Some General Methods for Tampering with Watermarks

Ingemar J. Cox

Jean-Paul M. G. Linnartz

IEEE Journal on Selected Areas in Communications 16(4):587-593, May 1998

Presented by Siriwat Karndacharuk

Summary

- How a watermark can be resistant to tampering, together with some possible attacks.

Motivation

“… professional piracy is unlikely to be prevented by technological means alone, it is hoped that the illegal casual copying that occurs in the home can be prevented …”

Three lines of defence for illegal DVD copying

1. Encryption
2. Analog Protection System (APS)
3. Watermark
   - Prohibit an illegal copy from being played on a compliant device

     [The users will have a choice between]
     - A compliant device that can play an original copy
     - A non-compliant device that can play a pirated copy, but not the original one.

Critical Comments

- Unintuitive referencing
  - Under section V p.589, “The above specification may not seem difficult since it only requires the embedding of 4 bits …”
  - “The specification mentioned in section III” should be used instead.
- Missing the source
  - On p.589-590, “… 4 bits of information in the data stream, and if the detection is only expected every 10 s say, then the total video data is approximately 720 x 480 x 30 x 10.”

1st Appreciative Comment

- Unambiguous terminologies are suggested.
  - Unrestricted-key watermark
  - Restricted-key watermark

1st Appreciative Comment (cont.)

- Before May 1998, the watermarks that are readable by many detectors were called “public”.
- For those that are readable by limited number of detectors were called “private”.

- This might cause a confusing since the currently known watermarks (up to May 1998) fell into the category of secret key cryptographic algorithm.
- Which means the keys for both public and private watermarks were actually “private”.

1st Appreciative Comment (cont.)

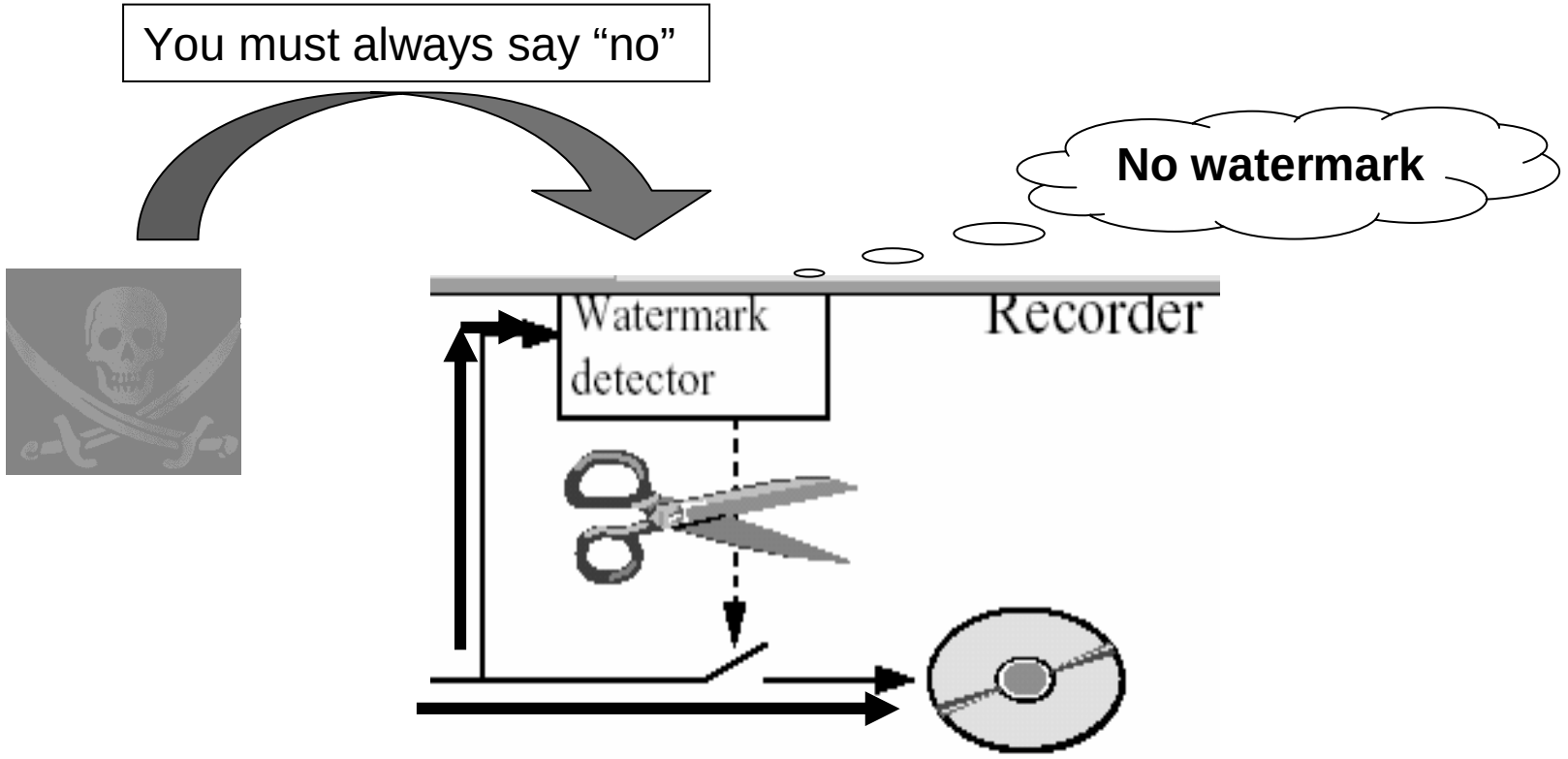
- “Unrestricted-key watermark” is proposed to be used instead of “public watermark”.
- “Restricted-key watermark” is proposed to be used instead of “private watermark”.

