Digital Watermarking and Steganography

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

Chapter 11. Content Authentication

Lecturer: Jin HUANG

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.

难以抵抗裁剪.

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 $\mathbf{w_r}$.

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

An Example

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

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

会溢出.

- But, the clamping of the value.
- Picking right $\mathbf{w_r}$ to avoid this problem?

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.

操作是否可逆
(溢出)

A Solution

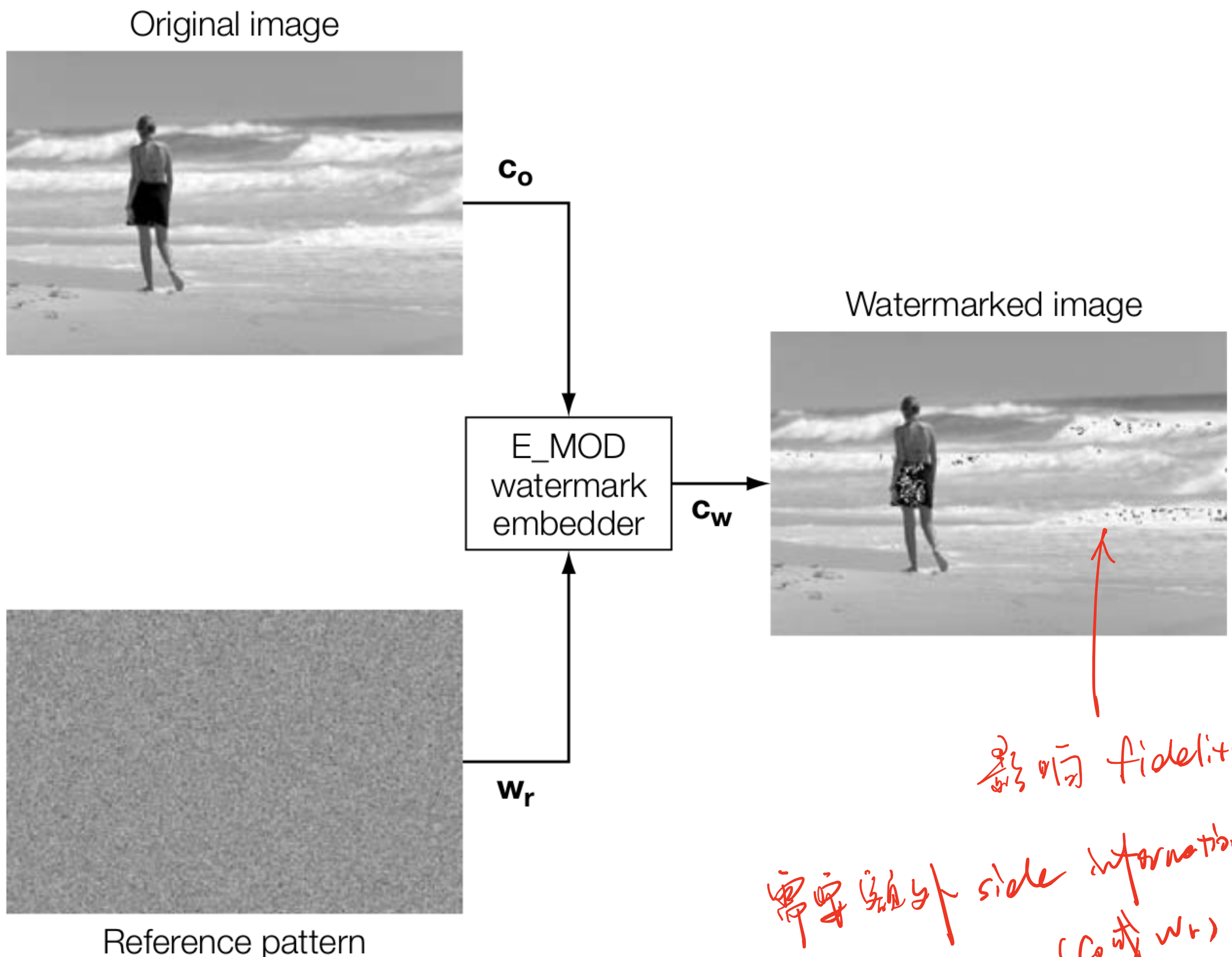
Modulo addition.

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

From the viewpoint of human:

- Salt-and-pepper noise.

Illustration



影响 fidelity.

需要额外 side information
(c_o 或 w_r)

Detection

From the viewpoint of detector:

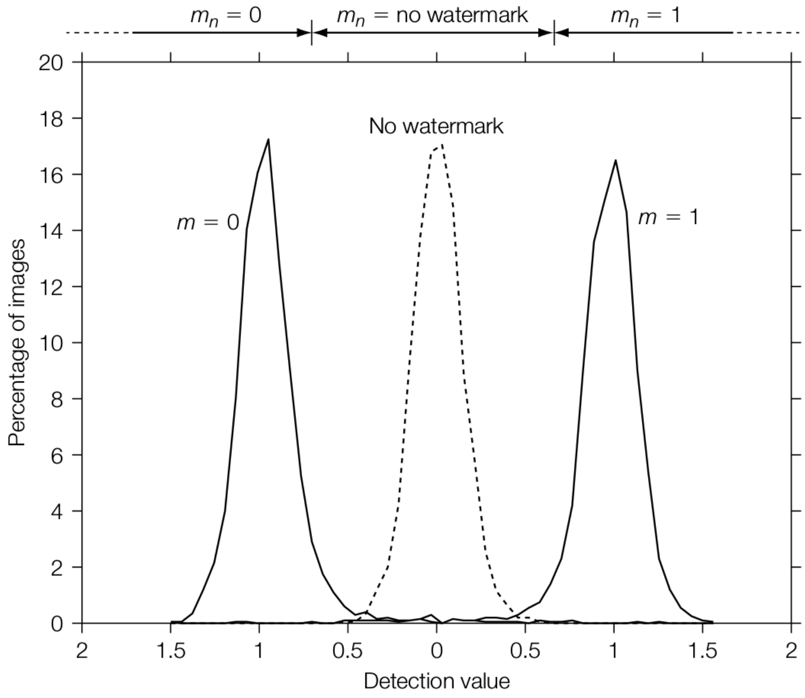
- Introduce some noise: from $253 + 5$ to 3.
- Compare to clamp: $255 \Rightarrow 3$.

