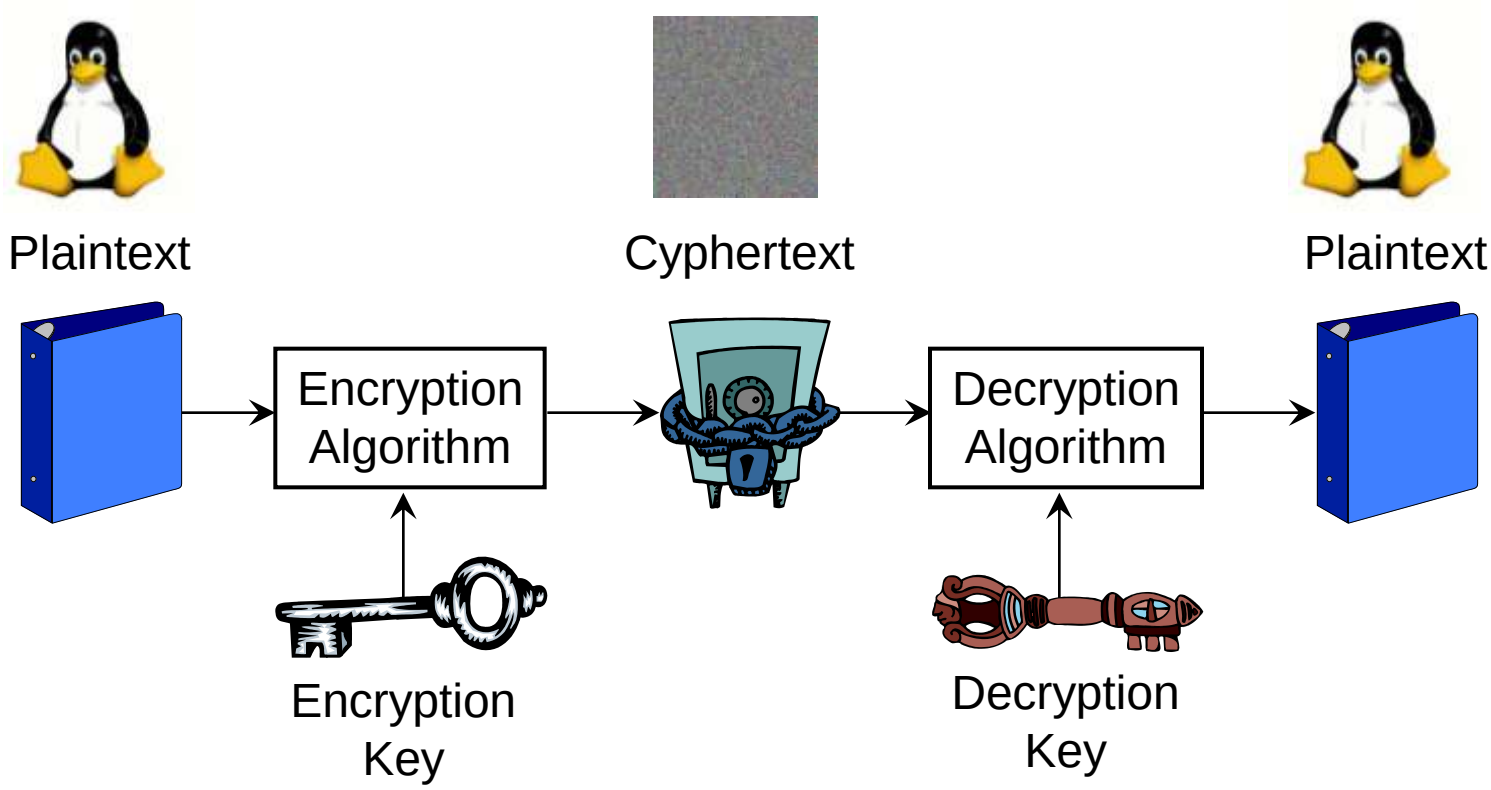
- Encryption of the content to disallow uncontrolled access.
- Decryption key management.
- Access control according to flexible usage rules
  - Number of times content can be accessed; times it can be accessed; trading of access rights.
- Copy control or copy prevention
  - Management of the number of copies that can be made of the content.
- Identification and tracing of multimedia data.
  - May be a requirement even if the copy is made from the analog version of the content, e.g., recording the analog outputs of a digital playback.

