Digital Watermarking and Steganography

by Ingemar Cox, Matthew Miller, Jeffrey Bloom, Jessica Fridrich, Ton Kalker

Chapter 11. Content Authentication

Lecturer: Jin HUANG

2015

The Motivation

- Has the Work been altered in any way whatsoever?
- Has the Work been significantly altered?
- What parts of the Work have been altered?
- Can an altered Work be restored?

Exact Authentication

Even a single bit change can be detected.

A Straightforward Method

- LSB
- Compare with predefined bit sequence.
- Limited authentication capabilities.

Embedded Signatures

Making the watermark “link” to cover.

- Signatures, e.g. SHA, MD5.
- But embedding change the cover.
- Partition the cover into two parts
  - One for signatures.
  - One for embedding.

Erasable Watermarks

It is the original unmodified work.

- But there is watermark in it!

The idea:

- $\mathbf{c_w}$ is a work with authentication $\mathbf{w_r}$.
- I can get the true original unmodified $\mathbf{c_o}$.
  - remove $\mathbf{w_r}$ from $\mathbf{c_w}$.
- Verify $\mathbf{w_r}$ with $\mathbf{c_o}$.

An Example

Simply use E_BLIND and D_LC with integer $\mathbf{w_r}$.

$$\mathbf{c_w} = \mathbf{c_o} + \mathbf{w_r}.$$

- But, the clamping of the value.
- Picking right $\mathbf{w_r}$ to avoid this problem?
  - No. It should be the signature.

A Solution

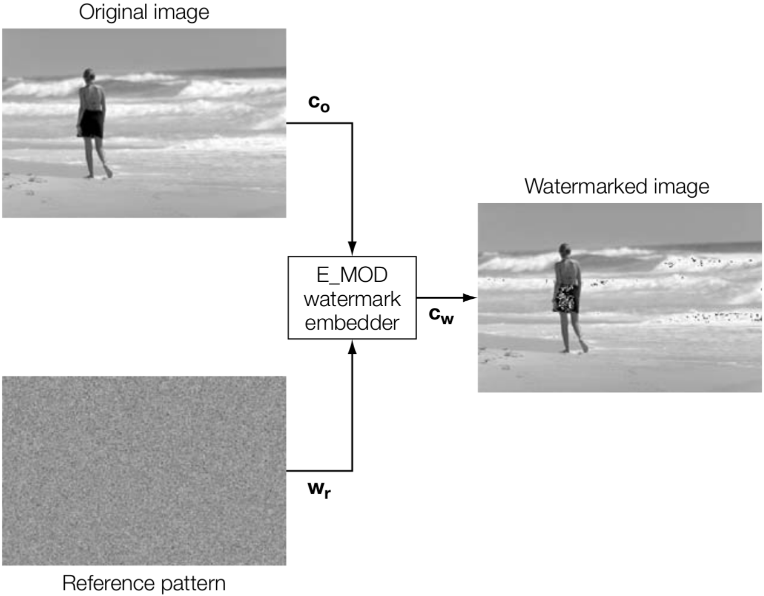
Modulo addition.

$$\mathbf{c_w} = \mathbf{c_o} + \mathbf{w_r} \mod 256.$$

From the viewpoint of human:

- Salt-and-pepper noise.

Illustration



Detection

From the viewpoint of detector:

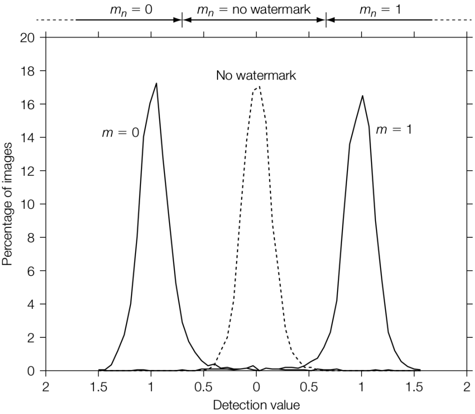
- Introduce some noise: from $253 + 5$ to 3.
- Compare to clamp: $255 \Rightarrow 3$.

