6 Digital Rights – Definition and Management

6.1 Media Rights

6.2 Rights Models

6.3 Principles of Encryption-Based DRM Systems

6.4 Watermarking

6.5 DRM Standards and Selected Commercial Solutions

Literature:

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

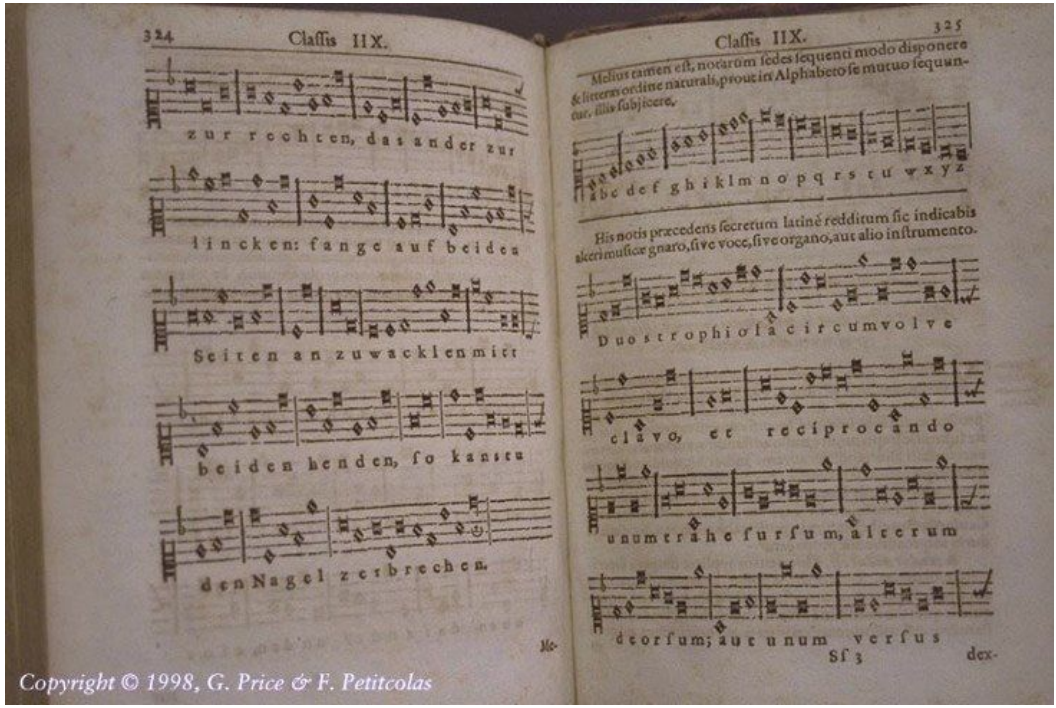
Wenjun Zeng, Heather Yu, Ching-Yung Lin: Multimedia Security Technologies for Digital Rights Management, Academic Press 2006

Hiding Secret Messages

- Herodot (440 BC) reports:
  - Demaratus hiding a message on a wooden tablet below the wax coating
- Histiaeus (6th century BC):
  - Shaved the head of a slave and tattooed a message on his head
- Gaspar Schott, *Schola Steganographica* (1665):
  - Sheet music as a representation of text
- Writing a concealed message: "Steganography"

http://hareenlaks.blogspot.de/2011/04/history-of-steganography

http://www.petitcolas.net/steganography/steganographica/



Watermarking

- Watermark:
  - Conveys information about a document
  - Keeps the document readable
  - Inextricably bound together with the document
- Recognizable vs. hidden watermarks
- Universal vs. individual watermarks

Manfred Sauke / Wikipedia

http://watermark factory.com

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
- Fingerprinting
- Copy control
- Broadcast monitoring
- Unauthorized modification detection: Using fragile watermarks
- Annotation and indexing
- Link media: Embed machine-readable information in images
- Medical applications
- Covert communications: Transmitting hidden data

