Profili tecnologici relativi all'esercizio del diritto d'autore e dei diritti connessi e dispositivi tecnologici di controllo dell'accesso ai prodotti culturali

Goffredo Haus
DICO - Dipartimento di Informatica e Comunicazione
Università degli Studi di Milano

Contenuti

- Introduzione concettuale
- Duplicazione
- Cessione
- Interscambio
- Interventi protettivi a priori
- Interventi protettivi a posteriori
- Tecnologie DRM
- Prospettive
- Riferimenti

Elementi costituenti i prodotti culturali

- Metadati
- Dati
- Informazioni
- Ontologie

Prodotto culturale digitale come bene “immateriale”

Il prodotto culturale digitale è multimediale (testo, audio, immagine, video) ed è un bene “immateriale”, completamente:

- codificabile
- conservabile
- trasmissibile
- riproducibile
- cedibile

Materializzazione del prodotto digitale

Il prodotto culturale digitale acquista aspetti di materialità per la conservazione (memorie), per la trasmissione (reti) e in generale per la riproduzione e le cessione.

Prodotti “immateriali” e “materiali”

- Prodotti “immateriali”:
  - metadati, dati, informazioni, ontologie
    - simbolici (codici testuali e non)
    - subsimbolici (segnali)

- Prodotti “materiali”:
  - canali mediali
    - temporali (memorie, supporti)
    - spaziali (canali di trasmissione, reti)

Codifica dei prodotti culturali

- Codifiche non compresse
- Codifiche compresse senza perdita di informazione (lossless)
- Codifiche compresse con perdita di informazione (lossy)
- Codifiche con pluralità di canali mediali
- Codifiche strutturate
  - modelli di analisi (coder)
  - modelli di sintesi (decoder)
- Formati di interscambio
- Formati per la fruizione e l’interazione
- Unità di misura della codifica

Trasmissione di prodotti culturali

- Canali spaziali
  - reti cablate (internet, digitale terrestre, intranet)
  - reti satellitari
  - broadcasting via etere
- Canali temporali
  - supporti di memoria di massa fissi o rimovibili
- Unità di misura dei canali spaziali e temporali
  - larghezza di banda
  - capacità delle memorie

Supporti per prodotti culturali

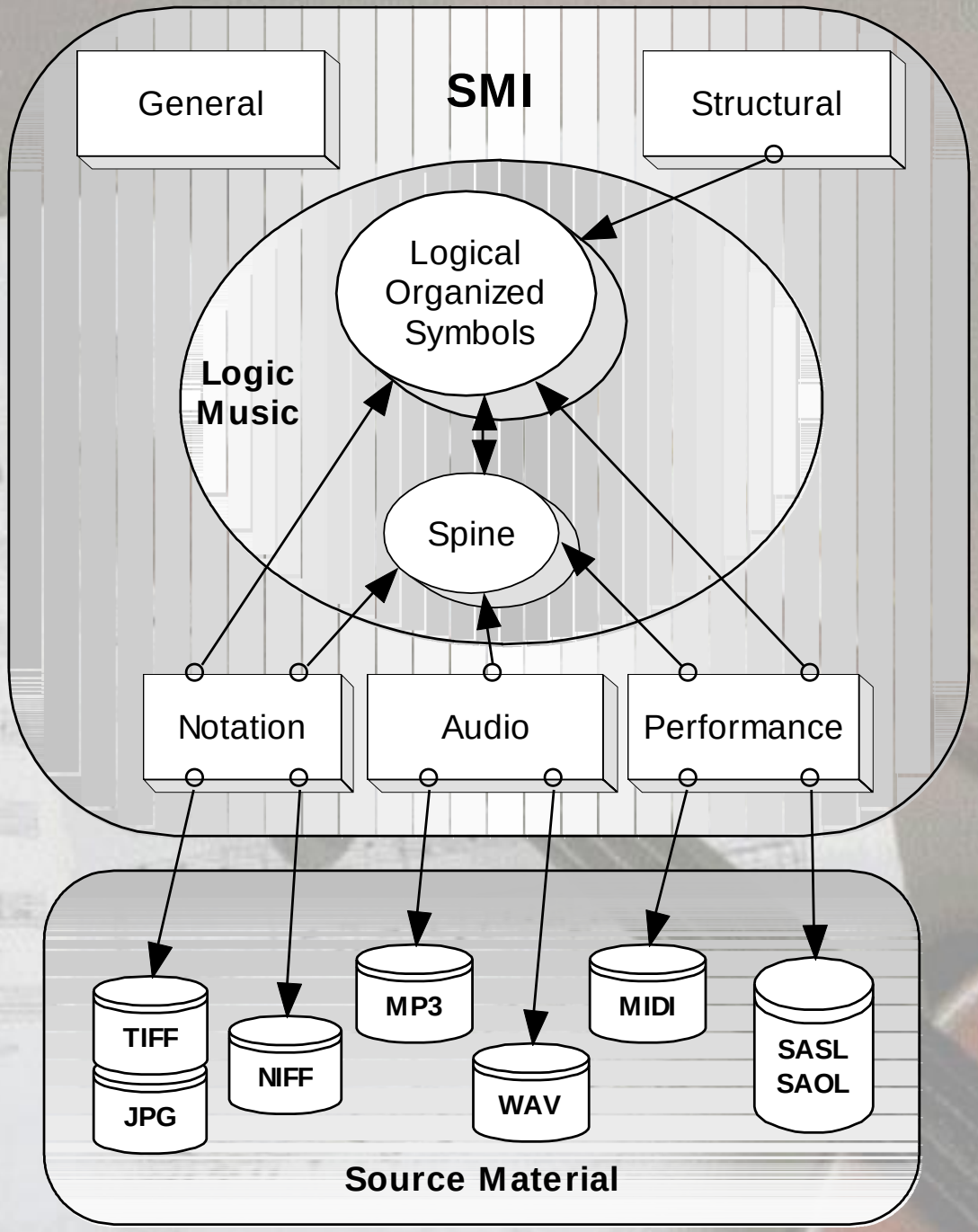
- Supporti specifici per un canale mediale
- Supporti general purpose

- Supporti registrati
- Supporti registrabili una o più volte

Il caso musicale

Elementi costituenti i prodotti musicali

- Metadati
  - anagrafici, editoriali, tecnici, economici, archivistici
- Dati per ogni livello di astrazione
  - strutturali (compositivi), testuali (partiture), interpretativi, strumentali, audio
- Informazioni
  - forme, strutture, note, melodie, accordi, interpretazioni, timbri, pan & mix, suoni
- Ontologie
  - caratterizzazioni oggettive, modelli cognitivi, reti di relazioni semantiche orientati all'organizzazione, al reperimento e alla fruizione del prodotto o di parte di esso



