# 5 Digital Rights Management

5.1 Media Rights

5.2 Rights Models

5.3 Principles of Encryption-Based DRM Systems

5.4 Watermarking

5.5 DRM Standards and Selected Commercial Solutions

Literature:

Bill Rosenblatt, Bill Trippe, Stephen Mooney: Digital Rights Management – Business and Technology, M&T Books 2002

Wenjun Zeng, Heather Yu, Ching-Yung Lin: Multimedia Security Technologies for Digital Rights Management, Academic Press 2006

# Hiding Secret Messages

- Herodot (440 BC) reports:
  - Demaratus wrote a secret message (about a forthcoming attack) on a wooden tablet before applying the wax coating (and adding another message)
- Histiaeus (6th century BC):
  - Shaved the head of a slave and tattooed a message on his head
  - After hair was grown again, slave was sent to Aristagoras who shaved the head to read the message
- Writing a concealed message: "Steganography"

# Watermarking

- Watermarks convey information about a document
  - Without interfering with the appearance or readability of the document
  - By being inextricably bound together with the document
- Recognizable watermarks:
  - Clearly recognizable, e.g. logos in video information
- Hidden watermarks:
  - Related to “Steganography” (or sub-area thereof)
    - » Steganographic message: existence usually not expected
    - » Watermark: hidden, but existence may be known
- Watermarks typically carry “metadata” about the document
  - Universal watermarks:
    - » All copies given away carry the same watermark
  - Individual watermarks (“fingerprinting”)
    - » Copies carry individual watermarks

# Characteristics of Digital Watermarks

- **Undetectability:**
  - The watermark does not detract from the visual or audible experience of the content
- **Robustness:**
  - The watermark survives copying to lower-resolution formats or from digital to analog formats
  - “Analog hole” = Circumvention of watermark by re-digitizing analog content
- **Capacity:**
  - The watermark should be able to contain as much data as possible
- **Security:**
  - The watermark resists attempts to erase or alter it
- **Efficiency:**
  - The overhead created by inserting or extracting the watermark is tolerable
- Watermarking cannot prevent unauthorized copying, but can help DRM controllers

# Applications of Digital Watermarking

- Copyright protection: Documenting the copyright
- Fingerprinting: Tracing individual copies given to different parties
- Copy control: Embed instructions to copying devices
- Broadcast monitoring: Enable automated tracking of broadcasts (e.g. for advertisements)
- Unauthorized modification detection: Using fragile watermarks being destroyed when document is modified
- Annotation and indexing: Identifiers leading to source, or metadata for search engines
- Link media: Embed machine-readable information in images (e.g. link encoded in poster)
- Medical applications: Protection of patient data by embedding them within medical images
- Covert communications: Transmitting hidden data
  - Potential for criminal misuse

# Classification of Watermarking Based on Domain

- Spatial domain methods:
  - Earlier works in the area
  - Examples:
    - » Least significant bit replacement scheme
    - » Patchwork scheme
    - » Spatial quantizer scheme
  - In general computationally less complex, but less secure and robust
- Frequency domain methods:
  - Based on transformation into frequency domain
    - » E.g. Discrete Cosine Transform (DCT),
      Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT)