# Underlying Technologies

- DRM is based on two fundamental underlying technologies:
  - Encryption
  - Watermarking
- ***Encryption*** is used to “lock” the content and deny access to it to those parties that do not possess the appropriate keys
  - Encryption enforces the restrictions placed on the content by the author/publisher
- ***Watermarking*** is used to “mark” the content so that a particular copy can be traced back to the original user
  - Digital Watermarking is used as a deterrent to large-scale unauthorized copying of copyrighted material.

# Encryption

- Encryption is the process of “obscuring” a message (content, media, file, etc.) so that it is undecipherable without the key.



# Types of Encryption

- ***Symmetric (Secure Key) Encryption***:

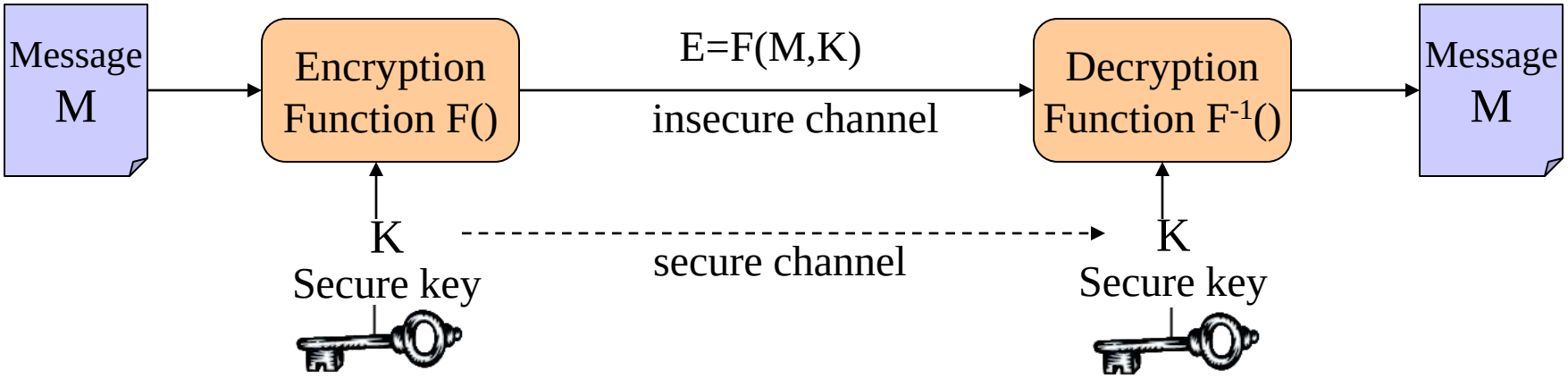

encryption and decryption keys are the same.

- ***Asymmetric (Public Key ) Encryption***:


keys come in pairs, one to encrypt, another to decrypt.

  - Used in Public-Key cryptography, where one key in the pair is kept secret, and another is published.
  - Whatever is encrypted with one key can only be decrypted with the other and vice-versa.
- Symmetric keys are very efficient, but need to remain a secret and must be securely communicated between the participants.
- Asymmetric Encryption is much slower than Symmetric Encryption and requires much larger key lengths to achieve the same level of protection.
- Asymmetric keys (public/private) are slow and inappropriate for actual content exchange.
- Idea: use asymmetric keys to encrypt the symmetric keys, in order to securely communicate them.