Esempio: metadati audio

- ID3v1: metadati MP3 (o altri formati come AAC), ultimi 128 byte
- ID3v2: evoluzione di ID3v1, metadati anteposti al bitstream MP3, dimensione variabile strutturata a chunk
- XING e LAME: metadati specifici degli omonimi codec MP3, usabili in alternativa o in congiunzione con ID3
- XML:
  - MPEG-7 (ISO/IEC 15938)(XML): "Multimedia Content Description Interface", set di Description Tools XML-based per la descrizione simbolica di contenuti multimediali audio-video (AV)
  - MPEG-A (XML): tentativo MPEG per integrazione standard (MP3 per la codifica audio, ID3 codificati in MPEG-7 i metadati, MP4 come contenitore multimediale
  - IEEE SA “MX” PAR1599: gruppo di lavoro per la definizione di uno standard orientato alla codifica dell’informazione multistrato, interattiva e interoperabile
- CD-Text: estensione del Red Book che integra metadati all'interno della codifica CD-DA

Esempio: dati audio

- PCM, DPCM, ADPCM, DM, … (tecniche di codifica)
- *.WAV, *.AU, *.AIFF, CD-DA, … (formati di codifica)
- MP3, AAC, WMA, OGG, GSM 06.10, … (formati di compressione lossy)
- SHN, FLAC (Free Lossless Audio Codec) , MPEG4 ALS (Audio Lossless Coding), Lossless iPod, Lossless WMA, … (formati di compressione lossless)
- MPEG4 SASL & SAOL, Csound, … (linguaggi di codifica per modelli)

Evoluzione del prodotto musicale

- dal prodotto:
  - costituito da dati propri di uno o solo alcuni livelli di astrazione
  - che permette la fruizione passiva o scarsamente interattiva di informazioni
  - prevalentemente fruibile mediante uno o solo alcuni canali mediali
- al prodotto:
  - costituito da dati propri di molti o tutti i livelli di astrazione
  - dotato di interoperabilità tra i diversi livelli di astrazione
  - che permette la fruizione fortemente (inter)attiva di informazioni
  - fruibile mediante molti o tutti i canali mediali

Duplicazione del prodotto culturale

- Immateriale
  - duplicazione della codifica
    - copie di file
    - copie di stream (sniffing)
- Materiale
  - duplicazione del supporto
    - tra supporti omogenei o eterogenei
    - mantenendo o degradando la codifica
    - masterizzazione (s. ottici) o copia (s. magnetici)

Duplicazione per copia personale

Duplicazione immateriale o materiale di codifiche di prodotti culturali per ottenere copie personale

Può essere fatta una o più volte

Può essere fatta avendone il diritto o meno

Cessione del prodotto culturale

- Cessione
  - monodirezionale
    - gratuita
    - a pagamento (vendita)
      - transazione
      - abbonamento
      - licenza
    - a pagamento (fruizione audiovisuale)
    - a pagamento (tempo e banda di connessione)
  - bidirezionale (interscambio)

Cessione “immateriale”

- Download di file
  - internet
  - intranet
  - via satellite
  - broadcasting
  - mobile services
- Licenza d’uso di codifiche
- Password per accedere a prodotti culturali
  - online
  - offline

Cessione “materiale”

- supporti stampati
- supporti generati “on demand”

Interscambio di prodotti culturali

- Prestito del supporto
- Peer-to-Peer (P2P)
- On Demand
- Mobile Services
  - SMS
  - MMS

Copyright e copyleft

- Relazione tra prodotti in regime di copyright e prodotti in regime di copyleft
- Copyright del prodotto materiale
- Copyright del prodotto immateriale

Strumenti di gestione e protezione

- Tecnologie sicure per i canali mediali (spaziali e temporali)
- Interventi a priori
- Interventi a posteriori
- Controllo delle transazioni di distribuzione, acquisizione, fruizione
- Tecnologie DRM per la gestione e protezione immateriale, materiale ed economica del prodotto culturale

Casi esemplari musicali

P2P Legali – Top Ten

http://www.top-rated-mp3-sites.com/limitedtimeoffer.html - Giugno 2004

1. MP3Downloading – www.mp3downloading.com
2. NetMP3Download – www.netMP3Downloads.com
3. KLiteGeneration – www.KLiteGeneration.com
4. KliteTK – www.KliteTK.com
5. FileSharingCenter – www.FileSharingCenter.com
6. KLitePro – www.KLitePro.com
7. MP3Advance – www.MP3Advance.com
8. K-LiteGold – www.K-LiteGold.com
9. MP3EBook – www.MP3EBook.com
10. KazaaLite – www.KazaaLite.nl

P2P Illegali – Top Twenty

http://www.download.com/sort/3150-2166_4-0-1-5.html?

1. BitTorrent 3.4.2
2. BearShare 4.6
3. iMesh 4.5 build 150
4. Warez P2P 2.6
5. Morpheus 4.6.1
6. Ares Galaxy 1.8.1
7. LimeWire 4.2
8. Freenet 0.5.2.8
9. Ares Lite 1.81
10. WinMX 3.53
11. eMule 0.44d
12. Grokster 2.6
13. BearShare Lite 4.6
14. eMule++ 1.0.6
15. iMesh 5 multinetwork beta 5.0.0.223
16. Piolet 1.05
17. Kazaa Speedup Pro 2.7.8
18. Kiwi Alpha 1.4.5
19. Soulseek 152
20. Songoog 2.2.4

P2P: il sistema Freenet

Applicazione SW per P2P che permette la pubblicazione, la replicazione, la ricerca ed il download dei dati, proteggendo l'anonimità di fruitori e fornitori.
Caratteristiche:

- nessun sistema centralizzato di ricerca in broadcasting, indicizzazione e localizzazione dei file è stato implementato
- i dati vengono deframmentati e criptati tra i vari nodi del sistema - tra loro paritetici ed indipendenti - e duplicati in nodi prossimi a quello del richiedente; in tal modo, diviene inapplicabile un algoritmo di tracking del traffico della rete volto a scoprire l'origine e la destinazione dei file trasmessi.

Il SW è sottoposto a licenza GNU.

website: http://freenetproject.org/

Music on Demand:
il caso russo e la licenza #LS-3M-03-79

Alcuni siti internet russi rendono possibile il download di brani a prezzi bassissimi senza oltrepassare i limiti della legalità; i materiali sono infatti disponibili per la distribuzione secondo la licenza della Russian Multimedia Internet Society e l'intera attività è soggetta alla legge della federazione russa sul copyright. Nei siti viene chiaramente sottolineato che il servizio è proibito se in conflitto con la legislazione del paese di appartenenza dell'utente e che il materiale è disponibile solo per uso personale.

Protocolli Sicuri: SSL, S-HTTP

- **SSL**: Secure Sockets Layer, protocollo sviluppato da Netscape per trasmettere documenti personali in internet; SSL usa una chiave privata per criptare i dati da trasferire; sia Netscape Navigator che Internet Explorer supportano SSL; molti siti gestiscono dati confidenziali (come i numeri delle carte di credito) mediante SSL; per convenzione, i siti che richiedono la connessione SSL iniziano con *https:* invece di *http*:

- **S-HTTP**: estensione del protocollo HTTP che supporta l'invio sicuro di dati nel World Wide Web; non tutti i browser web supportano S-HTTP.

- **SSL** vs **S-HTTP**: SSL e S-HTTP hanno caratteristiche molto diverse e possono essere usati anche in combinazione; mentre SSL è pensato per connettere in modo sicuro due computer, S-HTTP è pensato per mandare messaggi personali in modo sicuro; entrambi i protocolli sono stati sottoposti all'Internet Engineering Task Force (IETF) per essere riconosciuti come standard.