2nd Appreciative Comment

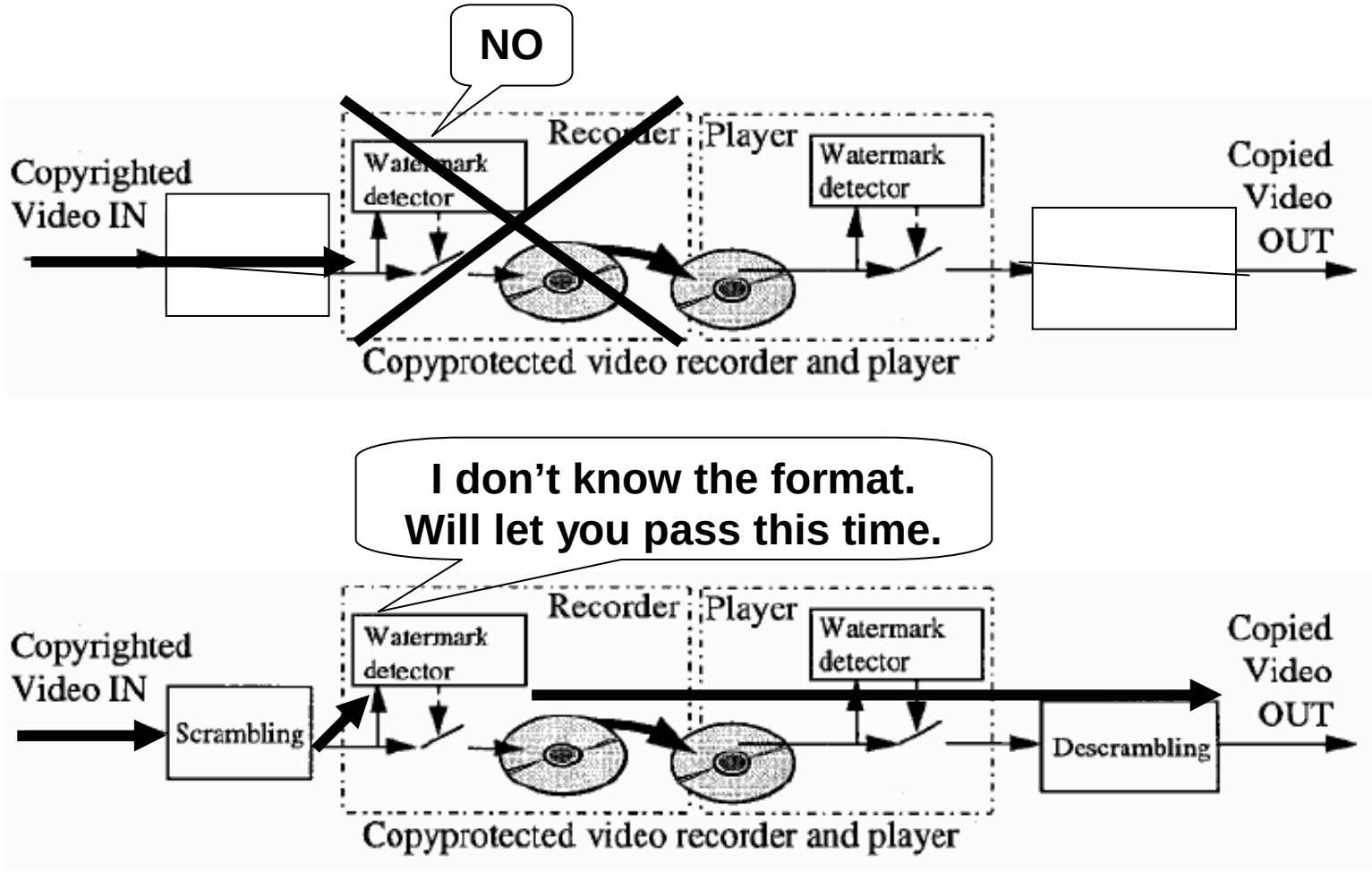
- The information that worth mentioning

> “… if a watermark detection algorithm could be placed in a perfectly tamperproof box, this does not necessarily imply that the attacker cannot find a method to remove the watermark.”

How to circumvent the watermark



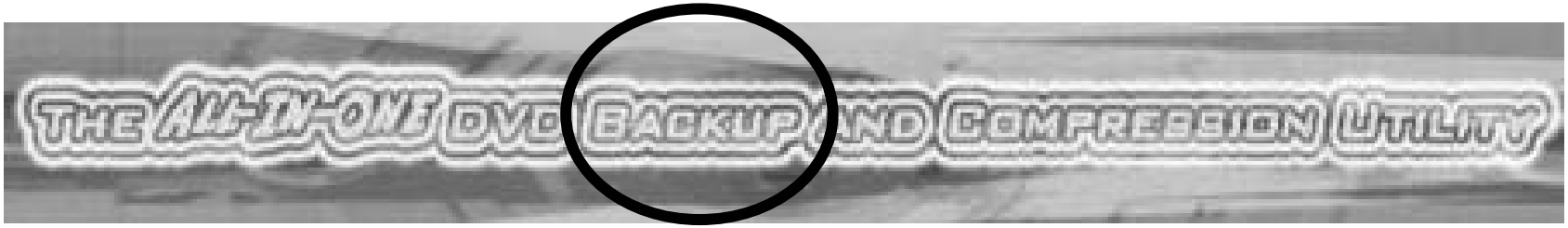
How to circumvent the watermark detector



1st Real life example

- Example of an advertisement on the internet.

2nd Real life example



1st Question

- How can we reduce the number of users who are trying to pirate the digital contents?

1st Question (cont.)

- Legal
  - Increase the penalty
- Economics
  - Reduce the price of the genuine softwares
- Ethics
- Technology

2nd Question

- Do you think the paper will lead to the increasing of new software crackers?

  Why?