# Principle of Watermark Insertion

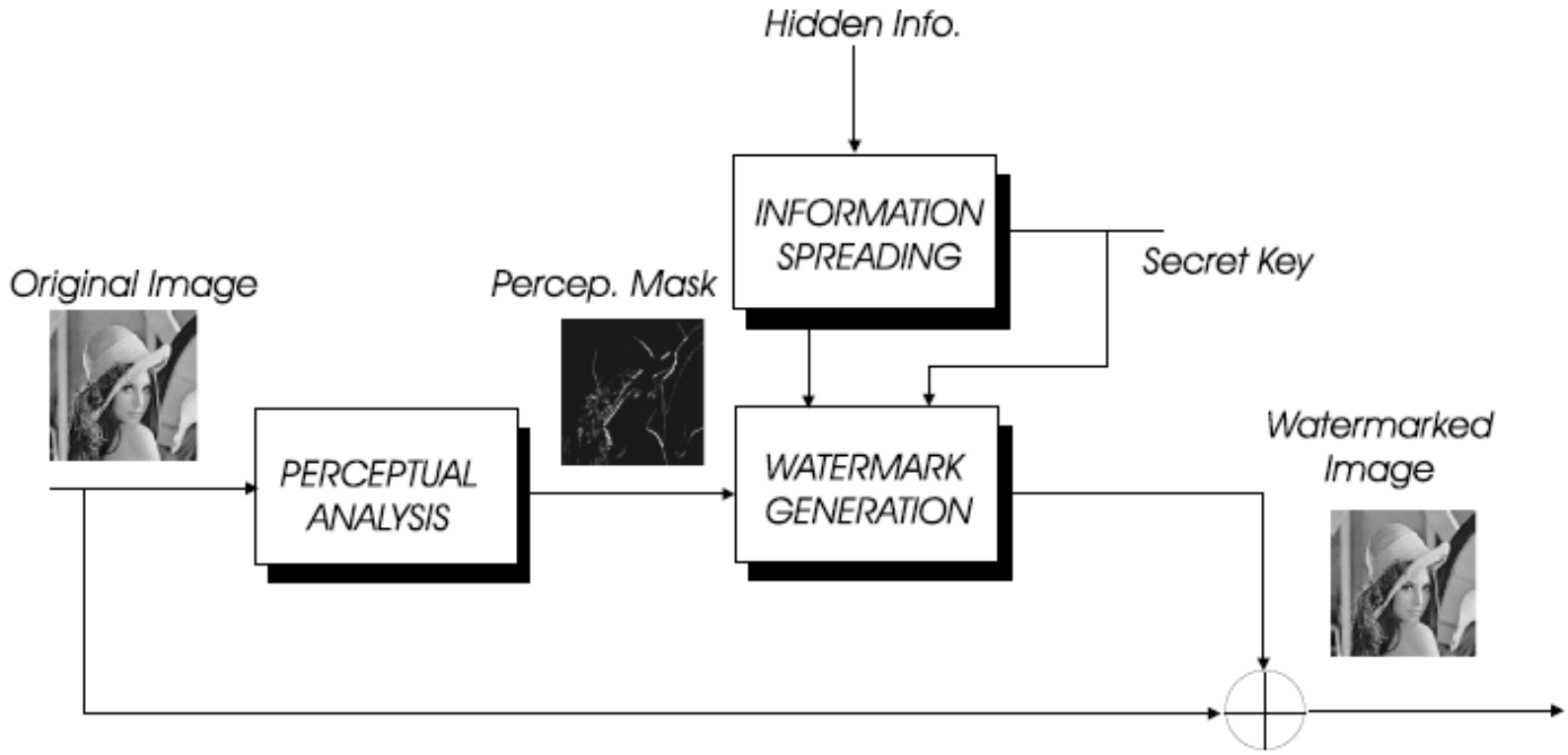



Figure 1: *Watermark insertion unit*

From: Fernando Perez-Gonzalez and Juan R. Hernandez, A TUTORIAL ON DIGITAL WATERMARKING, in: IEEE Intl. Carnahan Conf. on Security Technology, 1999