- Fonte: http://www.webopedia.com/TERM/S/SSL.html

Interventi protettivi a priori

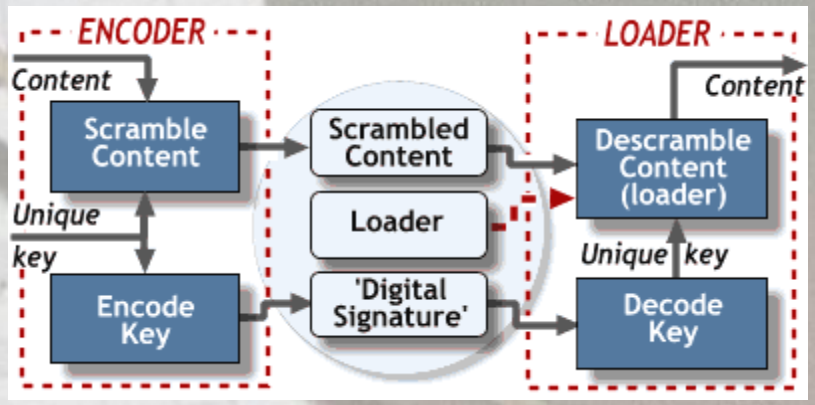
- Codici per l'identificazione
- Protezione del supporto
  - Inibizione dell'accesso
  - Inibizione della copia
- Watermarking (marcatura per identificazione a posteriori)
- Fingerprinting ("impronta" che identifica il prodotto culturale, ottenuta dai suoi stessi contenuti)
- Encrypting (crittografia, codifica criptata)
- Contenuti distribuiti
- "Intossicazione" dei sistemi P2P illegali

Codici per l'identificazione

- DOI (Document Object Identificator)
- ISRC (International Standard Recording Code)
- ISMN (International Standard Music Number)
- URL (Uniform Resource Locators)
- URN / URI (Uniform Resource Name / Uniform Resource Identifier)
- ...

CD / DVD Protection

- Esistono moltissime tecnologie per la protezione dei supporti di massa
- Esse evitano:
  - uso e riproduzione impropria del prodotto
  - copia illimitata del bene digitalizzato
  - → problemi collaterali:
    - → problemi nel creare copia ad uso personale
    - → problemi con i vari tipi di player



- Un esempio significativo
  - openMG (Sony)
    - http://openmginfo.com/
    - http://www.copycontrolhelp.com

Un elenco esaustivo al link:
http://www.cdmediaworld.com/hardware/cdrom/cd_protections_protectcd.shtml

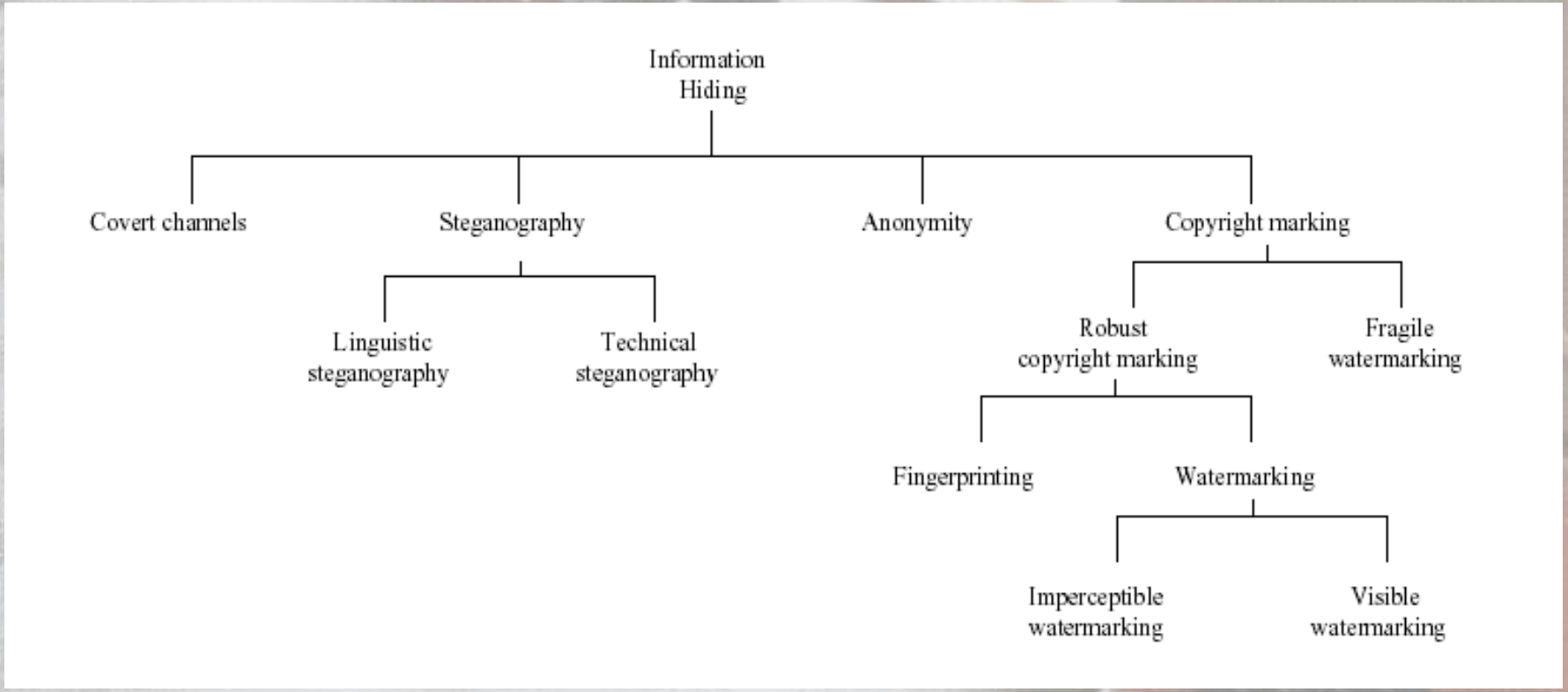
CD / DVD Protection

- CPSA (Content Protection System Architecture)
- L'obiettivo di CPSA è lo sviluppo di una piattaforma volta ad integrare le varie tecnologie audio/video, sia nel dominio analogico che digitale, tramite **watermarking**, **encrypting** e la definizione di **politiche** ad hoc per la gestione dei contenuti

- Link:
  - http://www.4centity.com/data/tech/cpsa/cpsa081.pdf
  - http://www.allformp3.com/dvd-faqs/111.htm