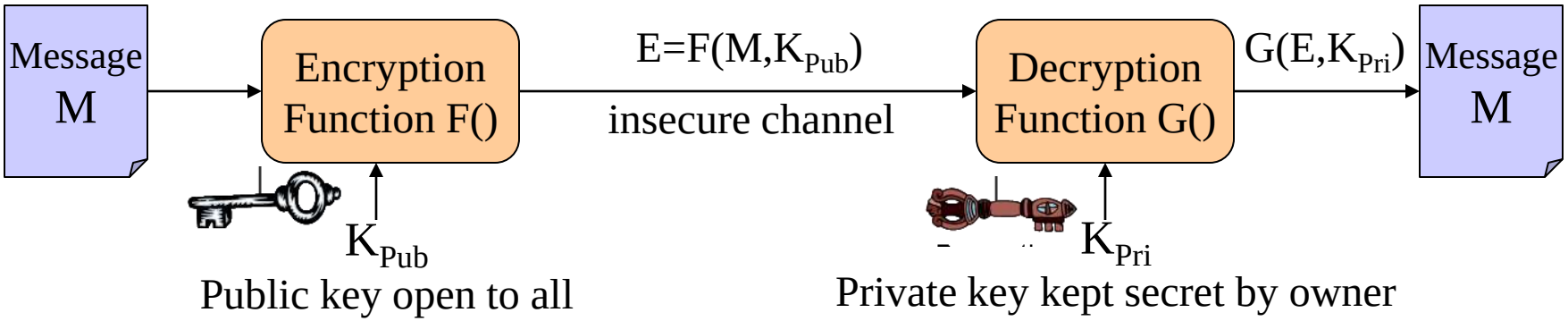
# Secure Key Encryption




Encryption Standards

- DES (Data Encryption Standard)
  - designed originally by IBM, and adopted by the US government in 1977 and by ANSI in1981
  - 64-bit block (encryption unit) and 56-bit key
  - not recommended use after 1998 because it can be broken
- Triple-DES
  - three keys and three executions of DES
- IDEA (International Data Encryption Algorithm) - 128-bit block/key
- AES (Advanced Encryption Standard) - 128-bit block/key

