Optimal adaptive diversity watermarking with state channel estimation

S. Voloshynovskiy\textsuperscript{ab}, F. Deguillaume\textsuperscript{a}, S. Pereira\textsuperscript{ab}, T. Pun\textsuperscript{a}

\textsuperscript{a}University of Geneva, CUI, Switzerland
\textsuperscript{b}Digital Copyright Technologies, Switzerland
Outline

1. Introduction
2. Watermarking Paradigm
3. Watermarking as Communication with Side Information
4. Stochastic models of watermarking channel
5. Adaptive diversity watermarking
6. Results
7. Conclusions
1. Introduction

Problem:
Market requires copyright protection technology for images, MPEG, and audio since copying is easy, quick and with the most recent technology lossless (e.g. CDROM writing)

Possible Solution: insertion of a watermark (WM) which can be used to authenticate an image, audio soundtrack, MPEG etc.

Watermark contains for example: unique identifier specifying buyer and seller, most useful are WM which have at least 60 bits of information.
1. Introduction

- **Robustness**: WM must resist main:
  - geometrical attacks (desynchronization), e.g.: cropping and translation, affine transformations (like rotation, scaling, aspect ratio changes), row/column removal, random local distortions;
  - signal processing attacks: non-linear and adaptive filtering, compression, (re)quantization, multiple watermarks and noise addition.

- WM should be invisible and detectable without original image (oblivious)!
1. Introduction

Existing watermarking technologies have the following problems:

- lack of encoder adaptivity to the host data;
- lack of prior information about undergone attacks (both signal processing and geometrical);
- lack of robustness to the attacks and corresponding adaptivity of watermark decoder.
1. Introduction

**Goal:** to develop generalized watermarking scenario:

- that takes into account **host or cover data** at encoder;
- is **stochastic**: applicable to a wide class of image and video watermarking algorithms operating in coordinate or transform (DFT, DCT, wavelet) domains;
- is **adaptive** to variability of channel parameters, i.e. undergone attacks, at decoder.
1. Introduction

The goal is reached using:

- adequate apparatus of communication theory;
- prior knowledge about cover-image and watermark statistics;
- optimal design of informed encoder and decoder.
1. Introduction

Notations:

\( x \) : original (cover or host image),
\( w \) : noise-like watermark,
\( y \) : watermarked or stego image, with
\[
  y = h(x, w|M)
\]

Main goal of watermarking attacks:
- preserve image quality
- \( y' \equiv x \) : attacked stego-image.
- render watermark undetectable/undecodable
2. Watermarking Paradigm

Embedding

Cover image $x$
Message $b$
Key
Perceptual model
Watermark Embedder $M$

Extraction

Attacks
Watermark Extractor
Decoder

$y$
$y'$
$y''$
$\hat{w}$
$\hat{b}$
3. Watermarking as Communication with SI

Watermarking Side Information (SI):

- both encoder and decoder can access the key;
- generalized channel state information is available.
  - host image
  - attacking channel
3. Watermarking as Communication with Side Information (SI)

Key

Message $b$

Watermark Encoder

$p(y|x,s)$

Attacking Channel

Watermark Decoder

$\hat{b}$

State generator

Cover image $x$
3. Watermarking as Communication with SI

Four possible classes of existing watermarking schemes:

Class I: Switches A and B open: SI is not available.

Class II: Switch A closed, and B open: SI is available at encoder only.

Class III: Switch A open, and B closed: SI is available at decoder only.

Class IV: Switches A and B closed: SI is available at both encoder and decoder.
3. Watermarking as Communication with SI

Class I: SI is not available.
3. Watermarking as Communication with SI

**Class I**: earlier watermarking algorithms.
Original papers of Cox 1997 and Tirkel 1996.

- Encoding and decoding are performed without reference to information about channel state.

- Watermark detection: linear correlator.
  (all attacks are modeled as additive stationary Gaussian noise).

- No geometrical attacks are assumed in the channel.
3. Watermarking as Communication with SI

**Class II**: SI is available at encoder only.

![Diagram of watermarking as communication with SI](image)

- **Key**
- **Message** $b$
- **Encoder**
- **Watermark Embedder**
- **Attacks**
- **Watermark Extractor**
- **Decoder**
- **Image channel state estimation**
3. Watermarking as Communication with SI

Class II: most of current watermarking algorithms.
Original papers of Costa 1983: IEEE IT
Watermarking application: Cox 1999: Proc IEEE

- Encoder is informed about channel state
  (optimal choice of codebook).

No more necessity to communicate the cover image to the decoder, if the cover data is used as SI by the encoder.
3. Watermarking as Communication with SI

**Class II: Drawbacks:**

- Complexity of the encoder can be very high (large codebook and corresponding complex search at the decoder).
- Watermarking channel is treated as cover image only.
- Attacks are not taken into account that can lead to the mismatch between the design of codebook and real situation.
- No robustness against geometrical attacks.
3. Watermarking as Communication with SI

Class II:
Possible solution:

to relax the lack of decoder adaptivity with respect to the attacking channel using the worst case scenario:

- for example the lowest lossy JPEG compression (Stirmark QF=10%)
- include quantization table in the design of the encoder.
3. Watermarking as Communication with SI

Class III: SI is available at decoder only.
3. Watermarking as Communication with SI

Class III: most of schemes that use synchronization (template or reference watermark: pilot).