# Principle of Watermark Extraction

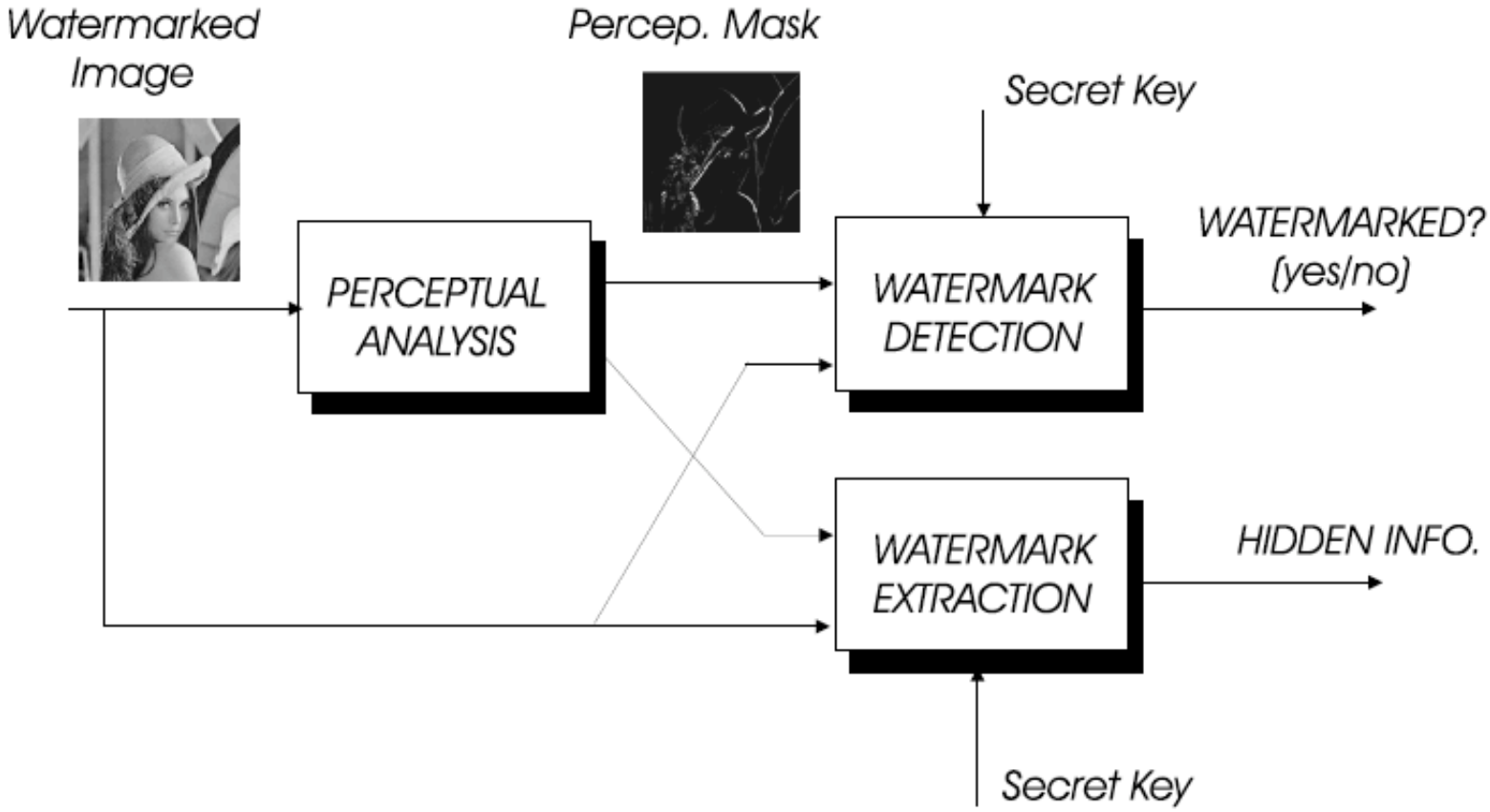



Figure 4: *Watermark detection and extraction unit*

From: Fernando Perez-Gonzalez and Juan R. Hernandez, A TUTORIAL ON DIGITAL WATERMARKING, IEEE Intl. Carnahan Conference on Security Technology 1999

# Watermarking and Perceptual Significance

- Naive idea:
  - Use parts of the audio/image encoding which are not relevant for user perception, e.g.:
    - » Masked frequencies in audio (e.g. between MP3 truncation threshold and perception threshold)
    - » High frequency AC coefficients in JPEG
    - » Low-significance bits (LSB) of samples
  - Robustness problem: Easy to remove
- Using a *perceptually significant* part:
  - E.g. Low-frequency parts of audio/image
  - Removing the watermark causes perceptible distortions
  - Undetectability problem: Danger of becoming perceptible

# Example for Naive LSB Steganography

- Spatial Domain, information encoded in Least Significant Bits
- Easy to remove by removing the respective bits
- Source: Wikipedia

Remove all but last 2 bits of each color component

Brighten by factor 85

# Patchwork: Stochastic Watermarking

- Choosing randomly many pairs of pixels and summing the difference of values for each pair:
  - Expected average value is zero
- Take pairs of pixels and increase value for one, decrease for other
  - To an extent becoming statistically significant
  - Several amounts of standard deviation
- Existence of watermark can be detected
  - Encoded information is 1 bit
  - Decoder has to know the secret = random sequence of pixel pairs to be inspected
- Improvement: Patches (regions) instead of single locations
- Very robust against image modifications

