Attacking and Defending Watermarks

- **Attacks**
  - Ghost Signatures
  - Tampering
  - Forging
- **Defenses**
  - Watermark Obfuscation
  - Multiple Small Watermarks
  - Parity in Watermarks

Ghost Signatures

- Intention: To announce a watermark when there is none
  - So that you may announce it contains your watermark as well
- Methods
  - Starting from solution characteristics, try to figure out the input pattern from current solution
  - Try different signatures, hope for a collision
    - Unlikely
  - Addition of a new signature
    - Easy to disprove

Tampering

- Alter, damage, or remove the watermark
  - Prohibitively large amount of effort required
- Move backwards through design phase
  - Keep going back until before the watermark was added, then remove or replace it at will
- Depend heavily on reverse engineering previous design steps

Forging

- Objective: to subvert proprietor's watermark by inappropriately watermarking other solutions with proprietor's watermark
- Need to Steal the Private Key of an IP Author
- Usually prevented by encryption
- Trying to argue the watermark is present in everyone's IPs. Good luck attacking encryption.

Defense Against Attacks on Watermark

- Watermark Obfuscation
  - Against tampering
  - Make watermark harder to detect
- Multiple Small Watermarks
  - Against tampering
  - Make watermark harder to alter
- Parity in Watermarks
  - Against tampering
  - Detect and repair tampering
  - Often use XOR for parity check (whether sum is odd or even)

Evaluation of Watermarking Techniques

- Proof of Authorship
  - As low as possible
- Err on overestimation when exact value is hard to calculate
- Basically calculate how unlikely it is for the accused to have made the same pattern by pure change.

$$P_c \equiv P(X \leq b) =$$
$$\sum_{i=0}^{b}\left[(C!/(C-i)!*i!)*(p)^{C-i}*(1-p)^{i}\right]$$

‘p’ - probability of satisfying one random constraint by coincidence.
‘C’ - number of imposed constraints.
‘b’ - number of constraints unsatisfied.
‘x’ - random variable, represents how many of the ‘c’ constraints were not satisfied.

Boolean Satisfiability Problem (SAT)

- Set of Variables
  - $U=\{u_1, u_2, \ldots, u_n\}$
  - $u_i = 1$ or 0, $i \in [1,n]$
- Clauses
  - Means logic OR; for example $\{u_1,u_2\}$ means $u_1|u_2$
- Satisfiability
  - Is there an assignment of U that satisfy all clauses?
- Example

$$U=\{u_1,u_2\};C=\{\{u_1,u_2\},\{\overline{u_1}\},\{\overline{u_1},\overline{u_2}\}\}$$

$$U=\{u_1,u_2\};C=\{\{\overline{u_1},u_2\},\{u_1\},\{\overline{u_1},\overline{u_2}\}\}$$

Example from ref[1]

Method to Add Constraint

- Assuming function of the IP is described by example problem to the right
- Task: To modify this SAT problem so that
  - Any solution to modified problem satisfies old problem
  - Both modified problem and solution contain information uniquely identifying author

$$
\begin{aligned}
U =&\{u_1, u_2, \ldots, u_{14}\}\\
C =&\{\{\bar{u}_1\bar{u}_2u_9\}, \{\bar{u}_1\bar{u}_3\bar{u}_4\}, \{\bar{u}_1u_2\bar{u}_5\}\\
&\{u_1\bar{u}_2u_{10}\}, \{\bar{u}_1\bar{u}_3u_8\}, \{\bar{u}_1\bar{u}_3u_7\}\\
&\{u_1\bar{u}_5u_7\}, \{\bar{u}_1\bar{u}_6\bar{u}_{12}\}, \{\bar{u}_1u_{10}u_{12}\}\\
&\{\bar{u}_1u_6u_9\}, \{\bar{u}_2\bar{u}_3\bar{u}_{10}\}, \{u_2\bar{u}_5\bar{u}_{14}\}\\
&\{\bar{u}_2u_7u_8\}, \{u_2\bar{u}_8u_9\}, \{u_3u_4u_8\}\\
&\{u_3u_5\bar{u}_7\}, \{\bar{u}_3u_8u_{13}\}, \{u_3\bar{u}_9\bar{u}_{11}\}\\
&\{u_3u_{10}\bar{u}_{12}\}, \{\bar{u}_4\bar{u}_7\bar{u}_8\}, \{\bar{u}_5\bar{u}_8\bar{u}_{12}\}\\
&\{u_4\bar{u}_7u_{13}\}, \{\bar{u}_5\bar{u}_9\bar{u}_{11}\}, \{\bar{u}_5u_7u_9\}\\
&\{u_6u_{10}u_{11}\}, \{u_6\bar{u}_8\bar{u}_{12}\}, \{u_7u_9\bar{u}_{12}\}\\
&\{u_7u_9\bar{u}_{13}\}, \{u_9u_{11}\bar{u}_{14}\}, \{u_{10}u_{11}\bar{u}_{12}\}\}.
\end{aligned}
$$

Figure from ref[1]