Change of $\mathbf{w_r}$

- Original: 5.
- Clamp: 2.
- Modulo : -250.

Illustration

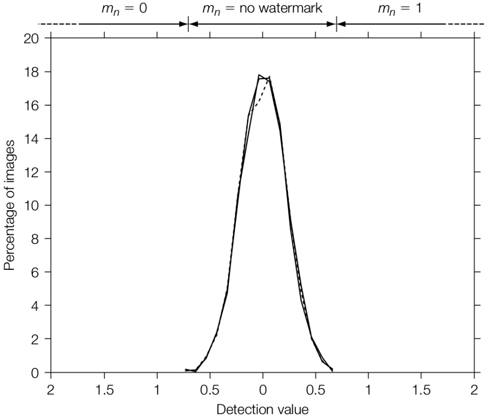
If the values of pixels are far from the borders.



Illustration

If the values of pixels are close to the borders.

- Blank and white strips.
- Images with equalized histograms.



Practical Solutions for Erasability

Difference expansion

- Neighboring pixels are more likely to have similar values.
- Difference between two neighboring pixels has a smaller dynamic range.

Using the difference as the channel.

One Bit Only

Giving two neighboring pixels
$x_1, x_2 \in \{0, \cdots, 255\}$.

- Transform

$$(y_1, y_2) = T(x_1, x_2) = (2x_1 - x_2, 2x_2 - x_1)$$
$$\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \left(\mathrm{Id} + \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \right) \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}.$$

Example:

$$T(59, 54) \Rightarrow (64, 49).$$

Modulo 3

How to embed?

- Modulo 3: $y_1 - y_2 = 3(x_1 - x_2)$.
- embed 1: $y_1 + = 1$.
- embed 0: $y_1 - = 1$.

How to detect?

- $y_1 - y_2 \mod 3$.

Convert It Back

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = T^{-1} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \big((4y_1 + 2y_2)/6\big)$$

An example

- Embedding:

$$c_o = x = (59, 54)$$
$$c_y = Tx = (64, 49)$$
$$c_{y0} = (63, 49).$$

- Extract message:

$$(63 - 49) \mod 3 = 14 \mod 3 = 2 \Rightarrow 0$$

- Recover $\mathbf{c_o}$:

$$14 \Rightarrow 15$$
$$63 \Rightarrow 49 + 15 = 64$$
$$c_o' = T^{-1}(64, 49)' = (59, 54).$$

Illustration

For More Bits

For n-bit:

$$\begin{aligned}(y_1, y_2) &= T_n(x_1, x_2) \\ &= ((n+1)x_1 - nx_2, (n+1)x_2 - nx_1) \\ \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} &= \left(\operatorname{Id} + n \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}\right) \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}.\end{aligned}$$

Embeddable Pixel Pair

Both values in the pairs $(y_1 - n, y_2)$ and $(y_1 + n, y_2)$ are within the dynamic range $\{0, \cdots, 255\}$.

How to know?

- $y_1 - y_2 \mod (2n+1) = 0$.

How to do?

- Modify x_1 to make $x_1 + c - x_2 \mod (2n+1) = 0$.
- ...

Illustration

$n = 3$.

Wait a Moment

It is stupid to make it so complex! Why not directly change x_1 so that:

$$x_1 - x_2 \mod 3 = 2 \text{ for } 0, \cdots$$

Benefit

$$y_1 + y_2 = x_1 + x_2.$$

- Less change on (average) brightness.
- Noisy is better than block change.

Question: Difference Expansion

What is the result of embedding 0 into $(60, 54)$?

What is the recovered result?

More Importantly

- $\mathbf{c_o} = (59, 54), (60, 54), m = 0$.
- By T:
  - $\mathbf{y} = (64, 49), (66, 48)$.
  - $\mathbf{c_w} = (63, 49), (65, 48)$.
  - $m = 0$
  - $\mathbf{c_o'} = (59, 54), (60, 54)$.
- $x_1 - x_2$:
  - $\mathbf{c_w} = (59, 54)$.
  - $\mathbf{c_o'} = (59, 54), (60, 54)$ ...