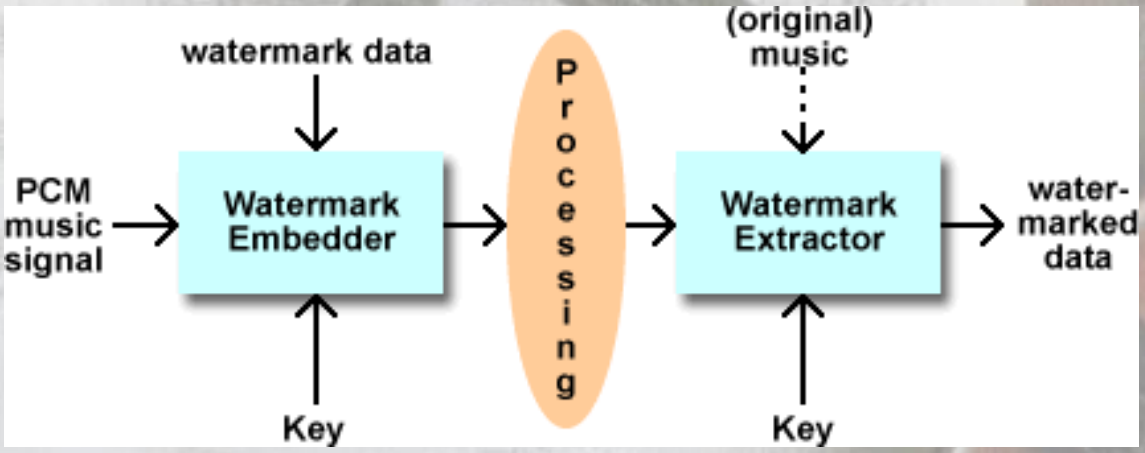
Watermarking

Il watermarking è una branca *dell'information hiding*, che raggruppa diverse discipline:



Audio Watermarking

- Consiste nell'inserire delle informazioni visibili o nascoste (il *watermark*) all'interno della traccia audio in modo da renderla riconoscibile ed identificabile
- se invisibile, il *watermark* deve risultare acusticamente impercettibile e tale da non modificare la durata del brano audio
- infine, il *watermark* deve essere tale da risultare riconoscibile anche dopo varie degradazioni del segnale audio



Audio Watermarking

- Principali applicazioni
  - Identificazione del proprietario
  - Controllo della distribuzione e diffusione
  - Controllo delle copie
  - Autenticazione
  - Embedding di “audio fingerprint”

- Principali parametri di un sistema di watermarking
  - **Robustezza** del sistema
  - **Trasparenza**, quanto impercettibile è il watermark
  - **Sicurezza**
  - **Complessità del sistema**
  - **Capacità**, quanti bit servono per descrivere un watermark

- Principali tecniche di watermarking
  - Tecnica additiva
  - Schemi basati su modulazione e quantizzazione
  - Tecniche di self-synchronizing

- Alcuni prodotti commerciali di watermarking e steganografia
  - AudioKey - http://www.homerecording.com/audiokey.html
  - Nabster (watermarking + fingerprinting) - http://www.cdfreaks.com/article/120
  - MP3Stego - http://www.petitcolas.net/fabien/steganography/mp3stego/index.html

Limiti dell'Audio Watermarking

- Oltre alla potenziale aggiunta di rumori acusticamente percepibili causati dall'introduzione dei watermark, le tecniche di watermarking si sono rivelate molto fragili agli attacchi
- Maggiori informazioni:
  - http://www.petitcolas.net/fabien/publications/ih98-attacks.pdf
- SDMI – Secure Digital Music Initiative rappresenta uno degli esempi più emblematici dell'inefficacia di questa tecnologia

SDMI – Secure Digital Music Initiative

- Obiettivo di SDMI
  - sviluppo di una piattaforma aperta e sicura per l'esecuzione, la distribuzione e l'archiviazione di musica digitale
  - capacità di supporto delle diverse tecnologie attualmente esistenti nel digital audio

- Caratteristiche SDMI
  - Open
  - Sicuro
  - Interoperabile
  - Semplice da usare
  - Facilmente aggiornabile
  - Testabile
  - Possibilità di supportare musica protetta e non protetta

- Tecnologia di protezione basata su tecniche di **watermarking**

- Riferimenti: http://ntrg.cs.tcd.ie/undergrad/4ba2.01/group10/SDMImain.html

SDMI Crack

- Il 6 settembre 2000 SDMI lanciò la sfida per validare il proprio sistema.
  - SDMI Challenge: http://www.sdmi.org/pr/OL_Sept_6_2000.htm
- Il sistema di watermarking presente in SDMI venne craccato quasi immediatamente dal team di ricerca di Princeton guidato dal Professor Edward Felton
  - Maggiori informazioni: http://www.cs.princeton.edu/sip/sdmi/faq.html
- Ci furono conflitti tra SDMI e Mr. Felton per il pagamento della “taglia” e la pubblicazione dei risultati
- Links
  - http://www.benedict.com/Digital/Internet/SDMI.aspx
  - http://ntrg.cs.tcd.ie/undergrad/4ba2.01/group10/againstSDMI.html#whywillfail

Fingerprinting

- Parametri di un sistema di fingerprinting
  - Robustezza del sistema: capacità del sistema di riconoscere un segnale, anche se degradato
  - Dimensione del fingerprint
  - Affidabilità
  - Granularità: quantità di dati necessaria per estrarre un impronta digitale
  - Velocità di ricerca
  - Scalabilità del sistema

Audio Fingerprinting System

- La tecnologia di Audio Fingerprinting permette di identificare e riconoscere un brano musicale automaticamente
- La prima fase consiste nell'estrazione di una "impronta digitale" attraverso un'opportuna analisi del segnale. Tale impronta identificherà univocamente il materiale audio analizzato.
- Nella seconda fase, quella di monitoraggio, viene nuovamente analizzato il segnale ed estratta l'impronta digitale. Tale impronta viene confrontata con quelle ottenute nella prima fase e quando una corrispondenza viene trovata, il brano è stato identificato.

Audio Fingerprinting System

- L’impronta digitale estratta nella prima fase può essere:
  - Memorizzata in un database ad hoc
  - Inclusa all’interno della traccia stessa tramite tecniche di watermarking
    - http://www.idiap.ch/~paiement/references/to_read/music/fingerprinting/its2002-egomez.pdf
  - Rappresentata in XML con opportuni sistemi di codifica
    - MPEG-7 “Audio Framework” - http://ismir2001.ismir.net/pdf/allamanche.pdf

Audio Fingerprinting System

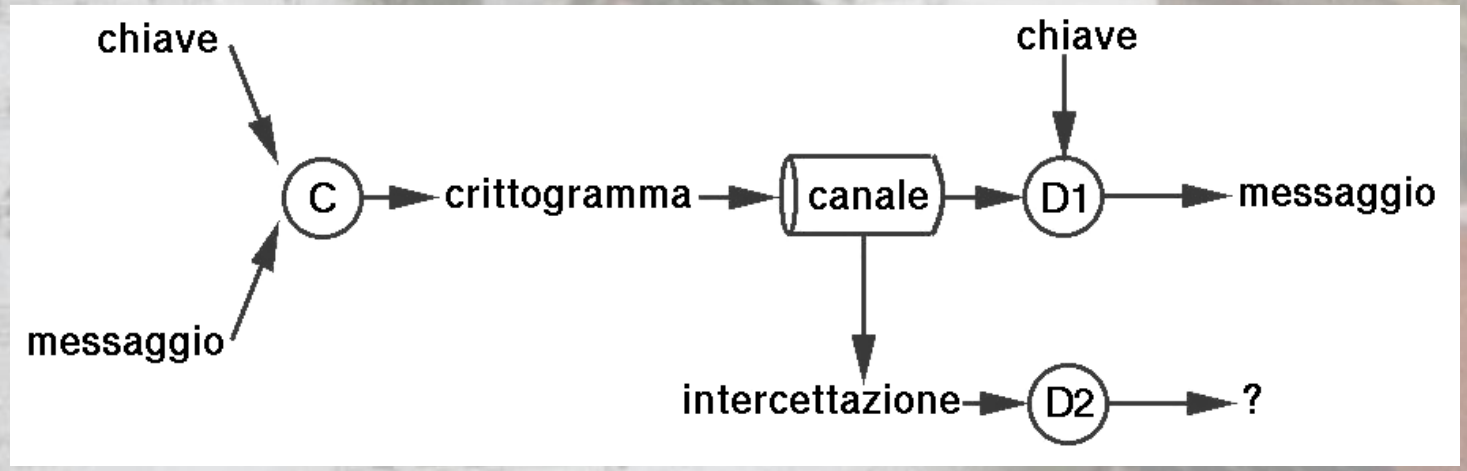
- Principali applicazioni:
  - Monitoraggio di canali broadcasting (radio, TV, ecc.) sia a fini statistici che per la ripartizioni dei diritti
  - Filtro per canali di scambio P2P
  - Organizzazione di librerie digitali automatiche

