Content

• Introduction
• Obscure SS (OSS)
• Conclusion
Classes of Spread Spectrum Watermarking

Trade-off between usability and error probability

- Non-blind SS: require original images in detection
- Blind SS: Do NOT require original images in detection
- Obscure SS: require Partial Info of original images in detection
  But the info will not disclose the original image
Blind Spread Spectrum Watermarking

SS Model:

Embedding:

Detecting:

if $r = \frac{y^T u}{u^T u} > \tau$, watermark $u$ exists, $b=1$. 

Watermarked image

Original image

Embedding function

Message

$\mathcal{F}(x, w, b)$

$x$

$w$

$s$

$y$

$u$

$\hat{b}$
Improved SS

\[ \mathcal{F}(x, w, b) = \alpha b - \lambda x \]

\[ x = \frac{x^T w}{w^T w} \]

\[ \alpha = \sqrt{\frac{N \sigma_u^2 - \lambda^2 \sigma_x^2}{N \sigma_u^2}} \]

Min FNR:

\[ \lambda_{opt} = \frac{\sigma_x^2 + \sigma_n^2 + N \sigma_u^2}{2 \sigma_x^2} - \sqrt{\frac{(\sigma_x^2 + \sigma_n^2 + N \sigma_u^2)^2}{4 \sigma_x^4} - \frac{N \sigma_u^2}{\sigma_x^2}} \]

\[ p = Pr(r < 0 \mid b = 1) = 0.5 \int_{-\infty}^{+\infty} \frac{1}{\sqrt{2\pi}} e^{-0.5x^2} \, dx \]

With assumption of the normality of original image and noise

\[ SNR = \frac{\sigma_x^2}{\sigma_n^2} = 10 \text{dB}, \quad p = 1.55 \times 10^{-43} \]

Much better than Non-adaptive blind SS (i.e., Fixed F())!

Impractical assumption due to computation error \( q \in [c, -c] \).

\[
\tilde{r} = \frac{y^T w}{w^T w} = \alpha b + (1 - \lambda)x + n + q
\]

\[
f_{\tilde{r}}(\tilde{r}) = f_{r,q}(r + q) = \int_{-\infty}^{+\infty} f_r(\tilde{r} - q)f_q(q) dq
\]

\[
= \int_{-c}^{c} f_r(\tilde{r} - q) \frac{1}{2c} dq = \frac{1}{2c} \int_{-c}^{c} f_r(q - \tilde{r}) dq
\]

\[
= \frac{1}{2c} \int_{c-\tilde{r}}^{c} f_r(r) dr
\]
Content

- Introduction
- Obscure SS (OSS)
- Conclusion
Obscure SS Watermarking

OSS Model:

\[ \mathcal{F}(x, w, b) \]

Embedding:

\[ \mathcal{F}(x, w, b) = \alpha \]
\[ s = x + \alpha w \]

Detecting:

\[ r = y^T u - c_u = (x + \alpha w + n)^T u - c_u \]
\[ = \alpha w^T u + n^T u \]

\[ \hat{b} = \text{sign}(r - \tau) \]
Assume Gaussian noise, and bipolar watermark elements

- No watermark

\[ p_1 = Pr(r_0 > \tau) = Pr(n^T u > \tau) = \frac{\sqrt{2}}{4} \text{erfc} \left( \frac{\tau}{\sqrt{N} \sigma_u \sigma_n} \right) \]

\[ \text{erfc}(x) = \int_x^{+\infty} \frac{2}{\sqrt{\pi}} e^{-t^2} dt \]