# Typical Spread-Spectrum Watermarking

- Spread-spectrum:
  - Signal is spread over more bandwidth than necessary for its encoding
- Spread-spectrum watermark:
  - Encoded in broad frequency spectrum
  - Mid band frequencies (not too high or too low)
- Spreading according to key:
  - Secret to be known for extraction (e.g. seed value for pseudo-random sequence)
- Sketch of a possible algorithm for images:
  - Select luminance component
  - Carry out DCT transformation as in JPEG
  - Add pseudo-random noise to a selection of mid-band coefficients
    - » May be scaled to match coefficient value
  - Carry out inverse DCT
- Detection:
  - Extract relevant frequency coefficients
  - Determine correlation with noise sequence (threshold)
  - Block decodes to 0 or 1 depending on outcome (1 bit)

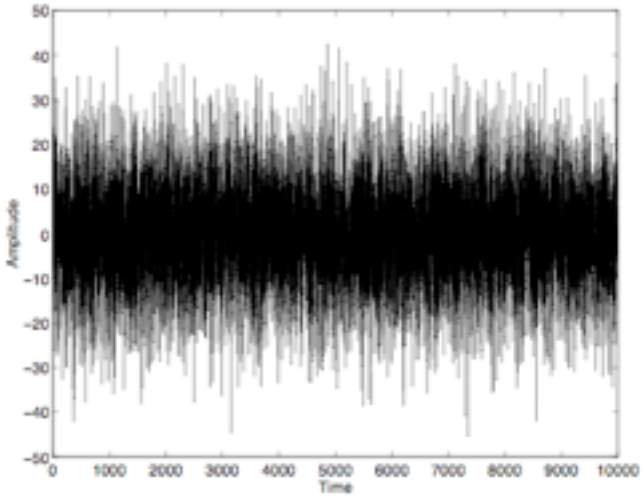



Image: O'Ruanaidh/Pereira

# Spread-Spectrum Watermarking for Sound

- Frequency domain manipulation applied to DCT coefficients in lossy audio compression (e.g. MP-3, MPEG-AAC)
  - Adding noise to mid-band frequencies
- Shape the noise according to psychoacoustic model of human hearing
  - Energy distribution over frequencies
- Amplify noise appropriately to keep information intact after quantization
- Listening tests to prove that watermark is "inaudible"
  - However: "more audible" than what lossy compression omits
  - "Almost inaudible"?

Boney/Tewfik/Hamdy: Digital Watermarks for Audio Signals, International Conference on Multimedia Computing and Systems, 1998

# Example: DigiMarc Technology

- www.digimarc.com (market leader in watermarking technologies)
- Specialized in pigital watermarking of images and pictorial documents:
  - Photographies, satellite images etc.
    - » Ensuring the integrity of the data, tracking the usage
  - ID documents (e.g. travel passports)
  - Financial documents (e.g. bank notes, financial instruments)
    - » Identifying genuine documents, detecting alterations


**PROFESSIONAL**
For photographers and image creators with up to 2,000 images. Digimarc Search Service is included to locate where your images are being used online.

# Example: Verance Audio Watermarking

- See www.verance.com
  - Business partnership with DigiMarc
  - Mainly used in DVD production (in particular DVD-Audio)
- Problem: High-quality audio vs. audible watermarks

VERANCE
EVOLUTION IN SOUND TECHNOLOGY

Hundreds of high-resolution DVD-Audio and digital cinema titles have been released to rave audiophile reviews, including the 2005 GRAMMY award winner for "Best Surround Sound Album", Dire Straits' "Brothers in Arms – 20th Anniversary Edition" and the 2007 Oscar winner for "Best Sound Editing", "The Bourne Ultimatum".

**Capacity**
The Verance audio watermarking technology allows for multiple layers of watermarked data that can be detected and decoded by different application-specific watermark decoders. These serve a variety of market needs simultaneously through the deployment of multiple independent watermarks including copy and usage control data, content identification data and specific transactional data.