- Alcuni prodotti esistenti:
  - Philips - http://www.research.philips.com/initiatives/contentid/audiofp.html
  - IDIOMA - http://www.idiomasolutions.com/Products/Products.htm

Crittografia

- In un sistema crittografico, il dato in chiaro viene trasformato, secondo regole, nel dato cifrato o crittogramma; tale operazione si chiama cifratura

- Il destinatario legittimo, in quanto possessore di chiave decifra il crittogramma e riottiene il testo in chiaro



Crittografia

- Esistono due classi di algoritmi:
  - **simmetrici** (o a chiave segreta): utilizzano la stessa chiave per cifrare e decifrare (o la chiave di decifrazione è facilmente ottenibile a partire da quella di cifratura)
  - **asimmetrici** (o a chiave pubblica): utilizzano due chiavi diverse e la chiave di decifrazione non può essere ricavata a partire dalle informazioni contenute nella chiave di cifratura

Esempio di sistema crittografico: DES

- Data Encryption Standard, crittosistema tra i più usati al mondo
- Fu sviluppato alla IBM, come evoluzione di un crittosistema più antico, LUCIFER, e fu pubblicato sul Registro Federale il 17 Marzo 1975. La definizione di DES è riportata nel Federal Information Processing Standards Publication 46, del 15 Gennaio 1977
- Viene revisionato con frequenza quinquennale da NBS
- Ha trovato applicazioni significative nelle transazioni bancarie: veniva utilizzato per codificare i PIN (Personal Identification Number) e le transazioni su conto corrente per operazioni da ATM (Automated Teller Machine). E' stato inoltre largamente impiegato da organizzazioni governative americane, quali il Department of Energy, il Justice Department ed il Federal Reserve System

Esempio di sistema crittografico: BlowFish

- **BlowFish** è un cifrario simmetrico a blocchi sviluppato da Bruce Schneier.
- Questo algoritmo utilizza varie tecniche tra le quali la rete Feistel, le S-box dipendenti da chiavi e funzioni F non invertibili che lo rendono, forse, l'algoritmo più sicuro attualmente disponibile.
- Le chiavi utilizzate sono di dimensioni variabili fino ad un max. di 448 bit; i blocchi utilizzati per la cifratura sono di 64 bit.
- Non si conoscono al momento tecniche di attacco valide nei suoi confronti. E' considerato uno degli algoritmi di cifratura a blocchi più veloce (risulta più veloce del DES e dell'IDEA).
- Blowfish non è brevettato ed è di dominio pubblico.
- Viene ampiamente impiegato in applicazioni di music-on-demand.

Interventi protettivi a posteriori

Riconoscimento dell'avvenuto accesso ai prodotti culturali

- Analisi archivi server provider (URL, URN / URI, LOG files, ecc.)
- Ispezioni su canali spaziali (reti) mediante identificazione run-time di spider, sniffer, …

Riconoscimento del possesso di prodotti culturali

- Riconoscimento di watermark
- Uso di fingerprinting
- Ispezioni su canali temporali (archivi e supporti)

Valutazione degli strumenti di gestione e protezione

- Sicurezza dei canali mediali (spaziali e temporali) necessaria per la protezione
- Identificazione del prodotto culturale indispensabile per la gestione e la protezione
- Caratterizzazione del prodotto culturale indispensabile per la gestione
- Watermarking utile ma non sufficiente per l'identificazione e la protezione
- Fingerprinting utile in alcuni ambiti applicativi
- Distribuzione dei contenuti utile per la protezione
- "Intossicazione" dei sistemi illegali utile per la protezione
- Combinazione degli strumenti tecnologici efficaci in tecnologie DRM "solide" e standard per la gestione e la protezione immateriale, materiale ed economica del prodotto culturale digitale, soprattutto rispetto alle transazioni di distribuzione, acquisizione, fruizione

Tecnologie DRM
(Digital Rights Management)

- Set di tecnologie che permettono ai proprietari di contenuti:
  - di controllare l'accesso ai contenuti
  - di definire le politiche di accesso

