Research on Re-shooting Countermeasures

Isao Echizen
National Institute of Informatics, Tokyo, Japan

Background: analog-hole problem

Conventional problem

- Originally intended to resolve security problems with analog-output terminals of digital equipment
- Resolution by replacement of digital terminals

Rise of new problem exploiting monitors and screens

- Trend of increasingly high-quality monitors and cameras makes it easy to reshoot presented content -> Distribution of illegally <u>re-shot</u> content
  Ex. re-shoot PC monitors with cell-phone cameras -> upload shot content
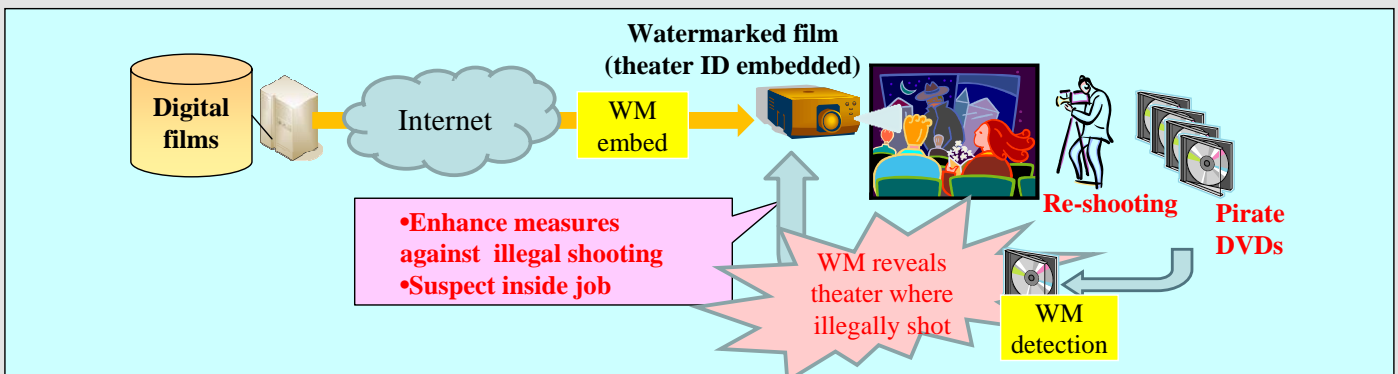 Ex. re-shoot theater screens -> sell pirate DVDs

  Loss of USD 3B per year (survey of Motion Picture Association of America)
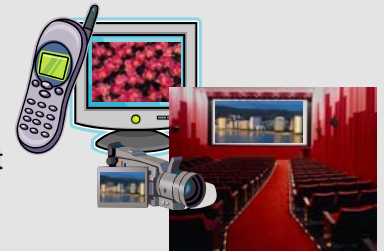
Conventional measures against re-shooting: use of digital watermarks

- Embed theater ID WM into digital cinema film
- Detect WMs in pirate DVDs and identify flow of illegal distribution

➡ But: no control of re-shooting

Watermarked film (theater ID embedded)

Digital films — Internet — WM embed

- Enhance measures against illegal shooting
- Suspect inside job

WM reveals theater where illegally shot

Re-shooting → Pirate DVDs → WM detection

Re-shooting countermeasures based on difference between sensory perceptions of humans and devices

Objective

- Establish countermeasure to stop re-shooting
  No new function is added into existing user-side device (ex. cam)

Approach

- Use of difference between sensory perceptions of humans and devices
  - Destroy shot content using invisible signals which add noise to content shot through CCD/CMOS devices
  - Near-infrared signals: CCD and CMOS react to them

Human-based perception

Device-based perception

Signal to be generated

Near-infrared signals

Unit of infrared light emission

100-inch screen

Beamer