# Public Key Encryption



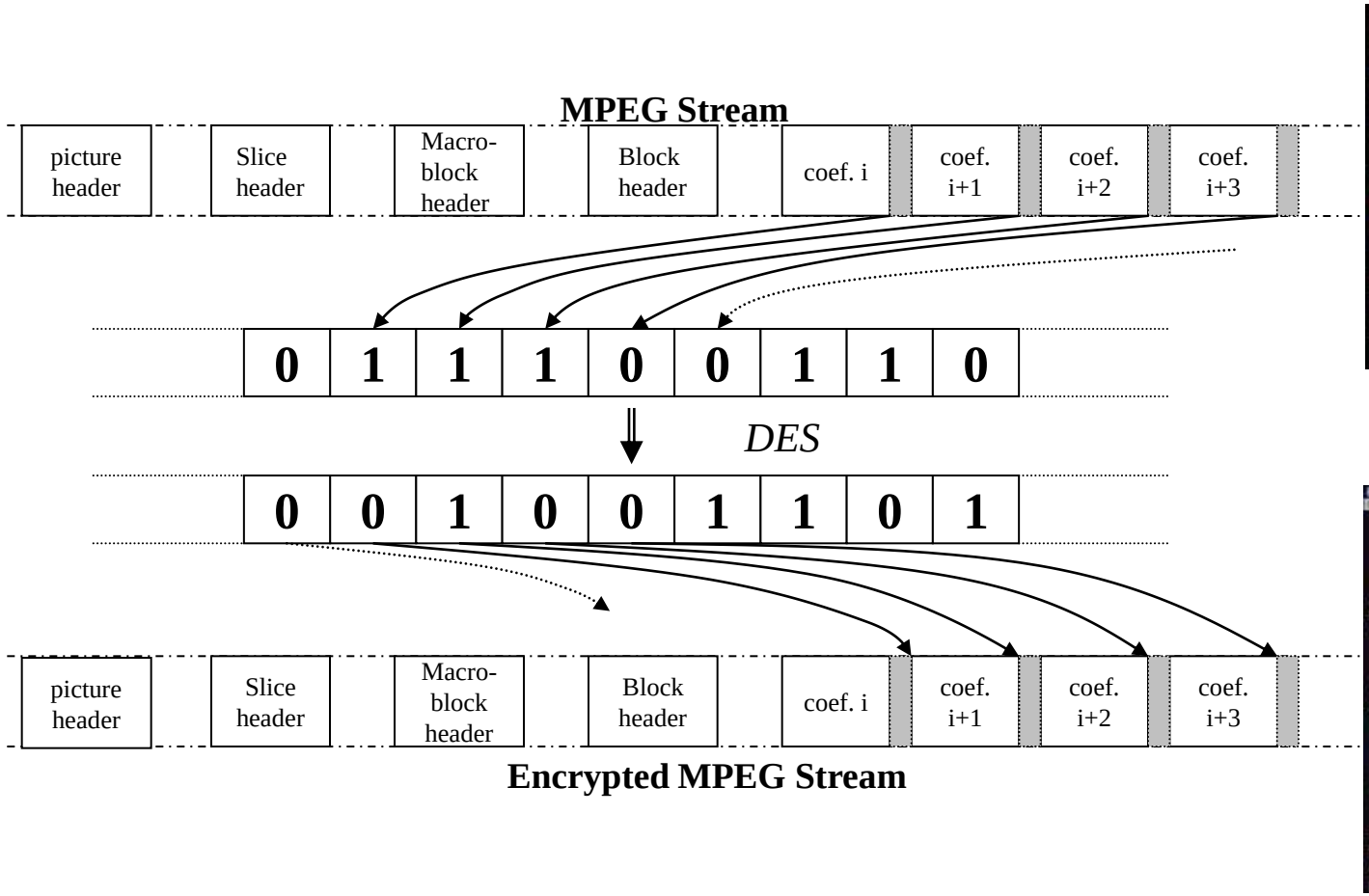

RSA (Rivest, Shamir, Adleman, 1978)

- Key Generation
  - Select p, q which are primes
  - Calculate n=pxq, and t(n)=(p-1)x(q-1)
  - Select integer e satisfied gcd(t(n), e)=1 and e<t(n)
  - Calculate d satisfied exd=1 mod t(n)
  - Public key: KU={e, n}
  - Private key: KR={d, n}
- Encryption
  - Plaintext: M < n
  - Ciphertext: $C = M^e \pmod n$
- Decryption
  - $M = C^d \pmod n$

- Hard to factor n into 2 primes p and q
- RSA key size: 128 to 300 decimal digitals i.e., 425 to 1024 bits
- RSA needs more computations than DES much slower than DES

- Example
  - Given M=19
  - Select two prime numbers p=7 and q=17
  - Calculate n=7x17=119, and t(n)=6x16=96
  - Select e=5
  - Determine d=77 since 5x77=385=4x96+1
  - Ciphertext $C=19^5 \pmod{119}=66$
  - Decryption $66^{77} \pmod{119}=19$

# MPEG Video Encryption Example

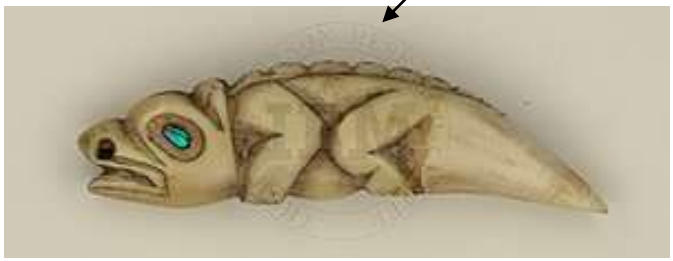



# Watermarking

- Watermarking is the addition of unremovable data to multimedia content, for the purposes of copy identification and tracking.