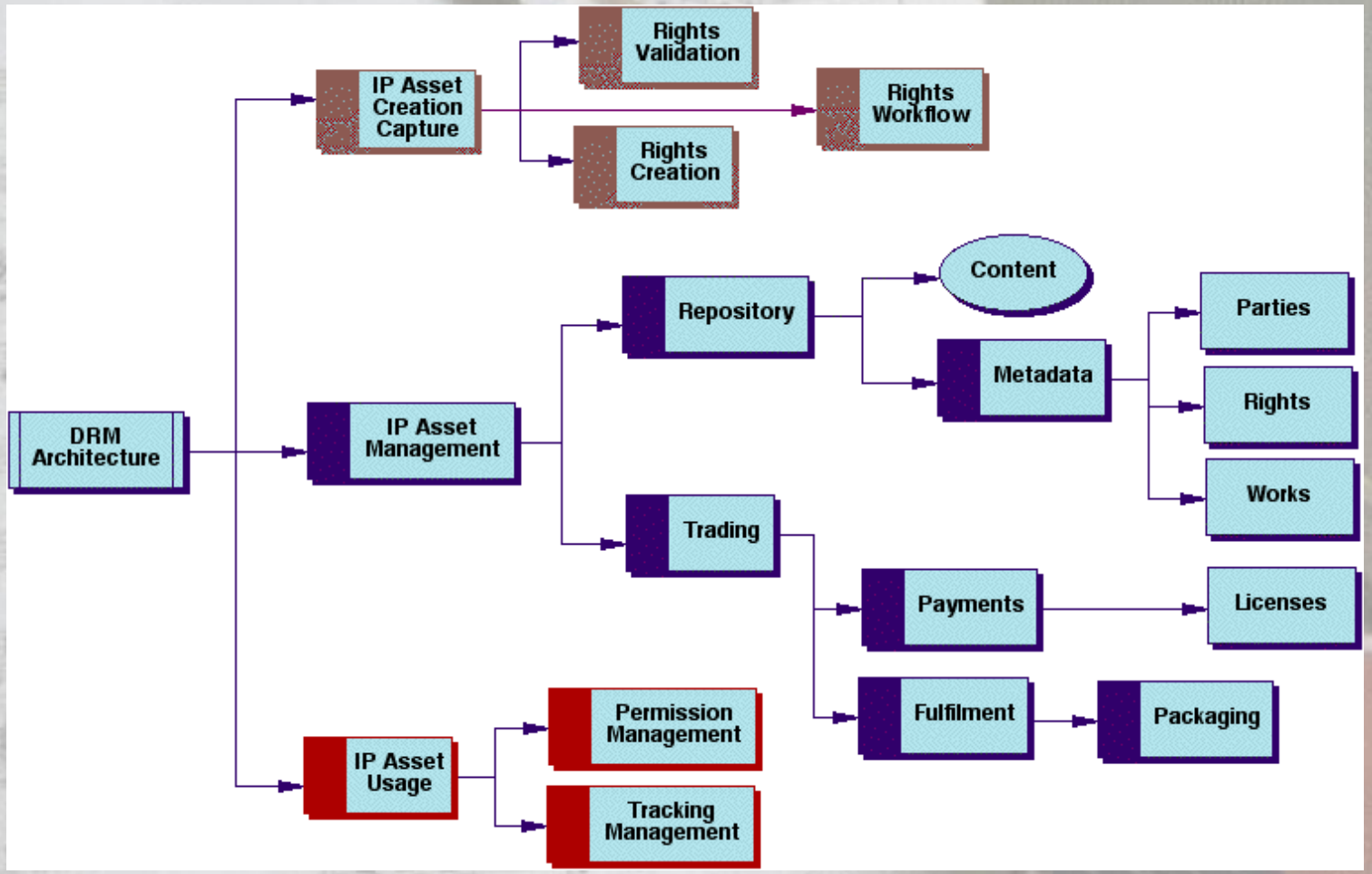
- Forniscono anche:
  - **Persistent Technology**: tecnologia per la protezione dei file tramite tecniche di crittografia e watermarking, accessibili solo dopo un'opportuna identificazione del fruitore
  - **Business Rights**: capacità di associare economia dei diritti a contenuti dotati di contratti
  - **Access Tracking**: sistema per il tracciamento delle operazioni di accesso ed utilizzo ai contenuti effettuate dagli utenti
  - **Rights Licensing**: sistema per la definizione di specifici diritti di un contenuto, rendendolo fruibile tramite contratto (manifest)

Architettura funzionale del DRM

Componenti del DRM di alto livello che permettono la gestione dei diritti:

- **IP Asset Creation and Capture**: definisce come gestire i contenuti in fase di creazione
- **IP Asset Management:** definisce come abilitare e gestire la commercializzazione dei contenuti
- **IP Asset Usage:** definisce la gestione d'uso dei contenuti una volta commercializzati

Architettura funzionale del DRM



Architettura dell'informazione nel DRM

Componenti del DRM per la descrizione e la modellazione delle entità

- Modellazione delle entità
  - Mediante codifiche di metadati, dati, informazioni, ontologie
- Identificazione e descrizione delle entità
  - tramite sistemi di identificazione (DOI, ecc.)
- Definizione dei diritti tramite REL

  (Rights Expression Language)
  - esempio: ODRL – Open Digital Rights Managements

Altre caratteristiche del DRM

- **Granularità:** capacità del sistema di gestire singole parti di un contenuto in differenti flussi di scambio
- **Interoperabilità:** capacità del sistema di permettere a creatori, produttori e venditori di comunicare col medesimo “linguaggio”
- **Personalizzazione**: possibilità di personalizzare i contenuti in funzione delle esigenze degli utenti, per esempio tramite watermaking visibili

Progetti DRM ad uno status di standard

- **ODRL (Open Digital Rights Language Initiative)**
  - REL open ed indipendente dalla piattaforma
  - Accettato ed usato dalla Open Mobile Alliance (OMA) e co-pubblicato da W3C
  - Attualmente utilizzato nelle applicazioni ludiche
- **OMA (Open Mobile Alliance) DRM Enabler**
  - DRM che implementa: preview dei contenuti, copia illegale e superdistribution
  - Usato nelle applicazioni della telefonia mobile GSM e 3G ed implementato in cellulari Nokia, Motorola, Siemens, Sony Ericsson
  - Attualmente è alla versone 2.0 e permette di gestire vari contenuti tra cui suonerie, loghi operatore, screen-saver, giochi Java, oltre che audio MP3, video MPEG, etc.
- **XrML (eXtensible Rights Markup Language)**
  - DRM proprietario e sottoposto a patent licence, sviluppato presso la Xerox Palo Alto Research Center e gestito da ContentGuard ed International Standards Community
  - È basato su XML
  - Fornisce una serie di metodi universali per la specifica sicura di politiche, metodi e condizioni per la protezione di qualunque genere di risorsa digitale e/o servizio da assegnare, sia a singoli che a gruppi di individui.
  - Utilizzato da Windows Media 9 di Microsoft la quale sta provando ad acquistare tale sistema (tramite l'acquisto di ContentGuard) per diventarne l'unica governatrice (bloccata dalla Comunità Europea ed in fase di esame)
- **IPMP (Intellectual Property Management & Protection)**
  - MPEG
- **XMCL (eXtensible Media Commerce Language)**
  - RealNetworks

MPEG-21 Multimedia Framework

- MPEG-21, partito nel Giugno 2000, ha come obiettivo quello di risolvere questi aspetti con lo sviluppo di un framework multimediale (*Multimedia Framework*) che fornisca all'utente un supporto per lo scambio, l'accesso, il consumo, il commercio ed ogni altro tipo di operazione inerente il multimedia, che sia efficiente, trasparente ed indipendente dalla piattaforma HW/SW utilizzata.

- MPEG-21 prevede un proprio REL (Right Espression Language), un RDD (Right Data Dictionary) e le specifiche per la descrizione dei contenuti, la loro elaborazione, ricerca, scambio, memorizzazione e protezione

- MPEG-21 si basa su due concetti fondamentali:
  - **Digital Item**: entità che rappresenta l'unità fondamentale per la distribuzione e la transazione; essa viene modellata attraverso il DID (Digital Item Declaration), un insieme di specifiche che permettono di descriverlo da un punto di vista astratto e concettuale.
  - **User***:* entità che interagisce con i Digital Item.

- I **Digital Item** possono essere considerati come elementi del Multimedia Framework (collezione di video, album musicali, ecc.) mentre lo **User** (singoli individui, società, enti governativi, comunità, consorzi, ecc.) è colui che li utilizza. La manipolazione di questi **Digital Item** è governata da una serie di meccanismi, regole e relazioni che ne tutelino il loro trattamento in funzione del fatto che lo **User** abbia privilegi sufficienti per poter eseguire una determinata operazione.