Ability to estimate channel state:
- channel noise (in general non-Gaussian: overcomes the problem of decoder adaptivity to channel variations);
- geometrical attacks (pilot is used as synchronization pattern).

In the case of replicated watermark:
- diversity watermarking;
- self-reference principle.
3. Watermarking as Communication with SI

Class IV: SI is available at both encoder and decoder.
3. Watermarking as Communication with SI

**Class IV**: the most likely scheme for future algorithms.

These algorithms can operate under a wide class of uncertainties with respect to the channel state.

The encoder is matched with the cover data and the decoder is adapted to the attacking channel variations assuming fading, non-Gaussian attacks and geometrical transforms utilizing advantages of diversity watermarking.
4. Stochastic models of watermarking channel

The generalized watermarking channel includes:

- cover image;
- attacking channel.

To characterize both we use stochastic framework.
4. Stochastic models of watermarking channel

Exponential family: Two possible approaches

\[ p(x) \propto e^{-U(\bar{x}, \sigma_x^2)} \]

Type I

Fixed energy function

Varying parameters

Type II

Varying energy function

Fixed parameters

Energy function:

\[ U(x) \]

Model parameters:

local mean

\[ \bar{x} \]

variance

\[ \sigma_x^2 \]
4. Stochastic models of watermarking channel
4. Stochastic models of watermarking channel

Models of Type I: image generation model

Source \( N(0,1) \) \( \times \) Process I \( \begin{array}{c}
\sigma_x \\
\bar{x}
\end{array} \) \( + \) \( x \)

Doubly stochastic process: gamma, exponential, Jeffrey

\[ x \sim N(\bar{x}, \sigma_x^2) \]

Main problem: estimation of \( \sigma_x^2 \) and \( \bar{x} \).
4. Stochastic models of watermarking channel

Models of Type II

Approximation of marginal distribution
4. Stochastic models of watermarking channel

Models of Type II:

- Markov Random Fields (MRF)
- Generalized Gaussian MRF (GGMRF)
- Generalized Gaussian (GG)
- Generalized Cauchy (GC)
- Line models (Talvar)
- Huber or mixture models
- Hampel, bi-weight and redescending models
- non-quadratic regularizers

Main problem: exact approximation of marginal distribution
5. Adaptive diversity watermarking

Multichannel model of watermark

Generalized channel: \( c' = Fc + \beta \)

Fading, non-Gaussian noise
5. Adaptive diversity watermarking

**Generalized channel:**
\[ c' = Fc + \beta \]

**Fading** non-Gaussian noise

\[ F(i) \beta(i) \]

\[ F_j(i) \beta_j(i) \]

\[ r(i) \]

Decoder

\[ \hat{b} \]
5. Adaptive diversity watermarking

Matched filer:

\[ r = \langle g(\hat{w}), p \rangle \]

Non-stationary Gaussian noise (whitening filter):

\[ r_{nG}(i) = \langle \hat{R}_\beta^{-1}\hat{F}\hat{w}, p \rangle \]

Stationary Generalized Gaussian noise:

\[ r_{sGG}(i) = \sum_{j \in P_i} \frac{\left| \hat{w}(j) + \hat{F}(j)p(j)^{\gamma_\beta(i)} \right| - \left| \hat{w}(j) - \hat{F}(j)p(j)^{\gamma_\beta(i)} \right|}{\sigma_\beta(i)^{\gamma_\beta(i)}} \]

ML message decoder:

\[ \hat{b} = \arg \max_{\tilde{b}} p(r | \tilde{b}, x) \]
6. Results: lossy JPEG compression

Marginal distribution approximation using sGG model

Non-linearity of optimal matched filter

Close to linear correlator  Close to sign linear correlator
6. Results: lossy JPEG compression

**Shape parameter**

**Variance**

**Conclusions:**
- shape parameter is not equal to 2:
  - the linear correlator is not optimal;
- variance of channel noise is increased that leads to the decrease of the SNR at the decoder.
6. Results: lossy JPEG and Wavelet compression

JPEG: QF=10%; CR=66 times

Wavelet: 0.3bpp; CR=94 times

Algovision wavelet coder
6. Results: Cropping and Lossy JPEG compression

- JPEG QF=80%
- Watermark extraction
- ID#: 14872903
6. Results: Print/Scan Demo
6. Results: Print/Scan Demo

Watermark extraction
ID#: 14872903
6. Results

Stirmark 3.1 score

Signal enhancement  1.00
Compression (JPEG/GIF)  0.99
Scaling  1.00
Cropping  0.99
Shearing  1.00
Rotation (auto-crop, auto-scale)  0.99
Column&line removal  1.00
Flip  1.00
7. Conclusions

- The encoder and the decoder should be adaptive to the variations of the watermarking channel.

- The generalized watermarking channel is modeled as fading and additive non-Gaussian noise.

- Widely used linear correlator is not optimal for many attacks including lossy compression, denoising and interpolation caused by geometrical transforms.