FACULTY OF ENGINEERING
AND ARCHITECTURE

IDLab
INTERNET & DATA LAB

Hannes Mareen, Johan De Praeter, Glenn Van Wallendael and Peter Lambert

Multimedia Forensics:

identifying digital **pirates** using a novel **watermarking** technique

True Story

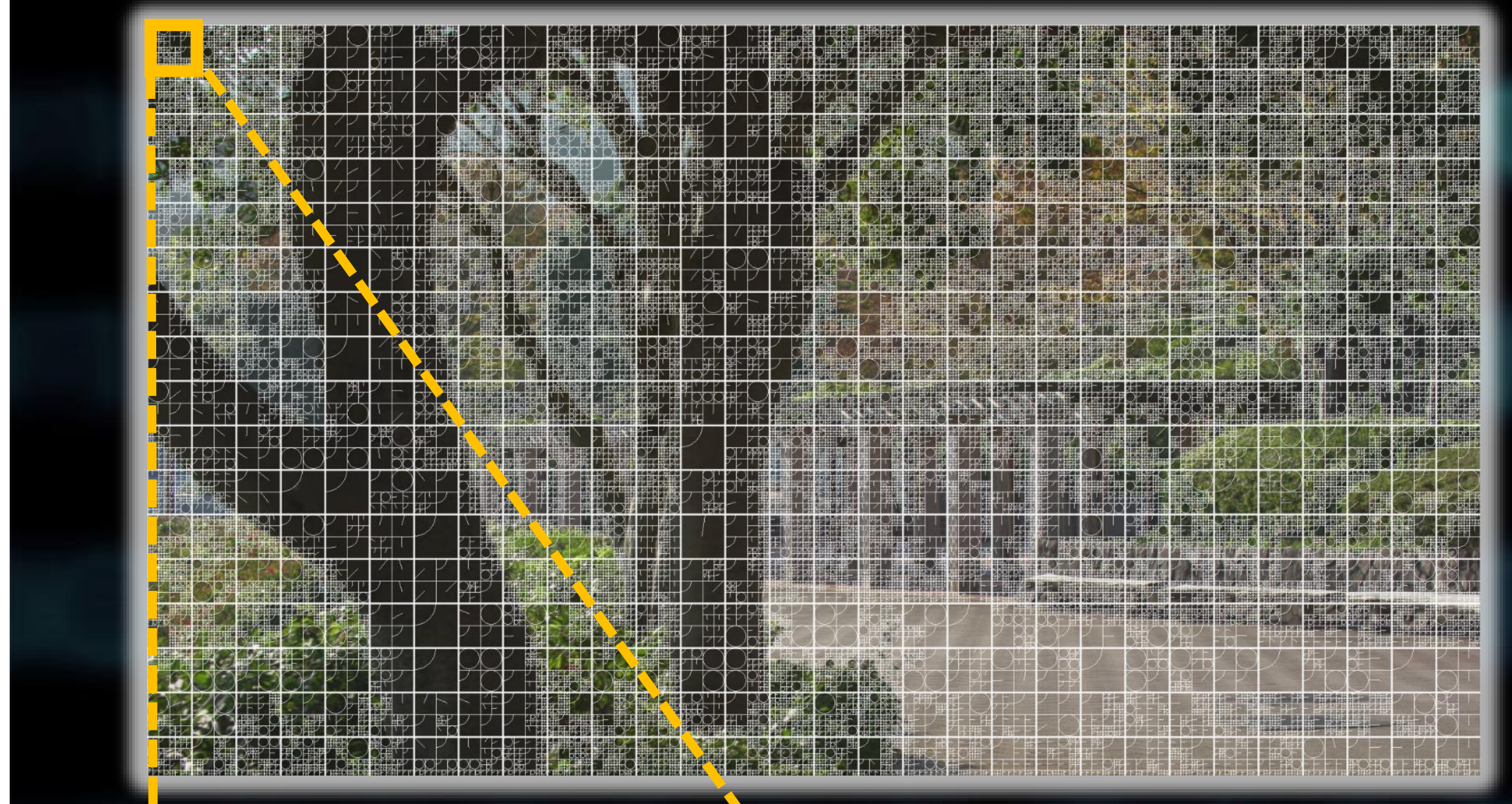
- In 2015, episodes of Game of Thrones were **leaked** before the official release date. These were screener episodes, sent to the press such that they could write a review about them.
- Every reviewer received the video with a **unique watermark** or **fingerprint**: the reviewer's name was inserted as text into the video. In this way, he could be **identified** if he would leak the video.
- However, the reviewer simply **deleted** this watermark by blurring the text, making him unidentifiable.

