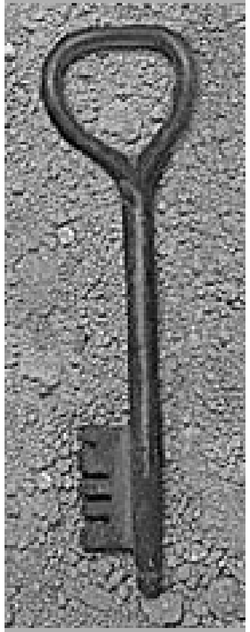
Some General Methods for Tampering with Watermarks

Cox, I.J.

Linnartz, J.-P.M.G.

IEEE Journal on Selected Areas in Communications, May 1998

Presented by Yizhe Lin



Summary

The paper introduces

- The usage of watermarks for DVD video copy protection, and
- Some general methods to break such protection.

Watermarks in DVD video copy protection

- Watermarks can be embedded in digital or analog content.
- The embedded watermarks can carry copyright control information such as ‘copy once’ or ‘never copy’.
- This information will tell compliant recorders not to illegally copy or play.

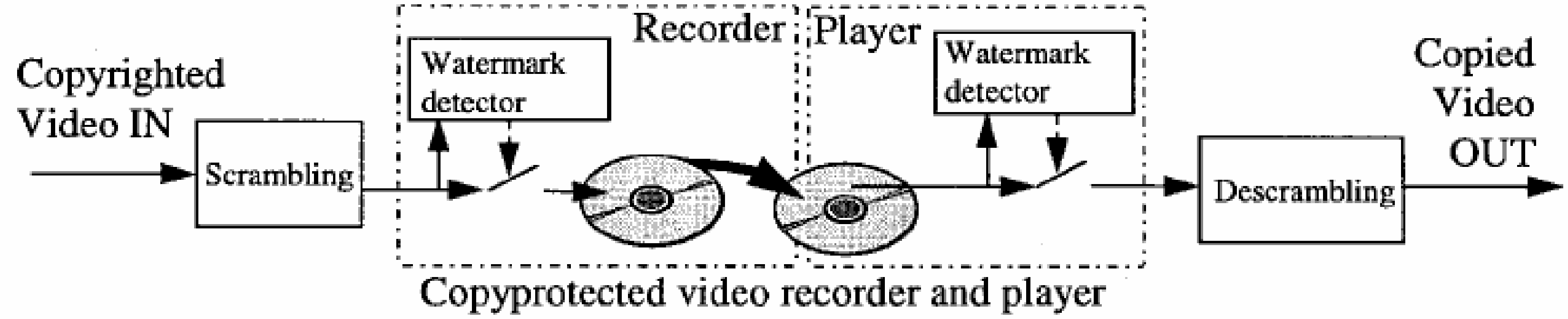
Attacks: removing

1. Experimentally deduce the behavior of the detector, discover a pattern that will cancel out the watermark.
2. Compare the content before and after the watermark insertion. The difference can be used to pre-distort the original to undo the insertion.
3. Use statistical averaging to estimate the watermark.

Attacks: bypassing

1. Block the output of the detector.

2. Pre-scramble the signal before recording.



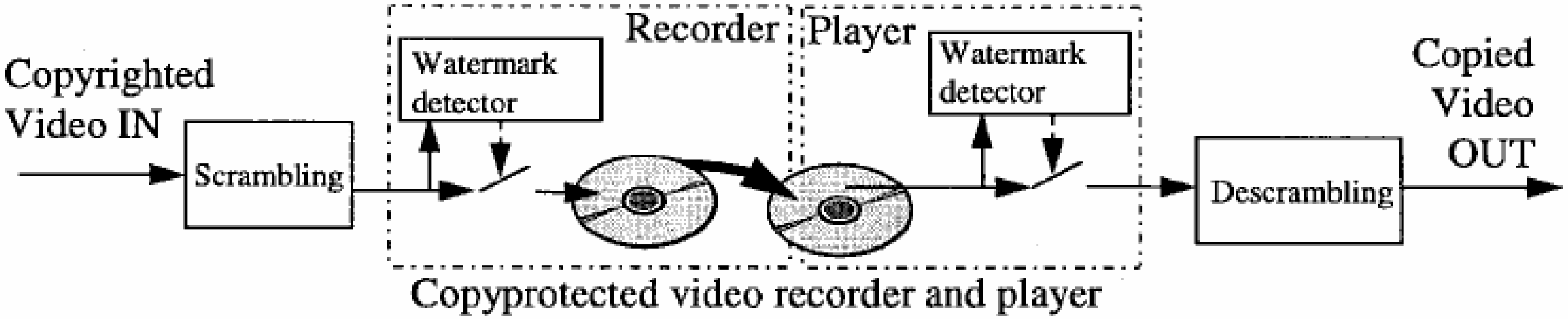
Appreciative comment

- The article was written in a clear, well-organized manner. After introducing some possible attacks, the authors concluded that watermarking is a useful technology but also a one that cannot be absolutely secure.
  - "Legal, economic, and technological efforts are all needed to prevent and/or deter piracy."

Critical comments

- The title is too broad
  - – The paper only addressed to digital watermark in the context of DVD video copy protection.
  - – Video, audio, image, software watermark etc.
  - – To prove the ownership, to verify the content etc.
- "…, the attacker can estimate both the sum and difference of p_1u_1 and $(1-p_1)u_2$. This reveals u_1 and u_2. "
  - – there are three variables but only two equations.

Question



This type of attack is very easy to carry out by ordinary users. It poses a fundamental threat to the DVD copy protection.

Is it possible to refute this kind of attack? What could be the counter-measure?