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

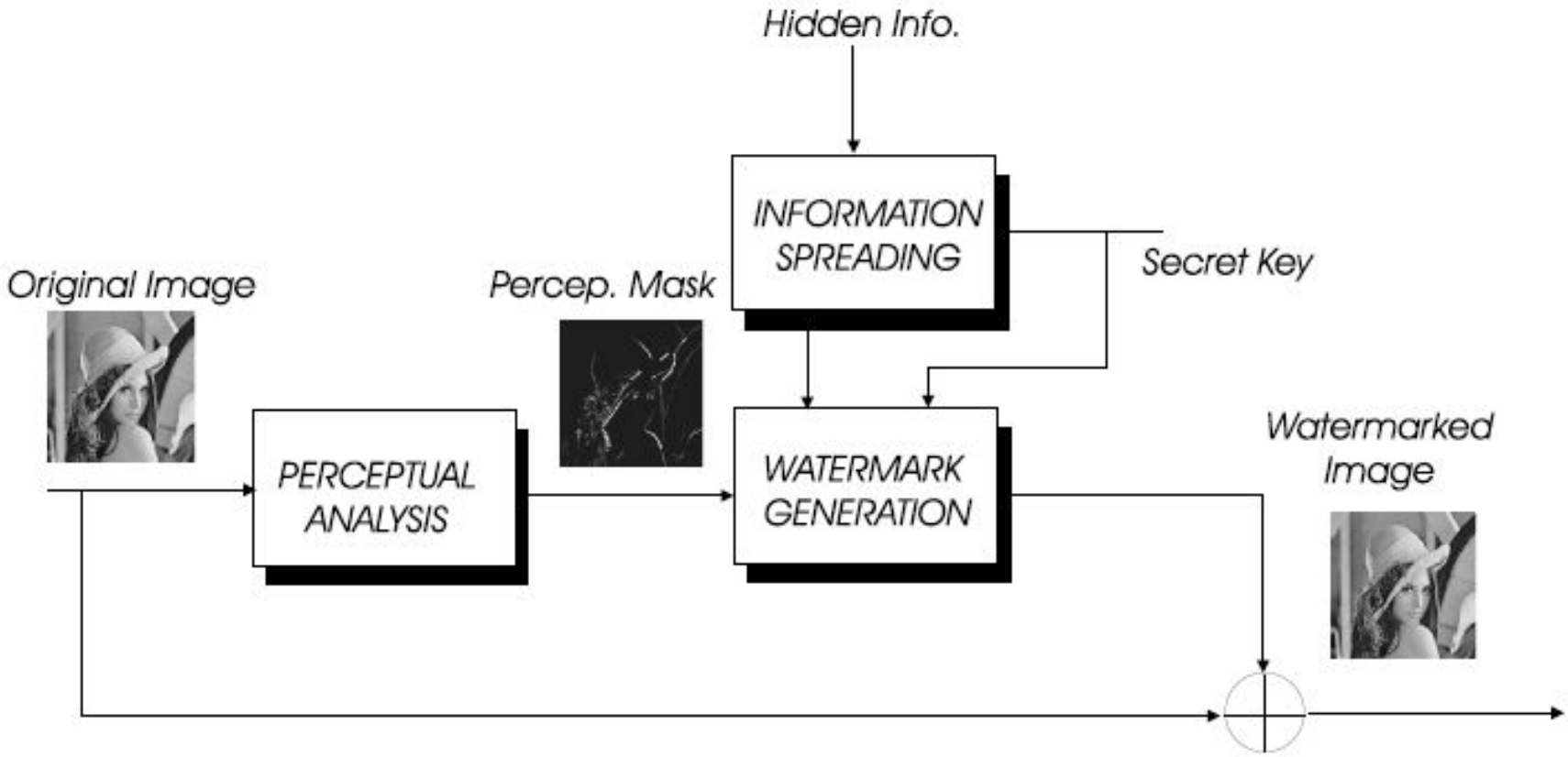


Figure 1: *Watermark insertion unit*

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

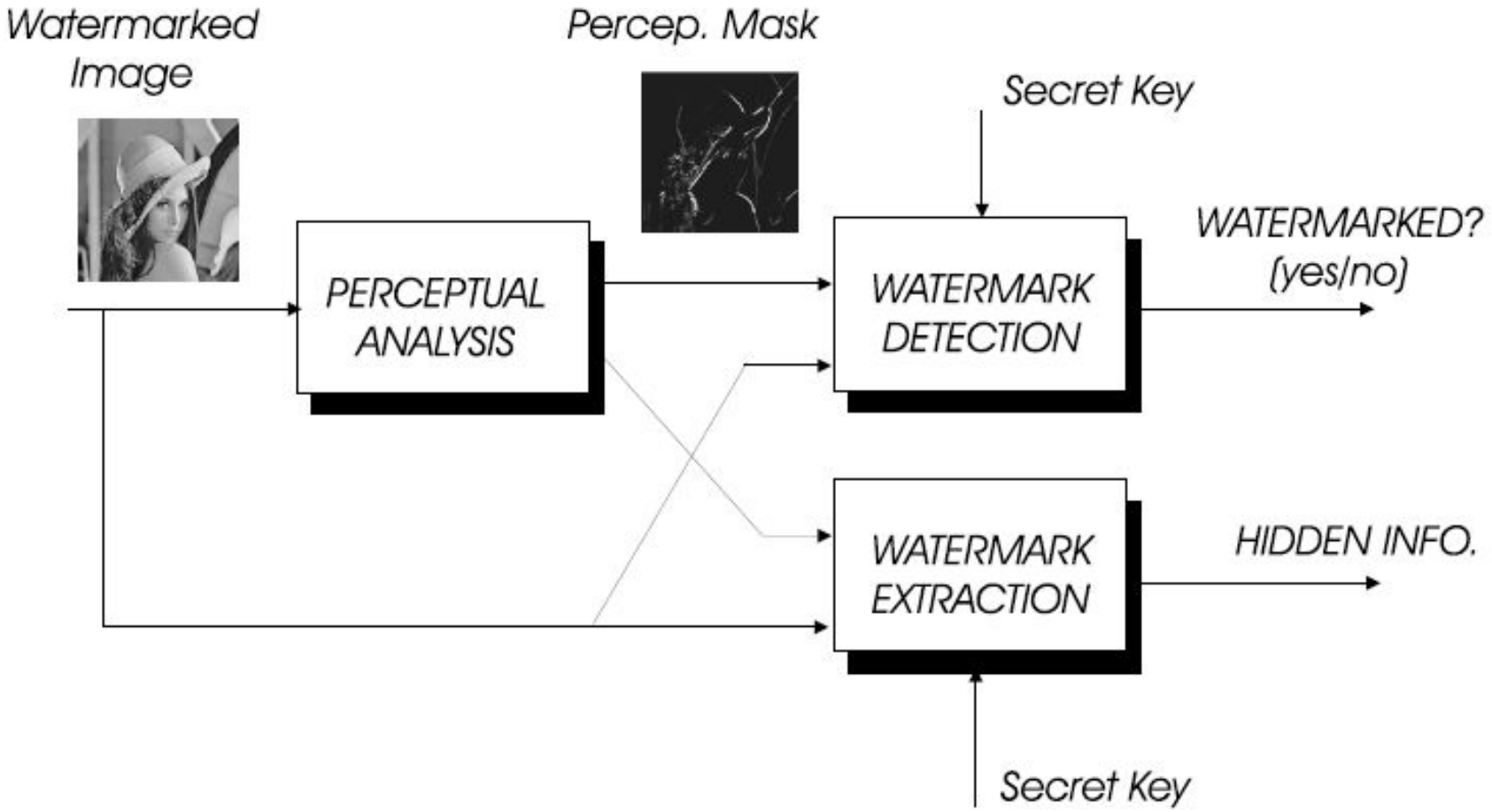


Figure 4: *Watermark detection and extraction unit*

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
    - » 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
- Create pseudo-random sequence of pairs of locations in picture
  - Using a seed value for random generator (same for encoder&decoder)
- 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
- Principle applicable also to audio

Bender/Gruhl/Morimoto/Lu,
IBM Systems Journal, 1996

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, including mid band frequencies
- 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)