Fundamental Problem with Erasability

Perfect erasable watermarking

- 100% effectiveness.
- Unique Restoration.
- Low false positive.

It is impossible!

- Media space cannot hold $\mathbf{c_o}$ and its $\mathbf{c_w}$ simultaneously.
- 100% effectiveness leads to 100% false positive.

Difference expansion

Expand the marking space by $(2n + 1)$.

- Message separation.

Digital Watermarking and Steganography

by Ingemar Cox, Matthew Miller, Jeffrey Bloom, Jessica Fridrich, Ton Kalker

Chapter 12. Steganography

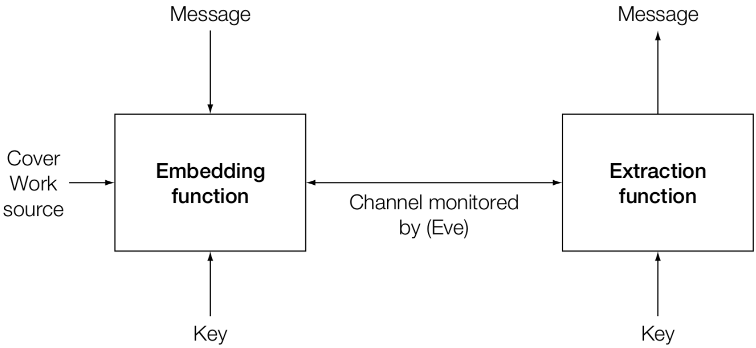
Lecturer: Jin HUANG

2015

Difference to Watermark

- Imperceptible: watermark.
- Undetectable: steganography.

The Model


Message
Message
Cover
Work
source
Embedding
function
Extraction
function
Channel monitored
by (Eve)
Key
Key

The Warden

The warden is part of the channel.

- **Passive**
- Active
- Malicious: trying to impersonate Alice or Bob or otherwise tricking them.

Embedding

The cover work is

- Preexisting, and will not be modified: cover lookup.
- Generated, and will not be modified: cover synthesis.
- Preexisting and modified: cover modification.

Look up

- Labeling work by messages.
- Deliver the messages by sequence of transmission.

Example

- 1024 songs for 10-bit message.
- 1024 sequential transmissions lead to $10k$-bit.

Synthesis

Creates the stego Work without recourse to a cover Work.

British spies in Wold War II

- Source: a big book of conversations.
- By selecting different phrases from the book.

Packed but nature sequence of look up.

Modification

- Type and magnitude of change.
- Location of change
  - Sequential
  - (Pseudo) random: pseudo-random walk.
  - Adaptive: informed.

The Secret Key

Shared between Alice and Bob

- Seed the pseudo-random walk.
- Seed the noise signal.

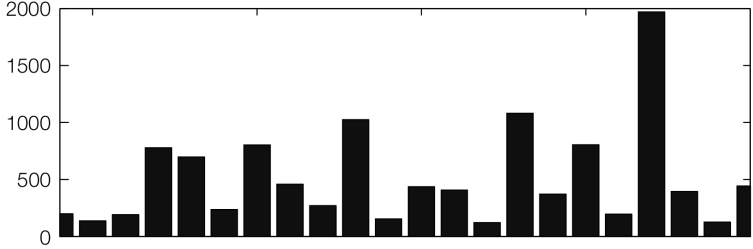
The First Attempt

Using LSB.

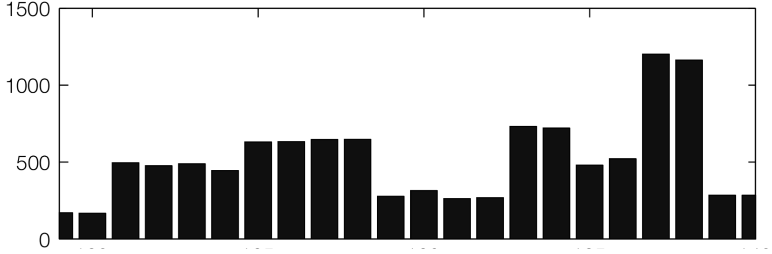
pixel values can be divided into disjoint pairs of values

- $(2i, 2i+1)$
- $2i \to 2i+1 : 1$, $2i+1 \to 2i : 0$.