In contrast to other technologies, such as "fingerprinting," that rely on pattern matching against a database of previously analyzed works to identify content, Verance's audio watermark:

- can be detected and interpreted locally, without reference to an external database;
- provides a precise and immediate result, without a computationally intensive search;
- scales easily, delivering both extremely low and constant processing load and false detection rate regardless of the population of identifiable works;
- enables different copies of identical works to be distinguished.

# Attacks on Digital Watermarks

- Removal attack
  - Consider watermark as noise and reconstruct original information, e.g. by median filtering
  - Variant: “collusion attack” on fingerprinted content, create mix of versions
- Oracle (or sensitivity) attack
  - Assumes access to a watermark detector
  - First step: Create modified image close to decision threshold of detector
  - Second step: Modify luminance of each pixel until detector switches
    - » Create minimal distortions but keep out of watermark detection
- Stirmark attack:
  - Create small random geometrical distortions (e.g. minimal warping)
  - Modified version is no longer recognized as watermarked by detector
  - Loss of synchronization/correlation in watermark information
- Tendency: Robust watermark technology is extremely challenging

# 5 Digital Rights Management

5.1 Media Rights

5.2 Rights Models

5.3 Principles of Encryption-Based DRM Systems

5.4 Watermarking

5.5 DRM Standards and Selected Commercial Solutions

Literature:

Bill Rosenblatt, Bill Trippe, Stephen Mooney: Digital Rights Management – Business and Technology, M&T Books 2002

# Intellectual Property Identification: DOI

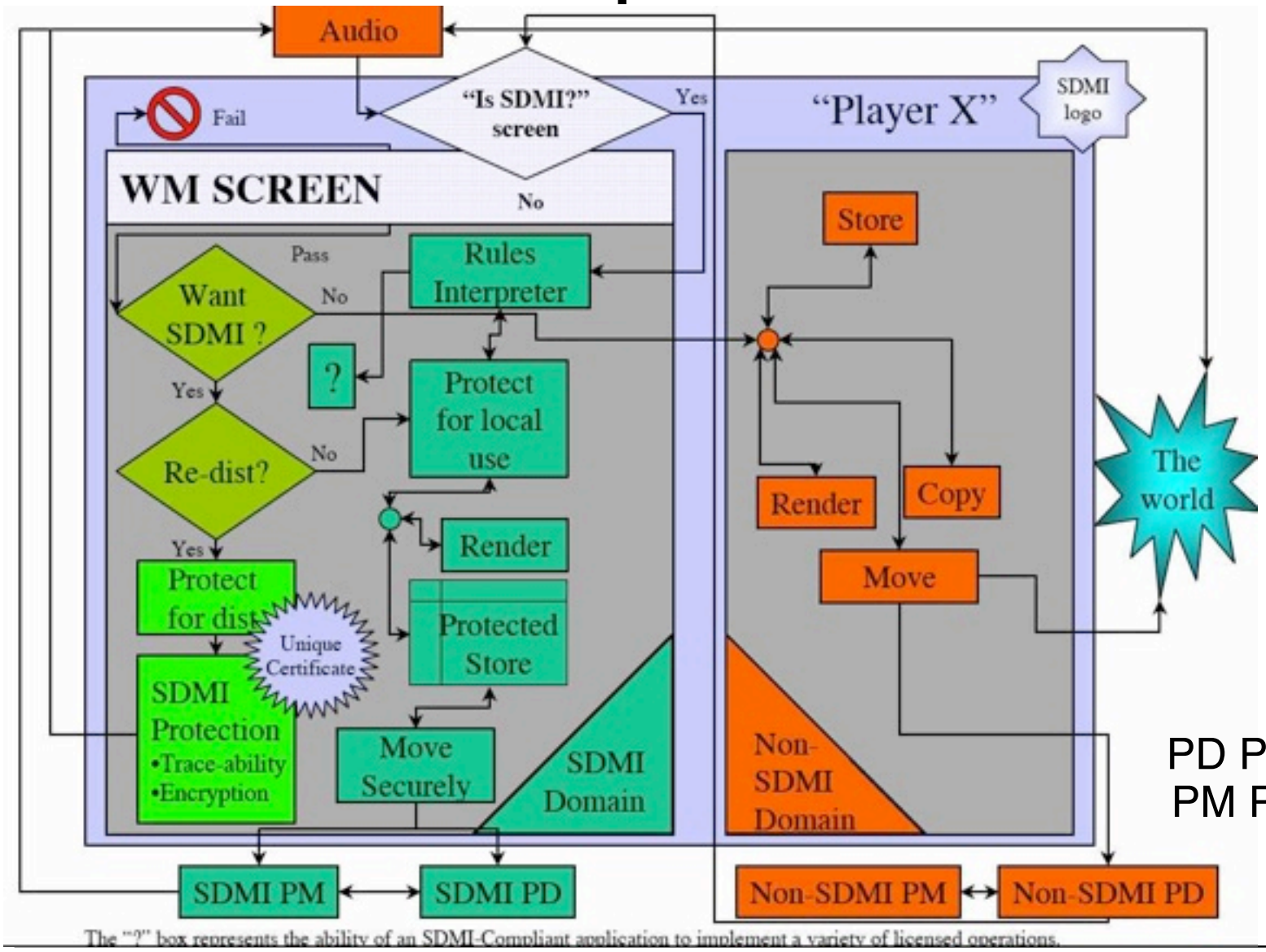
- Digital Object Identifier (DOI)
  - Unique identification of any kind of digital content
  - Initiative started 1994, active ANSI/NISO standard in 2004 (see www.doi.org)
    - » Currently over 20 million DOIs assigned
- Based on IETF “Uniform Resource Identifier” standard
- Syntax:

  **`doi:` *`Prefix / Suffix`***
- *Prefix* of form ***`directoryID . publisherID`***
  - Can be obtained by publisher from a registration agency
  - Currently always starts with “10.” (built for extension)
- *Suffix:*
  - Can be determined by publisher in arbitrary syntax
  - E.g.: **`doi:10.1016/S0167-6423(02)00032-1`**
- DOI directory (http://dx.doi.org/ ) resolves DOI to a URL
  - Publisher responsible for maintaining the information

# Secure Digital Music Initiative SDMI

- 1999: Initiative of music industry: Set of open standards for online distribution of digital music with built-in rights management
  - Recording Industry Association of America (RIAA)
  - “Big 5” record labels (Sony, Warner, BMG, EMI, Universal)
- First goal: Standard for DRM-enabled MP3 players
  - Chartered *Leonardo Chiariglione* from Telecom Italia (MPEG chair)
  - Result: High-level architecture for a long-term perspective in digital music
    - » Uses watermarking (for copy-protected content playable on other devices)
    - » Uses encryption (for fully protected content playable only on SDMI devices)
  - Plan for a two-phase transition:
    - » In phase I, players play music in any format
    - » When SDMI watermarked content is detected, users are asked to upgrade to a Phase II device

# SDMI Licensed Compliant Module Architecture




PD Portable Device
PM Portable Media

# The SDMI Challenge

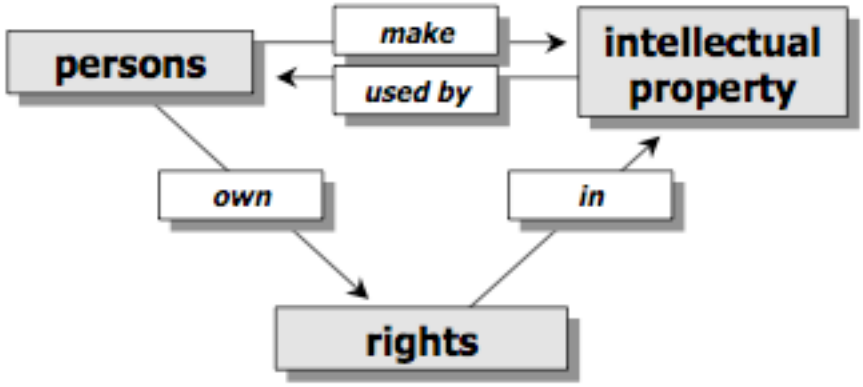
- 2000: SDMI technology evaluation for Phase II
  - Open call for proposals from technology vendors
  - Public challenge (“Hack SDMI”)
- Team from Princeton University around Edward Felten:
  - Successfully cracked most of the proposed technologies and was confident of being able to crack all
  - RIAA prohibited publication of paper on these results (Information Hiding Workshop, February 2001), using legal measures based on DMCA
  - After heavy media coverage, paper finally was presented at USENIX symposium (August 2001)
- Last statement (from www.sdmi.org):
  - “Based on all of the factors considered by the SDMI plenary, it was determined that there is not yet consensus for adoption of any combination of the proposed technologies. Accordingly, as of May 18, 2001 SDMI is on hiatus, and intends to re-assess technological advances at some later date.”
  - Since several years now, SDMI Web address is unreachable...

