Puppy: A Publicly Verifiable Watermarking Protocol
Devriş Işler\textsuperscript{1,2}, Seoyeon Hwang\textsuperscript{3}, Yoshimichi Nakatsuka\textsuperscript{3}, Nikolaos Laoutaris\textsuperscript{1}, and Gene Tsudik\textsuperscript{3}
\textsuperscript{1}IMDEA Networks, \textsuperscript{2}Universidad Carlos III de Madrid, and \textsuperscript{3}University of California, Irvine

**Introduction**

**How to protect the owner against piracy?**

**Ownership via Watermarking**

**Limitation: Public Verifiability**

Scenario: To detect a watermark on an asset,
- Owner has to reveal the watermarking secret;
- Only the intended party (e.g., DM) can run the detection algorithm and verify the claim; and
- Public verification can be done only once.

**Existing Solutions**

- Via a Certificate authority → Trusted Third Party needed
- Adding multiple watermarks on an asset → Limited # of detections
- Via Zero Knowledge Proof → Requires online Owner

Is it possible to convert any symmetric watermarking schemes into publicly verifiable ones without incurring any of these shortcomings?

**Evaluation**

Session Establishment: w/ SGX ~6.50 ms and w/o ~2.20 ms.
Session Termination: w/ SGX ~0.10 ms and w/o ~0.03 ms.

<table>
<thead>
<tr>
<th>WM Type</th>
<th>SGX</th>
<th>Receive Data</th>
<th>Reconstruct</th>
<th>Secret</th>
<th>Detect WM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Freq/WM Dataset</td>
<td>✓</td>
<td>0.53</td>
<td>0.03</td>
<td>0.06</td>
<td></td>
</tr>
<tr>
<td>OBT/WM Dataset</td>
<td>✓</td>
<td>0.31</td>
<td>0.01</td>
<td>0.02</td>
<td></td>
</tr>
<tr>
<td>Num. Database</td>
<td>✓</td>
<td>0.40</td>
<td>0.01</td>
<td>0.05</td>
<td></td>
</tr>
<tr>
<td>Image-WM</td>
<td>✓</td>
<td>0.20</td>
<td>0.0001</td>
<td>0.02</td>
<td></td>
</tr>
<tr>
<td>DNN-WM</td>
<td>✓</td>
<td>14.7</td>
<td>0.04</td>
<td>1.26</td>
<td></td>
</tr>
<tr>
<td></td>
<td>✓</td>
<td>1.44</td>
<td>0.01</td>
<td>0.70</td>
<td></td>
</tr>
<tr>
<td></td>
<td>✓</td>
<td>5040</td>
<td>4773</td>
<td>10333</td>
<td></td>
</tr>
<tr>
<td></td>
<td>✓</td>
<td>358</td>
<td>925</td>
<td>426.6</td>
<td></td>
</tr>
</tbody>
</table>

***All measurement units are in milliseconds (ms).***

**Conclusion**

- [Unlimited Verification] Puppy enables holders to verify a watermarked asset an unlimited number of times.
- [Owner-free Verification] Puppy does not require owners’ online participations.
- [Watermarking Secret Protection] Puppy protects watermarking secret known only by the owner.
- [Watermarked Asset Protection] No other party learns the watermarked asset.
- [Privacy] All communication history between an owner and a holder is kept private.