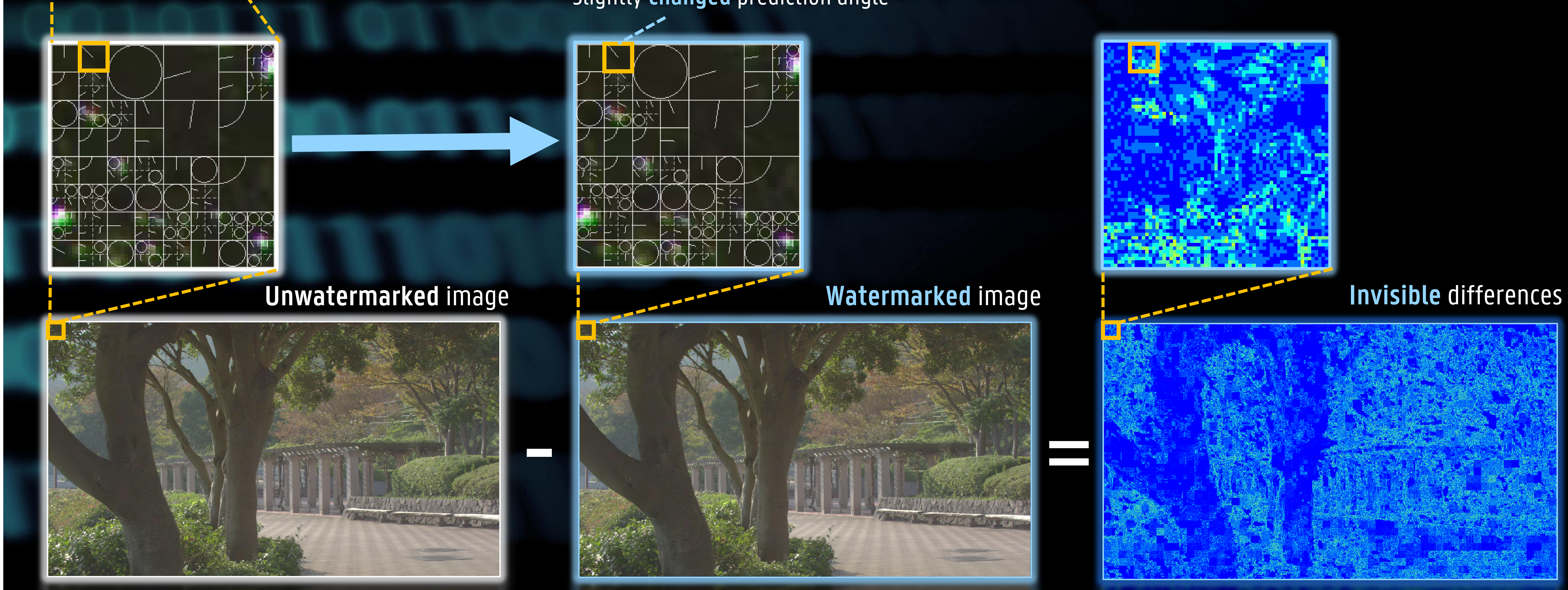
Proposed Technique

- A video encoder compresses a video by predicting every block in the video based on neighboring blocks.
- I slightly **change a single** encoder decision, while keeping the rest unchanged.
- This change **results in many** different predictions, or **compression artifacts**, that represent the watermark.

The Advantages

- ✓ **Invisible**
- ✓ **Applicable on a large scale**
- ✓ **Robust:** I can identify the **pirate** even when he tries to delete the watermark by reducing the quality of the video, like this:





Can you spot the differences?

Background image: "Security IT Symbol" by Christoph Scholz, www.flickr.com/photos/140988606@N08/28636420462 (CC BY-SA 2.0)
Icon with magnifying glass: "Search" by Luis Prado, www.thenounproject.com/term/search/176556 (CC BY-SA 3.0 US)
Images with and without watermark: "ParkScene" by Tokyo Institute of Technology, Nakajima Laboratory
Game of Thrones introduction image: property of Home Box Office

GHENT
UNIVERSITY

imec