# MPEG-21

- "Normative open framework for multimedia delivery and consumption for use by all the players in the delivery and consumption chain"
  - www.chiariglione.org/mpeg/standards/mpeg-21/mpeg-21.htm
  - Currently (2009) still under construction
- Users: Covers content providers and consumers
  - In principle, all operations on content available to all users
- Digital Item:
  - Definition non-trivial for dynamically changing content (e.g. scripting)
  - Precisely defined in MPEG-21 Part 2: Digital Item Declaration (DID)
  - Identification and classification of Digital Items (MPEG-21 Part 3)
- Intellectual Property Management and Protection (IPMP)
  - Interoperable framework for IPMP defined in MPEG-21 Part 4
  - Rights Expression Language (REL) defined in MPEG-21 Part 5
    - » Mainly based on XrML
  - Rights Data Dictionary (RDD) defined in MPEG-21 Part 6
    - » Mainly based on <indecs>

# Rights Data Dictionary (RDD)

- Rights Management Systems differ in their terminology schemes
- Rights management is combined with terminologies from other areas
  - E.g. domain-specific terminologies, financial terminologies, ...
- *Rights Data Dictionary*:
  - Provides a general structure of terms ("*rights metadata"*)
    - » <indecs> rdd: Verbs and Genealogies
  - Is open to integration of new terminologies
    - » Including "mix and match", e.g. several terminologies in one expression
  - Transformations between schemes
    - » Providing semantic relations between different schemes
- Similar to ontology languages, e.g. in the context of "Semantic Web"

