Protecting Digital Property: Algorithms to Solutions

Lyman P. Hurd Feb. 13, 2001
MediaBin Inc.
Outline

• What are we trying to protect?
  - User rights

• What tools are available?
  - Technological
  - Legal

• How are they doing?
  - Case studies

• Delivery Systems
What are we trying to protect?

- Enforcement of Usage Rights such as:
  - Transport Rights
  - Render Rights
  - Derivative Works Rights
  - Backup rights

- Source: Mark Stefik *Trusted Systems*
  Scientific American Special Report
Usage Rights

- Transport Rights
  - permission to copy, transfer or loan.
- Render rights
  - permission to play or print
- Derivative-work rights
  - permission to excerpt or quote
- Backup rights
  - making and restoring of archival copies
Tools: Technological

- Encryption
  - Private Key
  - Public Key
- Key Distribution
- Protocols
Encryption: Private Key (Symmetric)

- Parties A (Alice) and B (Bob) share a secret (key)
- Alice encrypts the message to Bob using this key and Bob decrypts the message using the same key
- Main problem: Alice and Bob must share a pre-existing secret
Private Key Encryption

- Strength determined by algorithm and size of key (in bits)
- Key length of 40 bits to 128 bits typical
- Key length mainly relevant to benchmark cost of a direct attack
- Algorithms include DES (digital encryption standard) and soon to be released AES (advanced encryption standard)
Encryption: Public Key

- Bob generates a public encryption key $E$ and a private decryption key $D$
  - $E$ is made public (published)
  - $D$ is kept as a secret
- Alice can send message using Bob’s public key without pre-arrangement
  - Given message $M$, Alice sends $E(M)$
  - Mathematics says that knowing the function $E$ is of little help in determining $D$
Encryption: Public Key cont.

- Much more complicated algorithms
- Much larger key length needed for comparable level of security
- Key lengths of 1024 to 2048 bits typical
- Therefore: main use is for exchange of a symmetric key (combination of public and private)
Copyright Law

- Multifaceted
- Rights not absolute
- see (e.g.)
  http://fairuse.stanford.edu/primary/
Title 17 Section 106

- Subject to sections 107 through 121, the owner of copyright under this title has the exclusive rights to do and to authorize any of the following:

- (1) to reproduce the copyrighted work in copies or phonorecords;
- (2) to prepare derivative works based upon the copyrighted work;
Cont’d

- (3) to distribute copies or phonorecords of the copyrighted work to the public by sale or other transfer of ownership, or by rental, lease, or lending;
- (4) in the case of literary, musical, dramatic, and choreographic works, pantomimes, and motion pictures and other audiovisual works, to perform the copyrighted work publicly;
- (5) in the case of literary, musical,
Copyright

- (6) in the case of sound recordings, to perform the copyrighted work publicly by means of a digital audio transmission.
Sec. 107. Limitations on exclusive rights: Fair use

- Notwithstanding the provisions of sections 106 and 106A, the fair use of a copyrighted work, including such use by reproduction in copies or phonorecords or by any other means specified by that section, for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research, is not an infringement of copyright. In determining whether the use made of a work in any particular case is a fair use the factors to be considered shall include -
Fair Use

• (1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes;

• (2) the nature of the copyrighted work;

• (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and

• (4) the effect of the use upon the potential market for or value of the copyrighted work. The fact that a work is unpublished shall not itself bar a finding of fair use if such finding is made upon consideration of all the above factors.
Case Study: eBooks

- Riding the Bullet by Stephen King
  - Distributed as an eBook in Adobe PDF format
  - Encrypted using 40 bit encryption
  - Vendor is discussing using 64 bit in future
Encryption Scheme Broken

- Unencrypted form of book distributed by Swiss user
- Break of scheme involved modifying software
  - replacing DLL
- I.e., strength of encryption was irrelevant!
Case Study: DVD’s

- Encrypted using CSS (Content Scrambling System)
- 40 bit key
Set-up

• Every DVD (disk) has a decryption key
• Every DVD decoder (hardware/software) has a key
  - (sometimes many for a given decoder)
• Every disk’s key is stored encrypted using the key for every decoder
DVD’s cont.

- Knowing one decoder’s decryption key enables breaking any DVD disk
- Each player needs to protect key
  - System only as good as weakest link
DVD’s cont.

- Decryption key from Xing broken by MoRE (Masters of Reverse Engineering)
  - Produced DeCSS utility
Another major impetus for breaking scheme was production of a Linux-compatible player.
People seeking right to display legitimately purchased DVD’s on their choice of platform.
Increasing importance of images

“The shortest distance between a customer and a buying decision is an image … and the better the image the shorter the distance.”