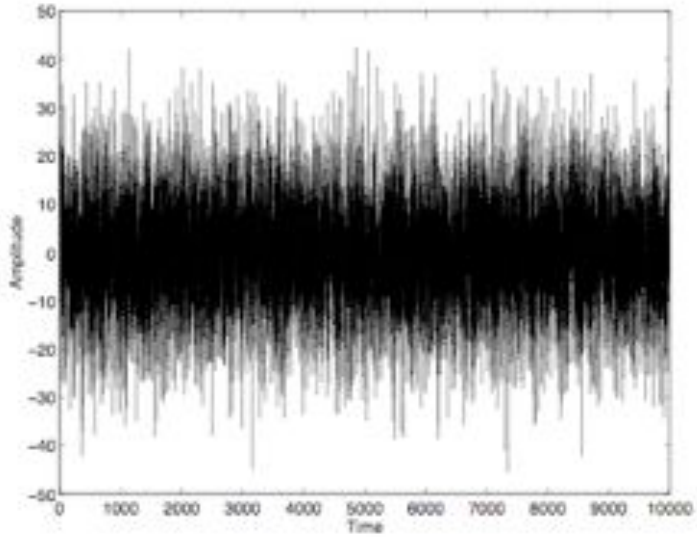


Image: O'Ruanaidh/Pereira

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

6 Digital Rights – Definition and Management

6.1 Media Rights

6.2 Rights Models

6.3 Principles of Encryption-Based DRM Systems

6.4 Watermarking

6.5 DRM Standards and Selected Commercial Solutions

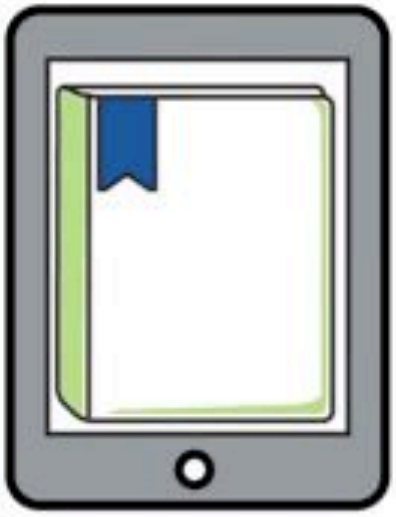
Literature:

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

Commercial Watermarking: DigiMarc

digimarc.com

Commercial Watermarking: DigiMarc



digimarc.com

Watermarking as Bar Code Replacement

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.

verance.com

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

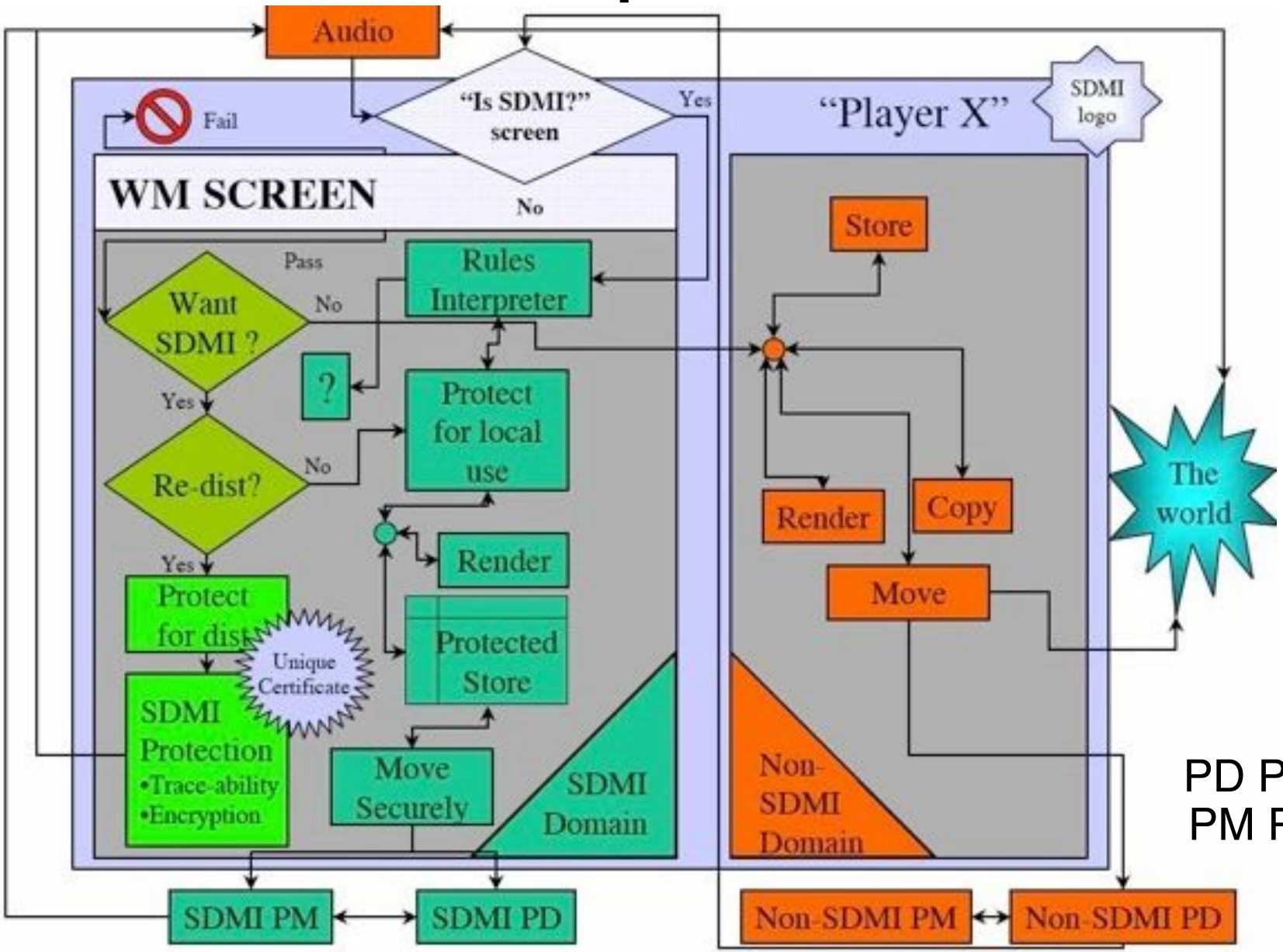
Intellectual Property Identification: DOI