- ***Visible*** watermark and ***invisible*** watermark

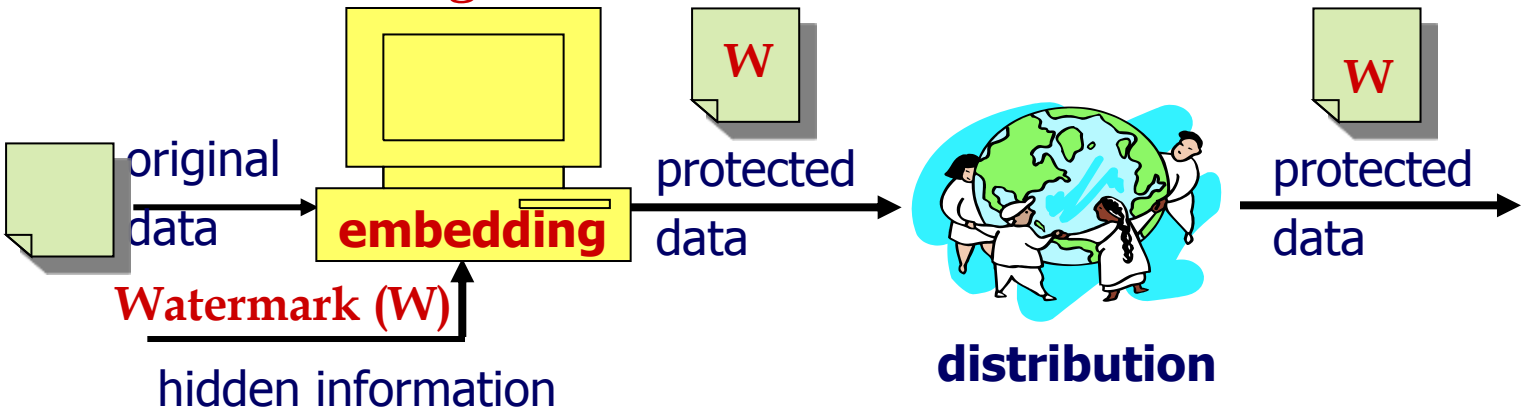
Visible even very light



Special Mark:, e.g.,
Owner's name/sign
Added to the image
But imperceptible
Hidden mark!!

# Watermarking Principle and Requirements

✓ Principle: insert information that travels with the protected data, wherever it goes




- The requirements for such a system are:
  - ***Imperceptibility:*** the addition of the watermark must not degrade the content in a perceptible way.
  - ***Security:*** the watermark must only be accessible by authorized parties.
  - ***Robustness:*** the watermark must survive data manipulation, including malicious manipulation with the intent of removing the watermark.

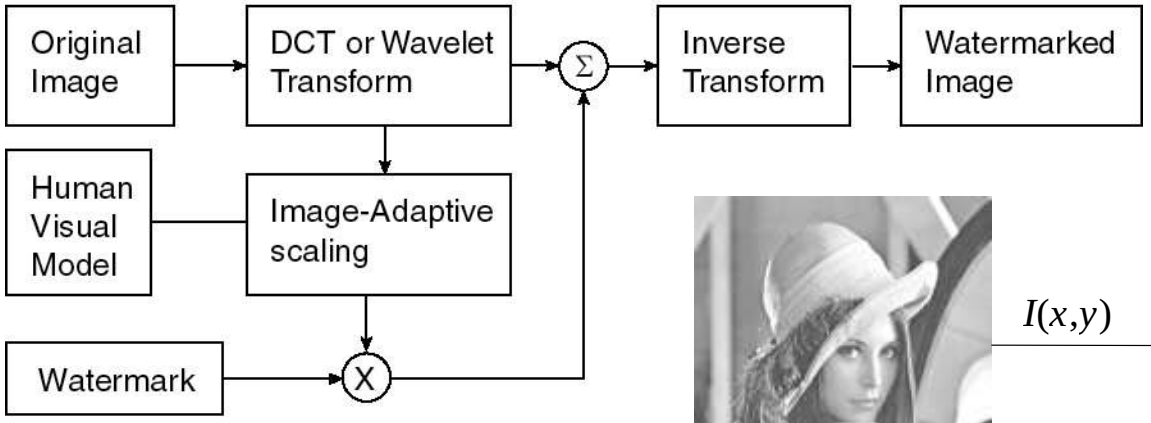
# Watermarking of Text

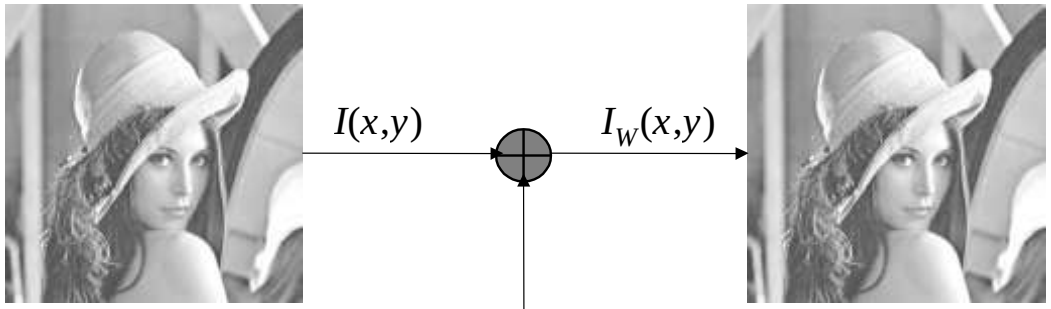
- Watermarking of formatted text is done using one of the following techniques:
  - Line shift coding: moving the lines of text up or down slightly; information is encoded in the way lines are shifted.
  - Word shift coding: same idea, but using spaces between words; much harder to extract.
  - Feature coding: slightly modify features such as the end line lengths of characters such as *b*, *d* and *h*.
- These techniques survive printing, consecutive photocopying up to 10 generations, and scanning.
- Easy to defeat, however: retype the text (OCR or manual).

