CryptMark: A Novel Secure Invisible Watermarking Technique for Color Images

Saraju P. Mohanty
VLSI Design and CAD Laboratory
Computer Science and Engineering
University of North Texas.
Email: smohanty@unt.edu
Outline of the Talk

- Introduction
- Related Research Work
- Contributions of this Paper
- The Proposed Approach
- Experimental Results
- Conclusions
Digital Rights Management (DRM) is a generic term that refers to any of several technologies used by publishers, creators, or owners to control access and usage of digital data.

Typically a DRM system:

- Protects intellectual property by encrypting the data so that it can only be accessed by authorized users.
- and/or
- Marks the content with a digital watermark so that the content can not be freely distributed.
Judicious use of both encryption and watermarking necessary for multilayer protection through DRM.
DRM : Objectives

- It is mine!
- It is mine!!

Hacker | Multimedia Object | Owner

- Whose is it?
- Is it tampered with?
- Where was it created?
- Who had created it?
- ... and more.

Researcher
Digital Watermarking

Digital watermarking is a process for embedding data (watermark) into a multimedia object for its copyright protection and authentication.

Watermarking Types:
- Visible and Invisible
- Spatial/DCT/ Wavelet
- Robust and Fragile
An Watermarked Image (from IBM)
Related Research Works

- **Sheppard, Naini, and Ogunbona – 2001**: Discuss techniques for embedding multiple watermarks into one multimedia object.

- **Jiang, Yu, Shi, Liu, and Kim – 2002**: DCT domain blind watermarking schemes adaptive to HVS.

- **Guo and Georganas – 2003**: Algorithm using generalized secret sharing scheme in cryptography to address joint ownership problem.
Related Research Works …

- **Lu, Xu, and Sun – 2005**: A multipurpose fragile-robust watermarking technique based on the multistage vector quantizer structures is presented.

- **Pai, Ruan, and Gotze – 2005**: Energy efficient DCT-based high performance watermarking algorithm is presented.
Novel Contributions of the Paper

- A novel invisible watermarking method that uses cryptography and watermarking.

- **Security**: The *advantage* of encrypted watermark processing is that at no point of time raw watermark information is passed, thus providing security.

- **Attack Resilience**: Unlike most of the existing algorithms who heavily rely on low frequency AC components, this approach uses both DC and AC DCT coefficients.
Proposed Approach: Insertion
Proposed Approach: Authentication

Key → Encryption Process → Binary Information

Watermarked Image → Extraction Process

Compare for Authentication → Yes/No
Algorithm Flow for Secure Insertion

1. Get Cover (Image) and Watermark Information (Image).
   Get Encryption key.
   Get AC and DC Embedding Parameters.

2. Color Image → Grayscale Image
   - Transform Cover to Y-Cr-Cb, Consider Y component.
   - Consider the intensity image of the Cover.

3. Divide Cover into 8x8 blocks, Take DCT of each block.
   Encrypt and zero-pad the Watermark.


   Fine tune AC and DC embedding parameters.

6. Quality needs improvement?
   - Y: Yes
   - N: No

7. Done.
Algorithmic Flow of the Extraction and Authentication


2. Color Images
   - Transform Cover to Y-Cr-Cb. Consider Y component.
   - Divide Cover into 8x8 blocks. Take DCT of each block.

3. Grayscale Images
   - Consider the intensity image of the Cover.
   - Encrypt and zero-pad the Watermark.


5. Match?
   - Y: Confirm authenticity of watermarked image.
   - N: Image is not genuine.

6. Done.
Insertion Operation

- $c_{ij}(k)$ and $w_{ij}(k)$ denote values at position $(i,j)$ of block $k$.
- Watermark is embedded in cover image using:

\[
c'_{ij}(k) = \begin{cases} 
c_{ij}(k)(1 + \alpha_{ij}) & \text{if } w_{ij}(k) = 1 \\
c_{ij}(k)(1 - \alpha_{ij}) & \text{if } w_{ij}(k) = 0 \end{cases}
\]

- Two embedding factors used:
  - $\alpha_{dc}$ for DC components $\alpha_{00}$.
  - $\alpha_{ac}$ for AC components $\alpha_{01}$, $\alpha_{10}$, and $\alpha_{11}$.
- The values of $\alpha_{dc}$ and $\alpha_{ac}$ are chosen for a specified SNR threshold.
Extraction and Authentication Operation

- $w_{ij}(k)$ and $w'_{ij}(k)$ original and extracted watermark blocks.
- Construct watermark using:

$$w'_{ij}(k) = \begin{cases} 1 & \text{if } c'_{ij}(k) > c_{ij}(k) \\ 0 & \text{otherwise} \end{cases}$$

- Compare $w_{ij}(k)$ and $w'_{ij}(k)$ for authentication.
System Implementation: ISWAR (Imaging System with Watermarking and Attack Resilience)

Available at: http://www.cse.unt.edu/~smohanty/ISWARwatermarker/
System Implementation: ISWAR ...
Experimental Results: Test Images

Original

Watermarked

Original Watermarked
Experimental Results: Performance

<table>
<thead>
<tr>
<th>AttacksPerformedforTesting</th>
<th>ForVariousTestImage</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Lena (SNR = 105)</td>
<td>F16 (SNR = 99)</td>
<td>mandril (SNR = 101)</td>
</tr>
<tr>
<td>JPEG Compression 0 quality</td>
<td>Survived</td>
<td>Survived</td>
<td>Survived</td>
</tr>
<tr>
<td>Gray scaling 16 levels</td>
<td>Survived</td>
<td>Survived</td>
<td>Survived</td>
</tr>
<tr>
<td>Gray scaling 256 levels, JPEG compression 0 quality</td>
<td>Survived</td>
<td>Survived</td>
<td>Survived</td>
</tr>
<tr>
<td>Blurring , 0 quality JPEG Compression</td>
<td>Survived</td>
<td>Survived</td>
<td>Survived</td>
</tr>
<tr>
<td>Partial cropping</td>
<td>Survived</td>
<td>Survived</td>
<td>Survived</td>
</tr>
<tr>
<td>Stirmark Self Similarities</td>
<td>Survived</td>
<td>Survived</td>
<td>Survived</td>
</tr>
<tr>
<td>Stirmark 0 quality JPEG compression</td>
<td>Survived</td>
<td>Survived</td>
<td>Survived</td>
</tr>
<tr>
<td>Stirmark median filtering</td>
<td>Survived</td>
<td>Survived</td>
<td>Survived</td>
</tr>
<tr>
<td>Stirmark Random Distortions</td>
<td>Survived</td>
<td>Survived</td>
<td>Survived</td>
</tr>
</tbody>
</table>
Conclusions

- A novel invisible watermarking method called CryptMark is presented that uses cryptography and watermarking simultaneously.
- CryptMark can be an effective technique for DRM.
- Exhaustive testing of proved that the algorithm works well and can survive various forms of attacks.
- A possible extensions include use of wavelet transforms for embedding of strong watermarks.
- Blind extraction of watermarks is also a planned extension particularly because of its usefulness in authentication at the receiver end as well as identification of secretive communication.
- Low-power version of the watermarking scheme is also planned to be developed.
Thank You

For more information:
http://www.cse.unt.edu/~smohanty