Change of $\mathbf{w_r}$

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

Illustration

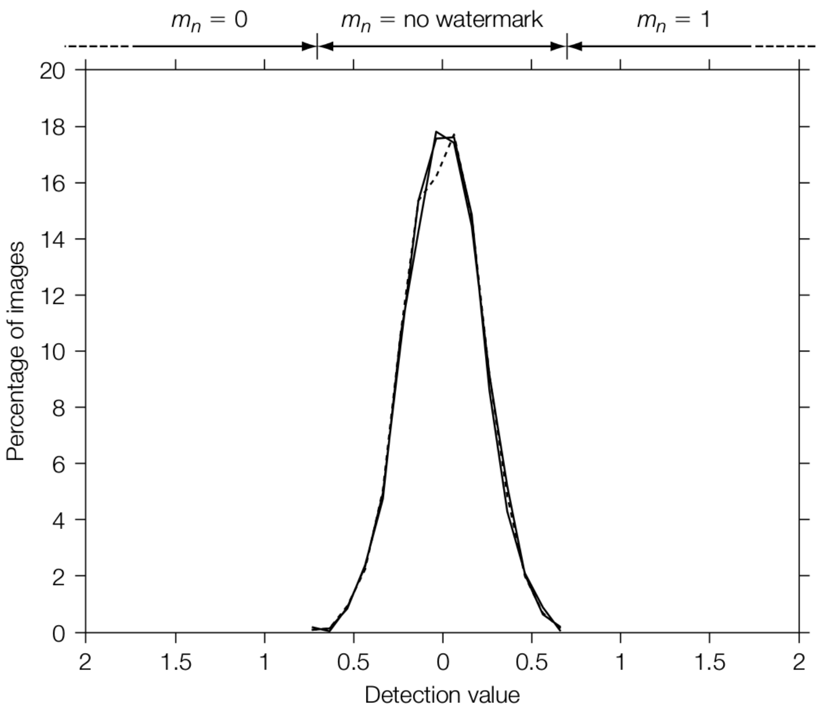
If the values of pixels are far from the borders.



Illustration

If the values of pixels are close to the borders.

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



Practical Solutions for Erasability

隐藏信道：人眼对高频不敏感

放水印.

Difference expansion

- Neighboring pixels are more likely to have similar values. 相邻像素大概率值相似
- Difference between two neighboring pixels has a smaller dynamic range. 相邻像素差为0的正态分布

Using the difference as the channel.

另一种方式拆分低、高频信道

1. 算MD5 2. 插入MD5

信道是一对像素的形式写入

One Bit Only

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

- Transform

$$(y_1, y_2) = T(x_1, x_2) = (\overset{x_1+(x_1-x_2)}{2x_1 - x_2}, \overset{x_2+(x_2-x_1)}{2x_2 - x_1})$$

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

Example:

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

Modulo 3

How to embed?

- Modulo 3: $y_1 - y_2 = 3(x_1 - x_2)$. 差放大三倍.
- embed 1: $y_1 + = 1$.
- embed 0: $y_1 - = 1$.

How to detect?

- $y_1 - y_2 \mod 3$.
  - 0: no message.
  - 1: 1.
  - 2: 0.

Convert It Back

After extracting the message and restore y_1:

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

要先提出message
否则会变成小数

An example

- Embedding 0:

$$c_o = x = (59, 54)$$
$$c_y = Tx = (64, 49)$$
$$c_{y_0} = (63, 49).$$

$\longrightarrow$ 能获得 message 和 C_o.

- Extract message:

被减过！

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

- Recover $\mathbf{c_o}$:

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

Illustration

For More Symbols

更多 symbol

For $2n$ symbols $(-n, \cdots, -2, -1, 1, 2, \cdots, n)$:

$$\begin{aligned}(y_1, y_2) &= T_n(x_1, x_2) \\ &= ((n+1)x_1 - nx_2, (n+1)x_2 - nx_1)\end{aligned}$$

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

Modifying y_1 by at most n.

Embeddable Pixel Pair

如果$2x_1-x_2$, $2x_2-x_1$溢出情况

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?

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

中间差 2n+1 表示没有嵌 message

eg. 255 250

$\Downarrow$

253 250. 差3.

(-2) 嵌入 correction.

MD5信息读完后, 再往后读纠正信息

How to do?

- Modify x_1 to make $x_1 + c - x_2 \mod (2n + 1) = 0$.
- The correct c is part of payload.

Illustration

$n = 3.$

Wait a Moment

It is stupid to make it so complex!

Wait a Moment

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

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

为什么要扩大 difference (eg. 上面的3倍)

因为不扩大得不到 C_0

Benefit

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

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

More Importantly

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

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 $(2n + 1)$.

- Half of pixels are kept, and others become the difference in a small range.
- The difference part is expanded for message separation.