IMAGE WATERMARKING

A

HOLOGRAPHIC IMAGE REPRESENTATIONS

Alfred M. Bruckstein
**IMAGE WATERMARKING**

**PROBLEM:** Given an image $I(x,y)$ generate another that looks the same but it carries a tag or watermark that encodes some information about its source and/or user.

**Applications:**
- copyrights & ownership rights
- tracking distribution of images
- proving illicit distribution

Of interest in this age of electronic distribution of images - when copies are as good as the originals.
A drawing of the San Antonio River that conceals a secret message (solution in Notes)

"The Codebreakers" by D. Kahn
A very clever approach:

A drawing of the San Antonio River that conceals a secret message (solution in Notes)

from "The Codebreakers" by D. Kahn

~ additional application:
covert channel of information transmission
The Context:

- steganography → cryptography
- software ownership rights → embed secrets in programs
- document authentication → watermarking → modify fonts, spacings etc...
- image watermarking → modifications of grey levels in the image plane directly → in conjunction with compression (lossy) algorithms → in the TRANSFORM DOMAIN
- sounds (audio) → video tagging
Requirements from a WM method

- Watermarks should be imperceptible
- Should be able to carry sufficient information (30 + 100 bits)
- Watermarks should not be easily identifiable from one or several watermarked images
- Watermarks should be recoverable from the watermarked image as the original
- Attempts to remove or alter the watermark should have ill-effects on the image
- Watermarks should not be wiped out by image modification/compression and other casual image processing procedures.
- Watermark info should be distributed to survive cropping (holoGRAPHIC)
The proposed METHOD

Watermarking in the Frequency Domain

1. \( I(x, y) \xrightarrow{\text{Fourier}} \tilde{I}(u, v) = M(u, v) e^{jP(u, v)} \)

2. Embed a watermark in magnitude of \( \tilde{I}(u, v) \)
   \[ M(u, v) \rightarrow M'(u, v) \]

3. Generate watermarked images as
   \[ I'(x, y) = \mathcal{F}^{-1}\{ M'(u, v) e^{jP(u, v)} \} \]

Solution looks circular: we are again facing the problem of watermarking \( M(u, v) \) but:

**Images are not too sensitive to modifications (in the transform domain) that affect the magnitude only!**
Common Wisdom in Image Processing

Phase is more "important" than Magnitude.

So we modify $M(u,v)$ by multiplying it with a "mask image" $W_M(u,v)$, that carries the watermark information in its geometry and profile.

$M(u,v) = M(-u,-v)$ (real images)

$W_M(u,v) = W(-u,-v)$ (real)

$W_M(u,v) = 1 + \varepsilon_M(u,v)$ (small)
The watermarked image will be

\[ I^w(x,y) = I(x,y) + I(x,y) \times \mathbb{F} \{ \mathcal{E}_w(u,v) \} \]

quantized to the #bits/pixel of I

\( \mathcal{E}_w(u,v) \) carries the watermark info; if small then \( I^w(x,y) \) looks like \( I(x,y) \)

How should \( \mathcal{E}_w(u,v) \) be designed to meet the WM requirements.

We need to model the various image modifications that the WM info has to survive and adapt \( \mathcal{E}_w(u,v) \) to the model.
Degradations in WM recovery

- Noise a linear operations on I
- Printing a rescanning
- Effect of lossy compression

were modeled as an unknown but smooth multiplicative noise over I(u,v) + an added N(u,v)
(flat for white noise).

- Cropping of parts of I

have an effect of additional smoothing in the frequency domain.

$\Rightarrow$ $E_H(u,v)$ should have enough "area" in the transform domain allocated to each info bit so encoding should be differential.
The design chosen a watermark recovery

\[ \varepsilon(\omega) = 1 - \bar{E} \]

\[ \varepsilon(\omega) = 1 + \bar{E} \]

\[ \{\varepsilon = 0.05, 0.1, 0.2\} \]

Watermark recovery by an **OPTIMAL DECISION RULE**

regard each frequency component as a little channel carrying information about \( \varepsilon(\omega) \)

\[ T\{I^w(\omega, \nu)\} = A (1 + \varepsilon) I(\omega, \nu) + N_{\text{noise}} \]

"measured"  \[ \beta \]

unknown  \[ \gamma \]

unknown  \[ \phi \]
- Hard Decisions for each BitRegion

- Estimate $\hat{p}$ for the subregions 1 and 2

- decide 0 or 1 according to $\hat{p}_1 \geq \hat{p}_2$

Result: with a WM of 120 bits

max count of errors $20 \div 25$

(under harshest of conditions)

But: errors occur in the high-frequency region & very low frequency (near DC)

so we have an error free band (ring) where about 40\% 50\% bits can be safely encoded even with HARD DECISIONS
Original images: Botticelli, Michaelangelo, Renoir.

Watermarked images

Watermark recovery: pointwise ratios

Figure 1: Original and Watermarked Images
Figure 3: Results for Michelangelo image: Watermarking at various intensities
**Some Experiments**

- Cropping (holographic prop.)
- Print/rescan/crop cycle
- JPEG compression (20% q.factor)
- Various $\xi$'s: $\xi=0.05, 0.1, 0.2$
- Contrast manipulations (gamma).
Figure 4: Results for Renoir image: Watermarking at various intensities
Printed/scanned watermarked image: Botticelli, Michelangelo, Renoir.

Watermark recovery: average values (note high frequency loss)

Watermark recovery: error locations; totals: 9, 3, 17 resp.

Figure 9: Results for printed/scanned images
JPEG compressed (20%) watermarked image: Botticelli, Michelangelo, Renoir.

Watermark recovery: average values (note high frequency loss)

Watermark recovery: error locations; totals: 29,18,24 resp.

Figure 7: Results for Images after 20% quality JPEG compression
Gamma curve 2 intensity adjustment: Botticelli, Michelangelo, Renoir.

Watermark recovery: average values (note darkness due to reduced contrast)

Watermark recovery: pointwise values

Figure 10: Results for Gamma adjusted images (all zero errors)
Figure 6: Watermarked Images after 20% quality JPEG compression
Cropped portions of watermarked image: Botticelli, Michelangelo, Renoir.

Watermark recovery: average values (note reduced contrast due to blurring)

Watermark recovery: error locations; totals: 2,1,1 resp.

Figure 5: Results for cropped images
Figure 2: Results for Botticelli image: Watermarking at various intensities
Cropped portions of printed/scanned watermarked image: Botticelli, Michelangelo, Renoir.

Watermark recovery: average values (note high frequency loss)

Watermark recovery: error locations; totals: 16,16,24 resp.

Figure 8: Results for printed/scanned and cropped images
CONCLUDING REMARKS

- The watermark is a combination of **GEOMETRY** + about 50 bits of **(ErrorFree) Info**
- Survives a variety of mistreatments and abuses of **I**
- It appears in portions (arbitrary portions!) of **I**

Ref: Bruckstein, summer 1994
Bruckstein Richardson, December 1996

**Competition**: NEC watermarking method (1995) in the DCT (like FFT) domain, embeds a random vector of 1024 values into selected comp.