Tony Henning, Future Image Report
Watermarking

- Can be visible or invisible
- Tracks image:
  - To copyright owner
  - Possibly to purchaser
- Watermark should ideally be applied after all other processing
Uses for Watermarking

- Fragile watermarks are designed to be destroyed by any manipulation of image data
  - Ensure authenticity
- Visible watermarks may be used as demonstration material and make images unusable for most applications
  - Large black lines across image
- Some image marking is done in metadata outside of image content
  - Need method of doing this in many different image formats
Invisible Watermarks

- Used to track images despite manipulation
  - Compression, scaling, colorspace conversion
- Most commercially prevalent is Digimarc (TM)
Web Content Management
a multi-billion dollar market

Estimated to reach 13 Billion in 2003

Source: GartnerGroup

MediaBin enables content management for images!
E-Commerce Image Content

Pressures

Increasing number of images
- More products (SKUs)
- More vendors/suppliers
- More “views” of the product

Increasing image deployments
- Thumbnail, low-res, high-res, cropped version
- Bandwidths: dial-up...now DSL/Cable modem and wireless devices
- Multiple web sites
Security Challenges

Every type of derivative work has different security implications

- Free
  - Low-res thumbnail
  - Visibly watermarked image

- Potentially more expensive
  - High resolution production-quality graphics
The MediaBin Platform

MediaBin is:

• a media database -
  a repository for original images

• an integrated image processing engine -
  to rapidly adapt images for multiple deployment requirements
MediaBin Platform Benefits

- **Speed**
  - Scale your business faster for more sales
  - What you need where you need it, NOW!

- **Centralized Control**
  - Brand control
  - Security and flexibility

- **Increased Sales**
  - Better customer experience

- **E-business Integration**
  - True scalability
Only one image is stored.
Typical Path for Web Image Content

creative + production workflows...

Adobe Photoshop

Adobe ImageReady

native Photoshop files (standard file server)

web content management system

JPEGs & GIFs

web server(s)

What’s wrong with these pictures?

- The relationships between web images and their source Photoshop files are unknown...
- No true management of web image content
Web Image Content via MediaBin

- Web images are now linked to source Photoshop files
- Automatic updating of web images is now possible!
Ford Enterprise Image Catalog

Image Producers
- ad agencies, J Walter Thompson
- web design teams
- internal graphics

Image Owners
- Brand Managers
- MarCom Managers
- Creative Directors

Ford Division Mkting Communications

Image Users
- Sales
- Training
- Investor Relations

MediaBin

Users get images just the way they need them!

web sites, e-commerce, product catalogs

advertising, printed & online collateral
One brand-approved source image ensures consistency and improves brand velocity through rapid cross-media adaptation.
Image Composition
Auto configurations managed by layers

digital camera
studio
people with Macs and Photoshop...

high-resolution images

web-ready images

web design teams

web e-commerce
Automated Composition of Auto Trimlines

- Digital camera
- Studio
- People with Macs and Photoshop...
- Multilayer Photoshop files
- IIS web server(s) with MediaBin Design-time control
- Clustered MediaBin Servers
E-business Collateral Auto-composition

- Complex images can be generated under application control
- Photoshop layer selection and replacement
- Dynamic images used for e-commerce, CRM, and print-on-demand
MediaBin Overview

- Cataloging
- Version Control
- Distributed Access
- Visual Searching
- Image Sourcing
- Directory Integration
- Image Routing

- Storage
- Automation
- Access

- Repurposing
- Imaging Tasks
- Auto-composition
Distributed Access

- Native Windows client
- Customizable web client
- Server and clients connect via standard Internet protocols
Task Automation

- Task: A simple or complex sequence of image processing steps executed by MediaBin
- Tasks can be generic or image-specific
- Tasks can be accessible to everyone or only to specific users or groups
The creation process for each derived image is recorded in a “derivative image database.”

Each derived image contains an embedded tag that refers to the source MediaBin and DID record.

An image can be regenerated:
- Whenever a source image is revised
- When output requirements change
Conclusions

• Protection of Intellectual Property has both business and technical implications.
• Solutions that give all the control to the end user even in the form of a closed application do not work.
• By centralizing image assets and allowing manipulation to be part of the process, one has the potential to keep control.
MediaBin Provides

- A centralized place to control access to images
- Integration of image processing and image storage
- The ability to assign security to different quality derivatives
- A single place to enforce work rules such as watermarking