DRM – esempi di tecnologie

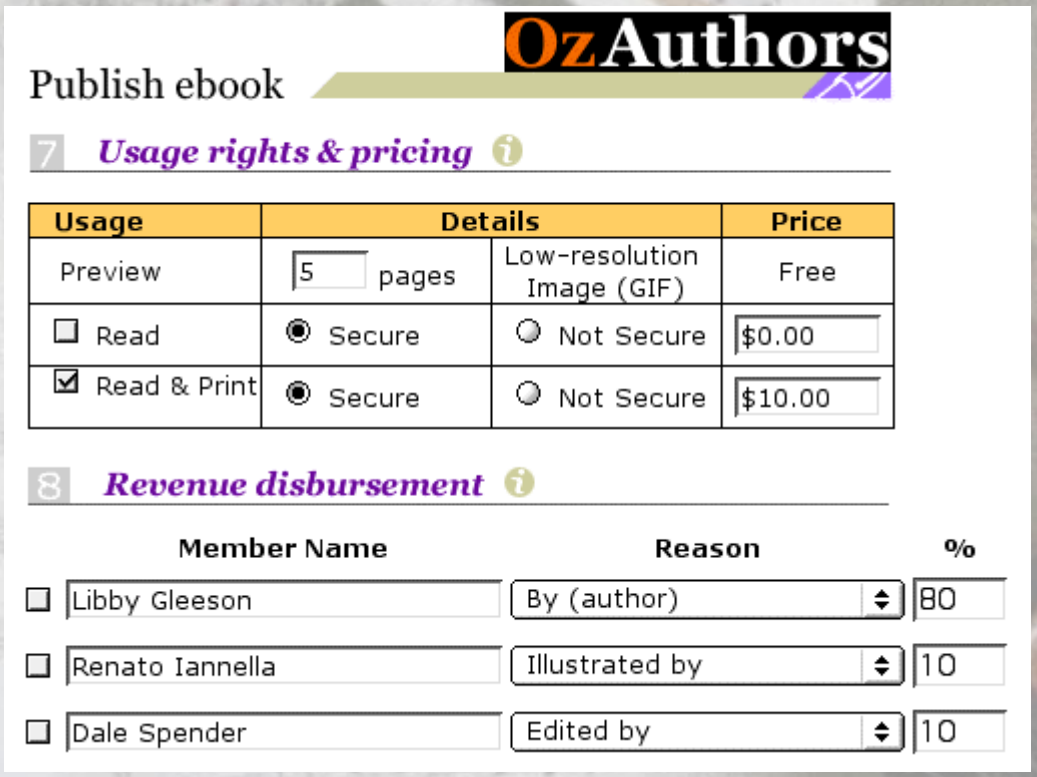
- Fraunhofer e **LWDRM** (Light Weight Digital Rights Management)
  - http://www.iis.fraunhofer.de/amm/techinf/ipmp/index.html
  - http://www.iis.fraunhofer.de/amm/techinf/water/index.html
- Apple e **Fairplay**
  - http://www.apple.com/gr/support/itunes/authorization.html
  - Crack di Fairplay
- Microsoft e **Windows Media**
  - http://www.microsoft.com/windows/windowsmedia/drm/default.aspx
- RealNetworks ed **Helix**
  - http://www.realnetworks.com/products/drm/

DRM – esempi di prodotti

- Liquid Audio: soluzione end-to-end proprietaria, utilizza encrypting e watermarking, supporto licenze dei contenuti impiegati su device multipli
- RioPort: architettura per dispositivi mobili, può eliminare l'uso del PC, adottato da Nokia, SONICblue, Samsung, Sanyo, Nike, Compaq
- Lockstream: soluzione end-to-end proprietaria, permette di creare interfacce personalizzate
- Musicrypt: sistema basato su autenticazione biometrica

Esempio implementativo di DRM

OzAuthors (on-line book store):



DRM e licenze

- Architettura usuale nella maggior parte dei sistemi DRM recenti

- Motivi:
  - Profilazione degli utenti mediante insiemi di diritti differenziati per un certo prodotto culturale
  - Abbonamento a librerie di contenuti mediante un insieme di diritti per una molteplicità di prodotti culturali
  - Contenuti non residenti sui supporti dell'utente (streaming media)

- Permettono di separare la gestione dei diritti dalla materializzazione e dalla distribuzione dei prodotti culturali immateriali

DRM e licenze

- **sistemi “incatenati”:** il servizio di licenze è centralizzato e sicuro; l’utente può effettuare operazioni solo on-line; è pensato per applicazioni general purpose; sistema usato da Microsoft, Intel e IBM.

- **sistemi "non incatenati":** il sistema di gestione delle licenze è gestito lato client; è promosso da InterTrust (www.intertrust.com); pensato per applicazioni di file-sharing; filosofia usata dal nuovo Napster.

Esempio di licenze nel DRM: Microsoft

- MS fornisce licenze differenziate in funzione delle attività come per esempio:
  - Creare e distribuire un'applicazione basata su Windows in grado di riprodurre contenuti protetti basati su Windows Media e di trasferirli in dispositivi portatili
  - Creare e distribuire un'applicazione basata su Windows in grado di riprodurre contenuti protetti basati su Windows Media
  - Creare CD o DVD audio che contengano contenuti protetti basati su Windows Media

- Un elenco completo delle tipologie di licenze fornite da MS:
  http://www.microsoft.com/windows/windowsmedia/it/drm/licensing.aspx

Esempi di DRM per abbonamenti

- MusicNet
  - BMG, EMI, Warner Bros
  - DRM: Tecnologia RealNetworks
- PressPlay
  - Sony, Universal
  - DRM: Tecnologia Microsoft
- FullAudio
  - licenze cataloghi Universal, EMI, e Warner
  - DRM: Tecnologia Microsoft
  - commercializzato mediante radio ClearChannel

Microsoft Longhorn e Palladium

- Nel giugno 2002, Microsoft ha annunciato l'introduzione di Palladium, noto anche come Next-Generation Secure Computing Base (NGSCB), che utilizza quattro componenti fondamentali:
  - Attestazione: verifica dell'identità dell'utente e della tipologia di software che sta utilizzando e della conoscenza dei contenuti che sta trasmettendo
  - Riservatezza: l'utente può criptare documenti e renderli disponibili solamente ad utenti ben definiti e certificati
  - Forte isolazione di processo: introduce un ambiente isolato dal resto del sistema, al riparo da attacchi
  - Sicurezza dei dati di input e di output: le informazioni tra i due ambienti creati sono criptate
- Palladium prevede l'uso della tecnologia DRM con certificazioni (gestite dalla stessa Microsoft) per tutti i tipi di file multimediali
    - Primo esempio d'uso di certificazione con i driver
    - Primo esempio di DRM nella tecnologia Windows Media 9

Dove stiamo andando

- La tecnologia procede in più direzioni, talvolta contraddittorie
- I controlli a livello personale non sono né facili né graditi
- I prodotti culturali evolvono rapidamente di pari passo con la tecnologia, pur mantenendo del tutto o in parte i mercati dei prodotti culturali tradizionali
- La maturazione di standard di DRM “vincenti” non è ancora avvenuta ed è prevedibile possa avvenire non prima che a medio termine
- La proprietà intellettuale e industriale deve essere tutelata e prima ancora rispettata; il rispetto della proprietà è la base per una tutela effettiva
- L’interscambio P2P globalizza la sfera del prestito personale ampliando gli orizzonti culturali e mettendo in crisi i tradizionali meccanismi di protezione della proprietà intellettuale e industriale
- L’assemblaggio e la generazione di prodotti culturali la cui composizione è realizzata on demand, direttamente da casa o in luoghi di ritrovo o in siti commerciali, consente vantaggi economici, logistici, di ampliamento del catalogo e del mercato