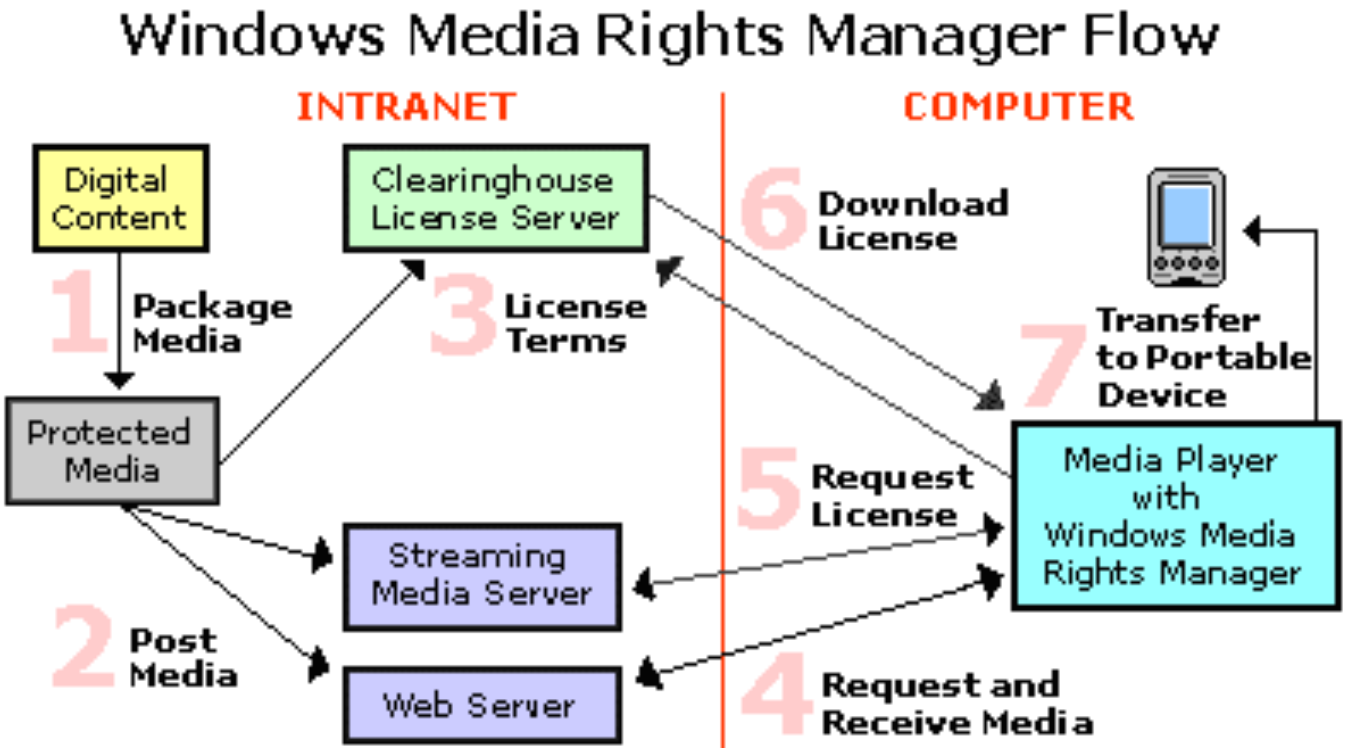



rightscom.com, <indecs> paper

# Pioneers of DRM

- InterTrust
  - "Electronic Publishing Resources" (1990-1997) did research in DRM base technology and filed many important patents
  - 1997: Name change to "InterTrust", marketing an end-to-end DRM-based publishing solution
  - 1999-2001: DRM products, many partnerships
  - 2004: $440 million deal with Microsoft on patent rights
- IBM infoMarket
  - 1994–1997 product targeted at an electronic marketplace which facilitates communication among independent sellers and buyers
  - Bases on original "superdistribution" idea
    - » "Cryptolopes" (Jeff Crigler) enabling distributed components to securely meter their usage and to initiate billing
    - » "Plug-N-Publish" toolkit for publishers (1995)
  - 1997 abandoned by IBM

# Microsoft Windows DRM




- DRM built into recent versions of Windows Media Player
- "Janus" architecture addresses also portable devices

# Apple FairPlay

- *iTunes Store* sells digital media in DRM-protected (encrypted) form
  - ".m4p" files: Protected MPEG-4 AAC files
  - MPEG-4 standard provides for "hooks" to be used by DRM
  - Apple encryption is proprietary ("AES CBC")
- Relatively loose rights regulations:
  - Files may be used on a certain number of "authorized" devices
- Principles:
  - Identification of computer, obtained by hashing various local data
  - Central server checks authorization based on computer ID and sends decryption key which is stored locally in encrypted form dependent on computer ID
- Since January 2009:
  - music files are sold without DRM protection
  - DRM is still used for video files

# Digital Cinema DRM

- Digital Cinema Initiative (DCI):
  - Standards for distribution of digital movies to movie theatres
- Distribution format (MXF):
  - Encrypted video content (using AES-128)
- Security Management at movie theatre:
  - Decryption keys transferred separately (Key Delivery Message KDM)
  - Keys are restricted in time and bound to a specific playback device
  - Trust infrastructure among devices
  - Theatre-internal links are encrypted
  - "Forensic Marking"
    - » Watermarking, individual marks per show
  - Extensive logging
- "Control lightly, audit tightly"

# Beyond DRM: Alternative Proposals

- Electronic Frontier Foundation (EFF): www.eff.org
- John Perry Barlow (former lyricist for the *Grateful Dead)*: The economy of ideas, *Wired* Magazine, Issue 2.03, March 1994

  www.wired.com/wired/archive/2.03/economy.ideas.html
  - Information wants to be free
  - Economy of information is different to economy of tangible goods:
    - » Value is in *familiarity* and *timeliness*, not scarcity
    - » Economy of relationship (real-time performance, services)
- Voluntary Collective Licensing
  - Flat rate for media sharing over the Internet (e.g. 5 €/month)
  - Paying the flat rate makes unlimited file sharing legal
  - Money is divided according to usage statistics and distributed back to artists (similar to ASCAP/BMI/GEMA system for radio broadcasts)

    http://www.eff.org/share/collective_lic_wp.php
- Music industry apparently moving towards less strict DRM systems
- Basic idea: ***Ethical*** principles, no "brute-force" technology approach