- 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 and encryption
  - 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



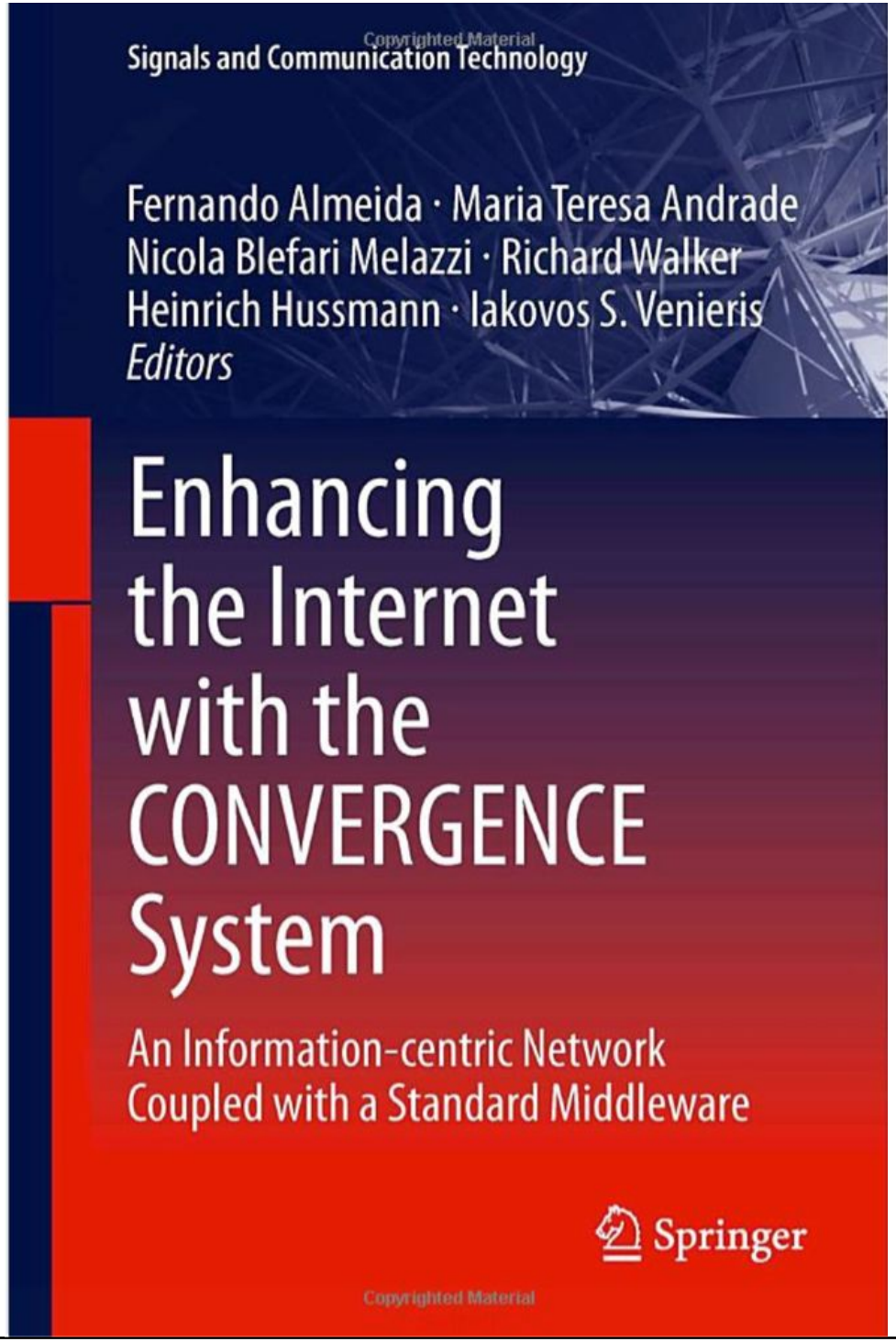
PD Portable Device
PM Portable Media

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)
- SDMI has disappeared from the public in May 2001

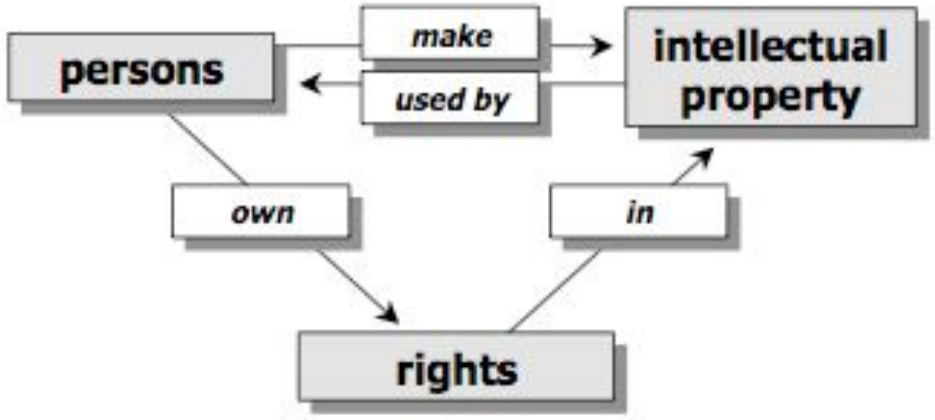
MPEG-21

- "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
  - Parts are ISO standard, work currently (2014) still ongoing
- ***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
  - Rights Data Dictionary (RDD) defined in MPEG-21 Part 6
- For recent work see:
  Almeida et al. (eds.): Enhancing the Internet with the CONVERGENCE system, Springer 2014


Copyrighted Material
Signals and Communication Technology
Fernando Almeida · Maria Teresa Andrade
Nicola Blefari Melazzi · Richard Walker
Heinrich Hussmann · Iakovos S. Venieris
Editors
Enhancing the Internet with the CONVERGENCE System
An Information-centric Network Coupled with a Standard Middleware
Springer
Copyrighted Material

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"