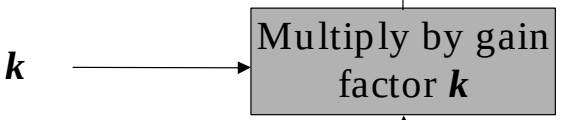
# Watermarking of Still Images

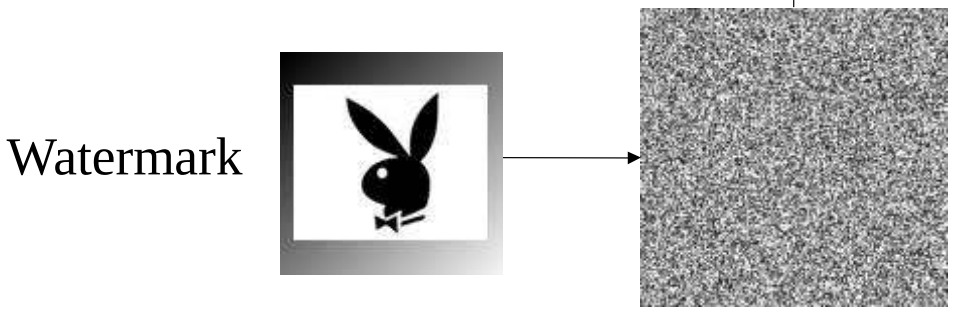
- There is a large body of techniques and literature on watermarking of still images.
- In general terms, the watermark is applied to the original, uncompressed image.
  - Some watermarks are designed in the space domain, while others are applied in the frequency domain.
- Some watermarks are designed to survive still image compression (JPEG), while others cannot.
- Simplest technique: replace the LSB of each pixel by a bit from the watermark.
  - Watermarks will be encoded in sequences of bits.
  - Image may be compressed to less bits prior to the injection of the watermark.

# Additive Watermark with Spread Spectrum




$W(x,y)$: Pseudo Random Pattern {-1,0,1}

# Sample Images

Original

Watermarked

Source: **`http://dynamo.ecn.purdue.edu/~ace/water2/digwmk.html`**
Prof. Edward J. Delp's research group

# Video Watermarking

- In general, the same techniques used for still images can be applied to video.
- Considerations:
  - The signal space for video is much larger than for still images; there is no need to use very complex schemes to minimize distortion while maximizing capacity.
  - Video watermarking schemes need to be less complex because in most cases they need to run in real time and need to address compressed video.
  - Video watermarks must be able to survive frame averaging, dropping and swapping - spread information over multiple frames
  - Depending on application, it is desirable to retrieve the watermark from short sequences from the material.

# Video Watermarking Techniques

- DCT-based method:
  - Use the watermark to modulate a pseudo-noise signal of the same dimensions as the video.
  - Compute the DCT of the watermark and add it to the DCT of the original video.
  - Do not use the coefficient if this increases data rate too much.
  - Add drift compensation to avoid artifacts.
  - Typically capable of achieving around 50 bits/sec watermark.
- Motion-Vector method:
  - Find motion vectors that point to flat areas.
  - Slightly modify them to add the watermark information (randomized).
  - Watermark can be derived directly from motion vectors.

# Audio Watermarking

- When compared with video, audio introduces the following issues:
  - Much less samples resulting in lower watermark capacity.
  - Humans are much less tolerant to audio changes than to video changes; harder to achieve imperceptibility.
- Basic spread-spectrum technique is also used for audio, but needs to be refined.
  - Example: making the power of the watermark signal vary with the overall power of the audio.
- Lot of activity in this area
  - See the “Secure Digital Music Initiative” (SDMI), at **http://www.sdmi.org**.

# Demos of Image Watermark