Dove investire

- Evitare che i meccanismi di protezione dei prodotti culturali facciano perdere:
  - qualità dei contenuti
  - facilità d'uso rispetto ai "modi" di fruire
  - facilità d'uso rispetto ai potenziali dispositivi di fruizione
- Incentivare la cultura del rispetto e della tutela della proprietà intellettuale e industriale
- Disincentivare l'illecita copia del prodotto culturale mediante opportune strategie che riducano la convenienza economica della copia stessa
- Incentivare la commercializzazione di prodotti culturali immateriali mediante cessione di licenze "personalizzabili", flessibili, orientabili a tipologie eterogenee di mercati
- Incentivare la cultura e la trasparenza dell'equa ripartizione dei diritti di proprietà intellettuale e industriale relativi ai prodotti culturali
- Definire strategie di collecting e ripartizione dei diritti in cui coesistano opportunamente i meccanismi dei "vecchi mercati" con quelli dei "nuovi mercati"
- Incentivare l'identificazione e il reperimento di soggetti collettivi - nuovi o non ancora gestiti - che fruiscono di prodotti culturali, al fine di ampliare l'economia del mercato dei prodotti culturali

Sitografia

Architetture per l’interscambio musicale P2P

- Napster – www.napster.com
- WinMX – www.winmx.com
- NapMX – www.napmx.com
- Gnutella – www.gnutella.it
- Freenet – www.freenet.org
- Kazaa – www.kazaa.com

Sitografia

Architetture di sistemi per *music on demand*

- iTunes – www.apple.com/itunes
- Starbucks (HP) - www.starbucks.com/hearmusic/
- MyEmotion - www.myemotion.it/
- Digital Music Dispenser - www.e-zmanaging.com/
- Siti russi:
  - http://www.allofmp3.com/
  - http://delit.net/
  - http://www.mp3search.ru/

Sitografia

Workshop for Technology, Economy, Social and Legal Aspects of Virtual Goods

3rd Edition, June 2 - 4, 2005, Ilmenau, Germany

http://virtualgoods.tu-ilmenau.de/2005/cfp.html

Approfondimenti

Progetto intercontinentale IMS “A Musical Application Standard Using the XML Language for Intelligent Manufacturing of Music for CDs, DVDs, Web”

http://www.ims.org/projects/project_info/musicxml.html

Standardizzazione IEEE dell’applicazione musicale di XML

http://www.lim.dico.unimi.it/maxproject/max2002/welcome.htm

AA.VV. (G. Haus & I. Pighi Editors): "Standards in Computer Generated Music", multiplatform mixed mode CD-ROM (Macintosh, Windows, Unix + CD-DA tracks), IEEE Computer Society Press, 1996.

G. Haus: "Elementi di informatica musicale", Gruppo Editoriale Jackson, Milano, 1984.

Ringraziamenti

La realizzazione di questa presentazione si è avvalsa della costante collaborazione del Dr. **Giancarlo Vercellesi** (LIM-DICO).

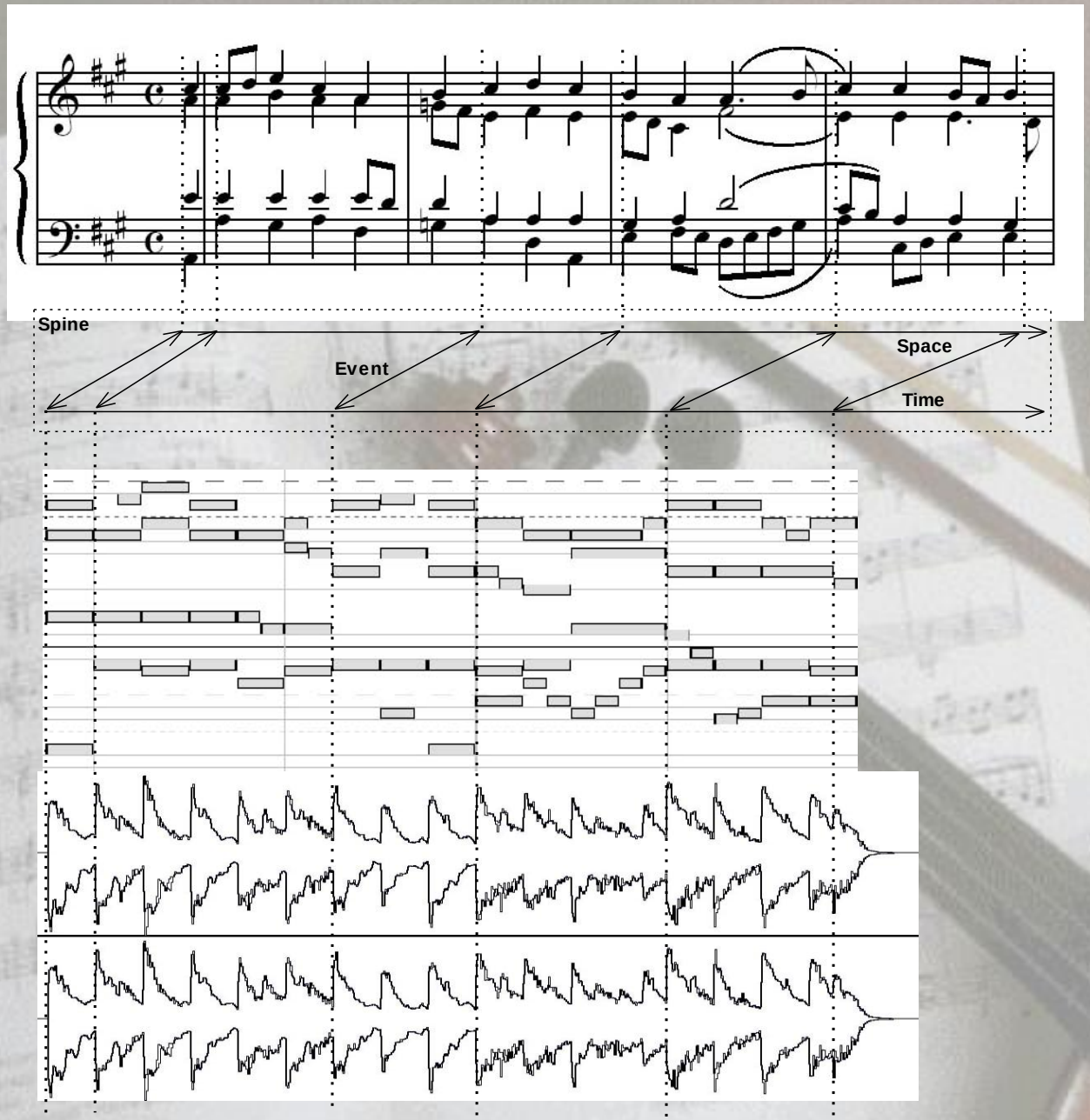
Contatti

email: haus@dico.unimi.it

website: http://www.lim.dico.unimi.it
http://www.dico.unimi.it

indirizzo: LIM - Laboratorio di Informatica Musicale
DICO - Dip. Informatica e Comunicazione
Università degli Studi di Milano
via Comelico 39
20135 Milano

fax: 02 50316373



Grazie
per
l'attenzione

!