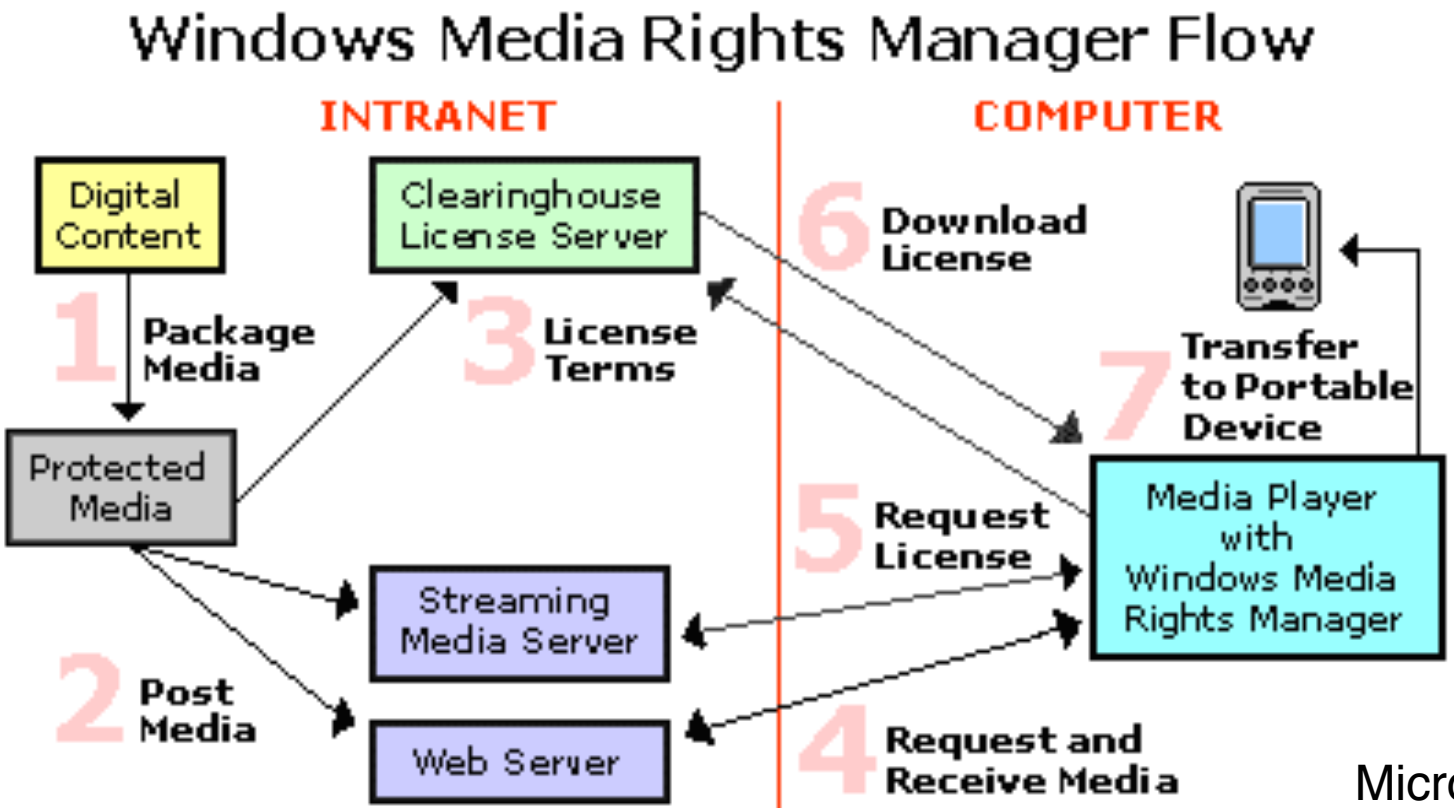


rightscom.com, <indecs> paper

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 Media DRM



Microsoft, 2004

- DRM built into Windows Media Player (“Windows Media DRM 10”)
- Supported in Windows Media Foundation (e.g. in Windows 8)

Apple FairPlay

- *iTunes Store* sells digital media in DRM-protected (encrypted) form
  - Old audio ".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
  - Identification of computer, obtained by hashing various local data
- Steve Jobs, 2007 ("Thoughts on Music"):
  - "DRMs haven't worked, and may never work, to halt music piracy."
- Since January 2009:
  - Music files are sold on iTunes Store without DRM protection
  - DRM is still used, e.g. for video files and eBooks
    - » Circumvention software exists but is under heavy legal attack by Apple

UltraViolet

- Digital Entertainment Content Ecosystem (DECE), since 2008
  - Consortium of film studios, consumer electronic manufacturers, hardware vendors, system integrators, DRM vendors
  - e.g.: Sony, Warner Bros., NBCUniversal, Paramount, Samsung, Panasonic, Netflix, LoveFilm, Cisco, HP, Rovi,…
- Standard “rights locker” service
  - to be combined with cloud streaming and download services
- Interoperable Common File Format (CFF)
  - based on MPEG-4 container format, using H.264/AVC video
- Interoperable DRM
  - “Common Encryption” technology ensures interoperability of five DRM systems:
    - » Google Widevine DRM, Marlin DRM, OMA CMLA, MS PlayReady, Adobe Flash Access 2.0
- Rolled out 2012/13, growing support in 2014
  - e.g. Amazon, Flixster