A Comparison



normal picture



LSB picture

Practical Steganographic Methods

- OutGuess
- Masking Embedding as Natural Processing

For Simple Detection

In a bin consists of a pair of values $(f, \bar{f})$.

In normal work, if $f > \bar{f}$, how much information can be embedded into this bin?

Let fraction α is used to embed

$$f' = f - \frac{\alpha}{2}(f - \bar{f})$$
$$\bar{f}' = \bar{f} + \frac{\alpha}{2}(f - \bar{f})$$

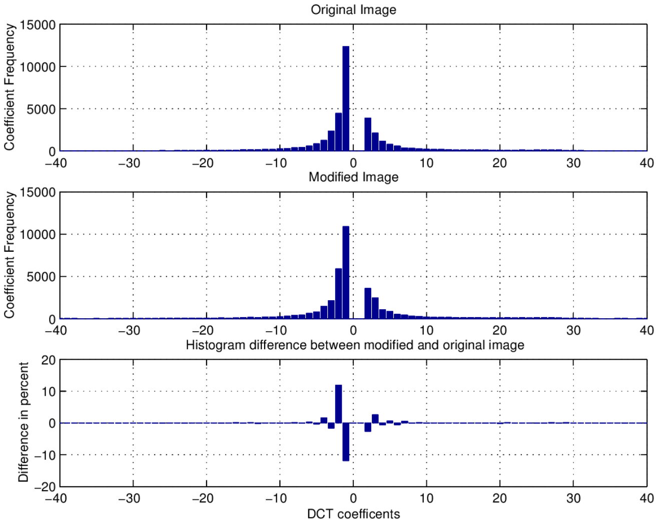
So

$$f' > \bar{f}' \Longrightarrow \alpha \leq \frac{2\bar{f}}{f + \bar{f}}.$$

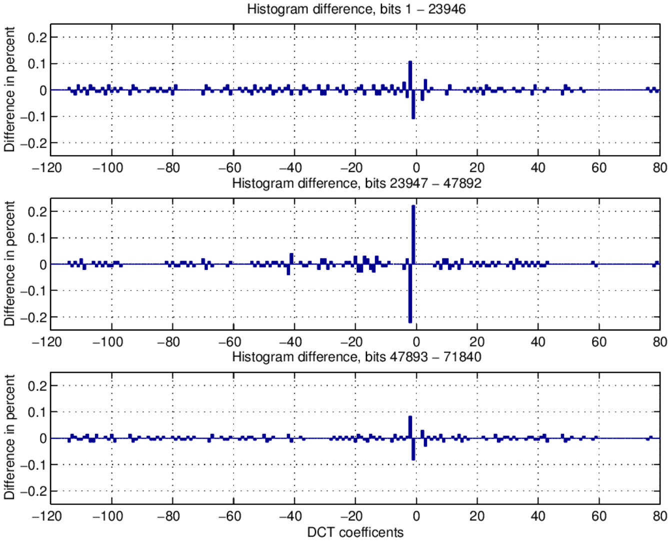
Capacity

- Embedding capacity.
- Steganographic capacity.

Small α


Original Image
Coefficient Frequency
15000
10000
5000
0
−40
−30
−20
−10
0
10
20
30
40
Modified Image
Coefficient Frequency
15000
10000
5000
0
−40
−30
−20
−10
0
10
20
30
40
Histogram difference between modified and original image
Difference in percent
20
10
0
−10
−20
−40
−30
−20
−10
0
10
20
30
40
DCT coefficents

More Advanced Method



Defending Against Statistical Steganalysis.

Basic Idea

Each bin contains a lots of pixel pairs.

- Some of them for embedding.
- Some of them for correction.

Identical histogram

- One embedding goes with one correction.