- Detecting Watermark ≠ embedded watermark

\[ p_2 = Pr(r_0 > \tau) = Pr(\alpha w^T u + n^T u > \tau) \]

\[ = \frac{\sqrt{2}}{4} \sum_{k=0}^{N} \text{erfc} \left( \frac{\tau - \alpha(N - 2k) \sigma_u^2}{\sqrt{N} \sigma_u \sigma_n} \right) Pr \left( \frac{w^T u}{\sigma_u^2} = N - 2k \right) \]

\[ = \frac{\sqrt{2}}{4} \sum_{k=0}^{N} \text{erfc} \left( \frac{\tau - \alpha N \sigma_u^2 + 2\alpha k \sigma_u^2}{\sqrt{N} \sigma_u \sigma_n} \right) \binom{N}{k} 2^{-N} \]
FNR of OSS

FNR: Watermark is not detected from a watermarked image.

\[ p_3 = Pr(r_0 < \tau) = Pr(\alpha w^T w + n^T w < \tau) \]
\[ = Pr(n^T w < \tau - \alpha N \sigma_u^2) \]
\[ = 1 - \frac{\sqrt{2}}{4} \text{erfc} \left( \frac{\tau - \alpha N \sigma_u^2}{\sqrt{N} \sigma_u \sigma_n} \right) \]
Parameter Selection

\[
\begin{align*}
\{ & p_1 \leq \beta_1 \\
& p_3 \leq \beta_3 \\
& WN = \frac{\alpha^2 \sigma_u^2}{\sigma_n^2} \geq \beta_4^2 \\
\{ & \frac{\tau}{\sqrt{N} \sigma_u \sigma_2} \leq k_1 = \text{erfcinv}(2\sqrt{2} \beta_1) \\
& \frac{\tau - \alpha N \sigma_u^2}{\sqrt{N} \sigma_u \sigma_n} \leq k_3 = \text{erfcinv}(2\sqrt{2} - 2\sqrt{2} \beta_3) \\
& \alpha \sigma_u = \beta_4 \sigma_n
\end{align*}
\]

Min \[ p_2 = \frac{\sqrt{2}}{4} \sum_{k=0}^{N} \text{erfc} \left( \frac{\tau - \alpha N \sigma_u^2 + 2 \alpha k \sigma_u^2}{\sqrt{N} \sigma_u \sigma_n} \right) \binom{N}{k} 2^{-N} \]

\[ = \frac{\sqrt{2}}{4} \sum_{k=0}^{N} \text{erfc} \left( \frac{\beta_4 (\gamma - N + 2k)}{\sqrt{N}} \right) \binom{N}{k} 2^{-N} \]

\[ \tau^* = \alpha \sigma_u^2 \left( \frac{k_3 \sqrt{N}}{\beta_4} + N \right) \]
## Comparison

<table>
<thead>
<tr>
<th>Scheme</th>
<th>FPR₁</th>
<th>FPR₂</th>
<th>FNR</th>
<th>Host</th>
<th>Detector</th>
</tr>
</thead>
<tbody>
<tr>
<td>SS [1]*</td>
<td>Eq.8</td>
<td>Eq.9</td>
<td>Eq.10</td>
<td>All</td>
<td>Non-blind</td>
</tr>
<tr>
<td>ISS [3]⁺</td>
<td>0.5</td>
<td>0.5</td>
<td>≈ Eq.10</td>
<td>N(.)</td>
<td>Blind</td>
</tr>
<tr>
<td>OSS</td>
<td>Eq.8</td>
<td>Eq.9</td>
<td>Eq.10</td>
<td>All</td>
<td>≈Blind×</td>
</tr>
</tbody>
</table>

* The watermark distribution in [1] is normal N(.) , but it is uniform over [−σ_u, σ_u] here. Note that the left-values in Eq.8 and Eq.9 are less than 0.5, i.e., \( p_1 < 0.5 \), \( p_2 < 0.5 \).

+ The FNR of ISS [3] can be adapted to \( p_3 \) by selecting \( \tau \) properly.

× OSS detector knows the index of the original one, but do not know the content. Image search technology can help to index automatically.


Conclusion

• ISS has higher FRR than claimed in practice

• With auxiliary data, OSS has the same performance as SS [1], but content-blind detection
  - OSS needs the index of an image so as to extract auxiliary data
  - Extra storage for indexing
Thanks