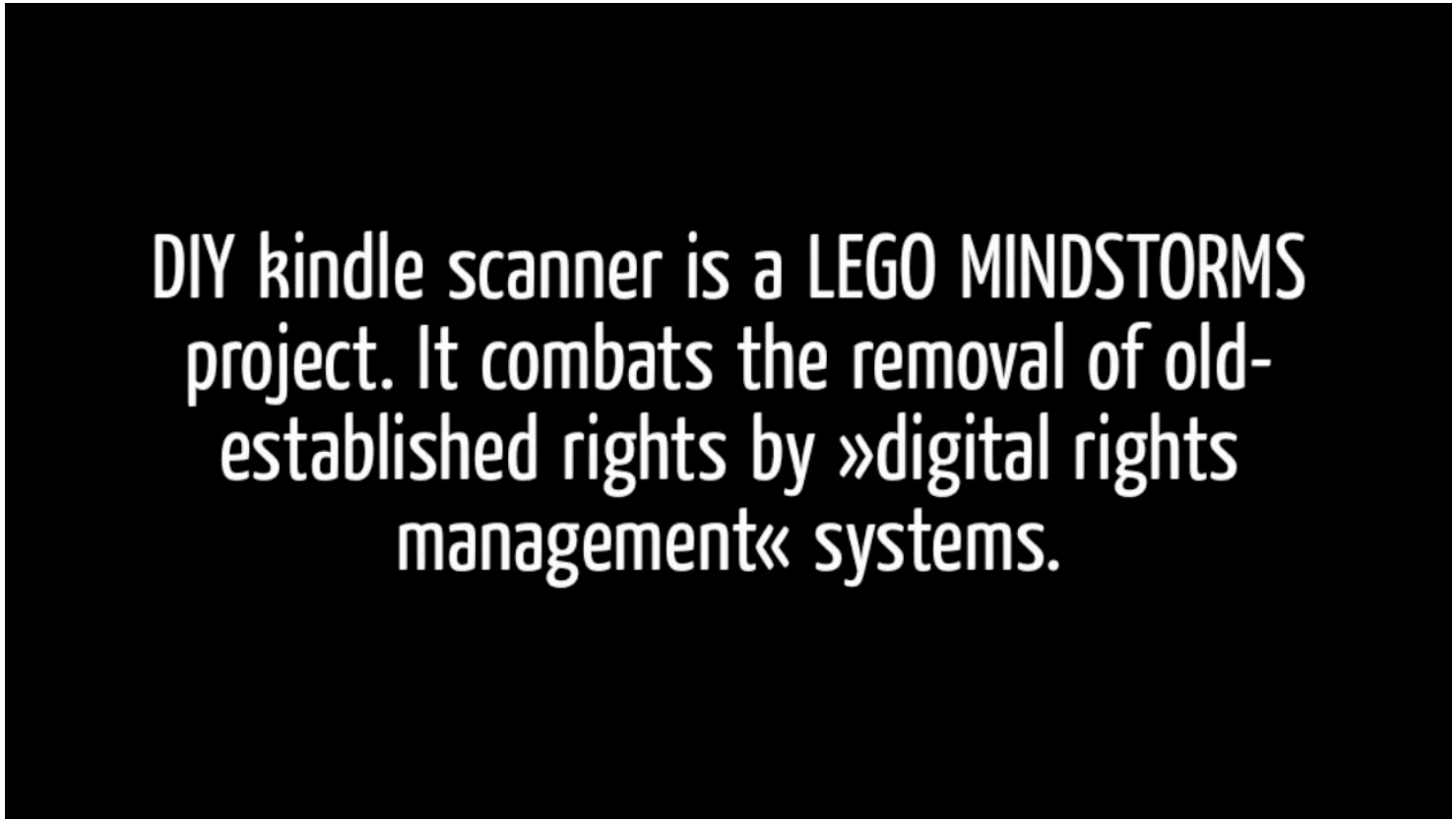
www.uvvu.com

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"

DRM Systems for E-Books

- Adobe Digital Editions
  - Flash-based reader for digital publications (PDF, XHTML, ePUB)
  - Content provided and encrypted through “Adobe Content Server”
  - Proprietary ADEPT DRM (Adobe Digital Experience Protection Technology)
- Amazon Kindle



Peter Purgathofer, Wien (Source: vimeo)

Beyond DRM: Alternative Proposals


Source: Wikipedia

- 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
- Basic idea: ***Ethical*** principles, no "brute-force" technology approach