



DIGITAL WATERMARKING

Jeff Hinson

CS525, Spring 2010

Outline

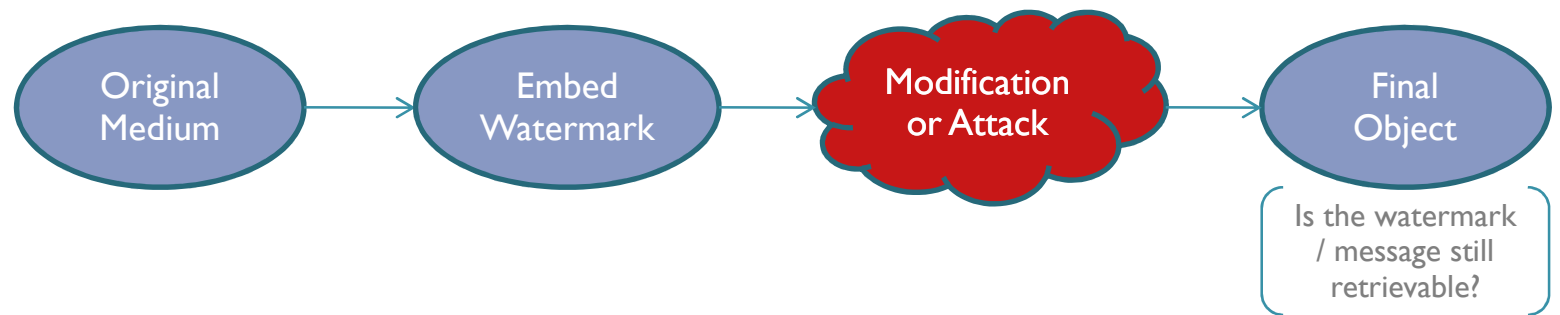
- Introduction
- Challenges
- Algorithms / Methods
- Detection
- Existing Programs
- Lessons Learned / Conclusion
- Questions

Introduction

- Digital Watermarking is embedding information into a digital signal that is difficult to remove
- Visible vs. invisible
- Examples
 - Television (the station mark in a corner)
 - Photos (copyrighting, etc.)
 - Music, videos, movies (to prevent piracy)
- Applications
 - piracy prevention/copyright infringement
 - Source Tracking
 - Covert Communication / Steganography

Challenges

- Media may be vulnerable to attacks and/or modifications after watermarking



- Minimize the size of the watermark
- Prevent errors during compression/decompression
- Prevent hackers from just editing out the watermark
- How to detect tampering?
 - not just retrieving watermark, but telling if someone has changed the original work in any way

Algorithms / Methods

- Steganography: more than just encryption
 - Where cryptography seeks encryption, steganography seeks obscurity
 - Watermark is invisible
 - Hide watermark (i.e., some unique value) into object
- Seek to hide information in images, audio, and/or video so that you don't know it's there unless you are looking for it

Watermarking Images

- LSB – Least Significant Bit Hiding
 - Original pixels: 10110001 and 01100100
 - Secret Byte: 11001011
 - New Pixels: 10111100 and 01101011
 - Easy and effective, but easy to detect
- DCT – Direct Cosine Transformation
 - Recall JPEG compression – we use DCT to make multidimensional array of coefficients
 - as we are using DCT to compress, stuff hidden data in
 - Effect and almost impossible to detect, but vulnerable to noise
- Wavelet Transformation
 - used for higher compression than plausible with DCT
 - same basic idea as DCT – add data during compression stage
 - is still an ongoing research topic

Watermarking Audio

- MIDI
 - Change numeric values of pitches with hidden data
 - Changes are barely noticeable to human ear (at worst)
 - Easy to do, but easy to detect
- MP3
 - Similar to DCT and Wavelet: as audio is being compressed, toss some information in and/or control rounding
- Spread Spectrum
 - Algorithm to add background noise that is barely audible
 - Noise contains the secret information
 - Can be applied to numerous formats, including MP3 (after compression)

Watermarking Video

- Watermarking Video
 - Combination of Image and Audio techniques
 - It all depends on the specific codec
- For example, H.264
 - Compression method similar to DCT
 - Control compression process to insert information instead of rounding off

Detection

- Must know what method was used to encode watermark
 - There are too many formats and methods to check every possible method on a single medium
 - Computers not fast enough to check every method
- Detection is a large concern, and has much research
 - called “Steganalysis”
 - lots of good papers on steganalysis for audio and still images, but nothing great for video
 - detecting watermark in video is a good topic for future research

Existing Programs

- Image Watermarking / Steganography
 - JSteg <<http://www.jsteg.org>>
 - QuickCrypto <<http://www.quickcrypto.com>>
 - VisualWatermark <<http://www.visualwatermark.com>>
- Audio
 - MP3Stego <<http://www.petitcolas.net>>
 - AudioPaint <<http://nicolasfournel.com/audiopaint.htm>>
- Video
 - Hermetic Stego <<http://www.hermetic.ch>>
 - Video Watermark Factory
<<http://www.videowatermarkfactory.com>>

Lessons Learned / Conclusion

- No “set way” to watermark something
- General ideas:
 - minutely altering numerical values
 - control rounding of values during compression
 - it all depends on what format/codec you are using
 - no good way to recover info after tampering
- Detection is near impossible
 - Easy if you know what you are looking for
 - Too many methods and formats to check them all
- Digital Watermarking is a hot topic
 - Concerns for intellectual property, copyrights, terrorism, source tracking, etc.



Questions or Comments?