

Introduction to Information Hiding

Guest Lecture for CS555 Cryptography

Mercan Topkara

CERIAS

Purdue University



02.10.2005

PURDUE
UNIVERSITY

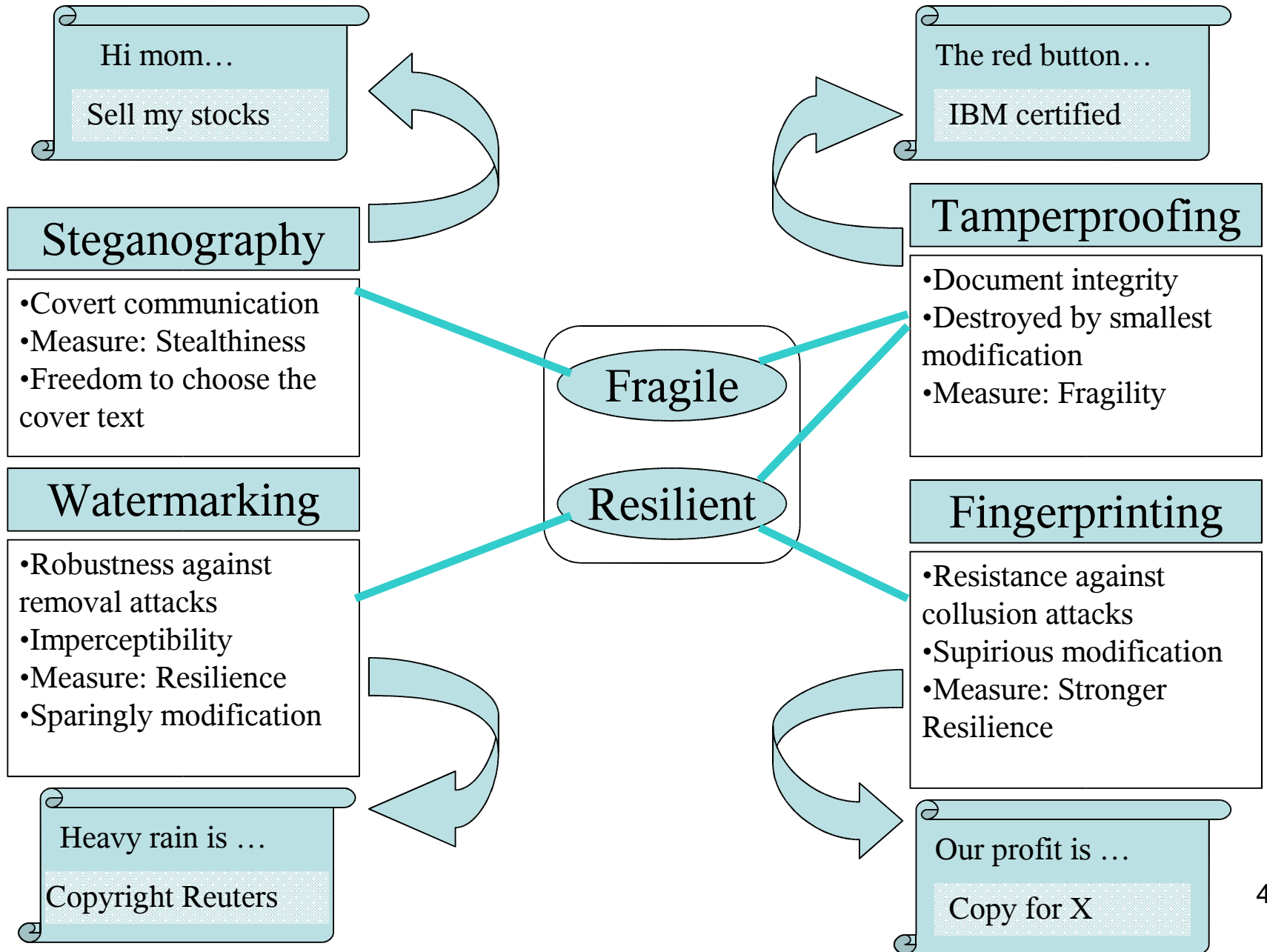
Outline

- **Information Hiding in General**
- **Steganography**
 - Case study (Image and Linguistics Steganography)
- **Watermarking**
 - Case Study (Image and Natural Language Text Watermarking)
- **General Look at the Current Information Hiding Research**
- **Discussions and Conclusion**

Why Information Hiding?

- **Can you give some examples?**
- **Why do you think we need information hiding?**
- **Can you think of any alternative ways of solving these problems without information hiding?**

Information Hiding



Digital Media

- **Audio, Image, Video, Text, etc.**
- **Easy to create perfect copies**
- **Easy to distribute via Internet**

Steganography

- **Secret writing:**
 - **Covert communication**
- **Tattoo of the slave (400 BC)**
- **Prisoner's problem**



Alice



Bob



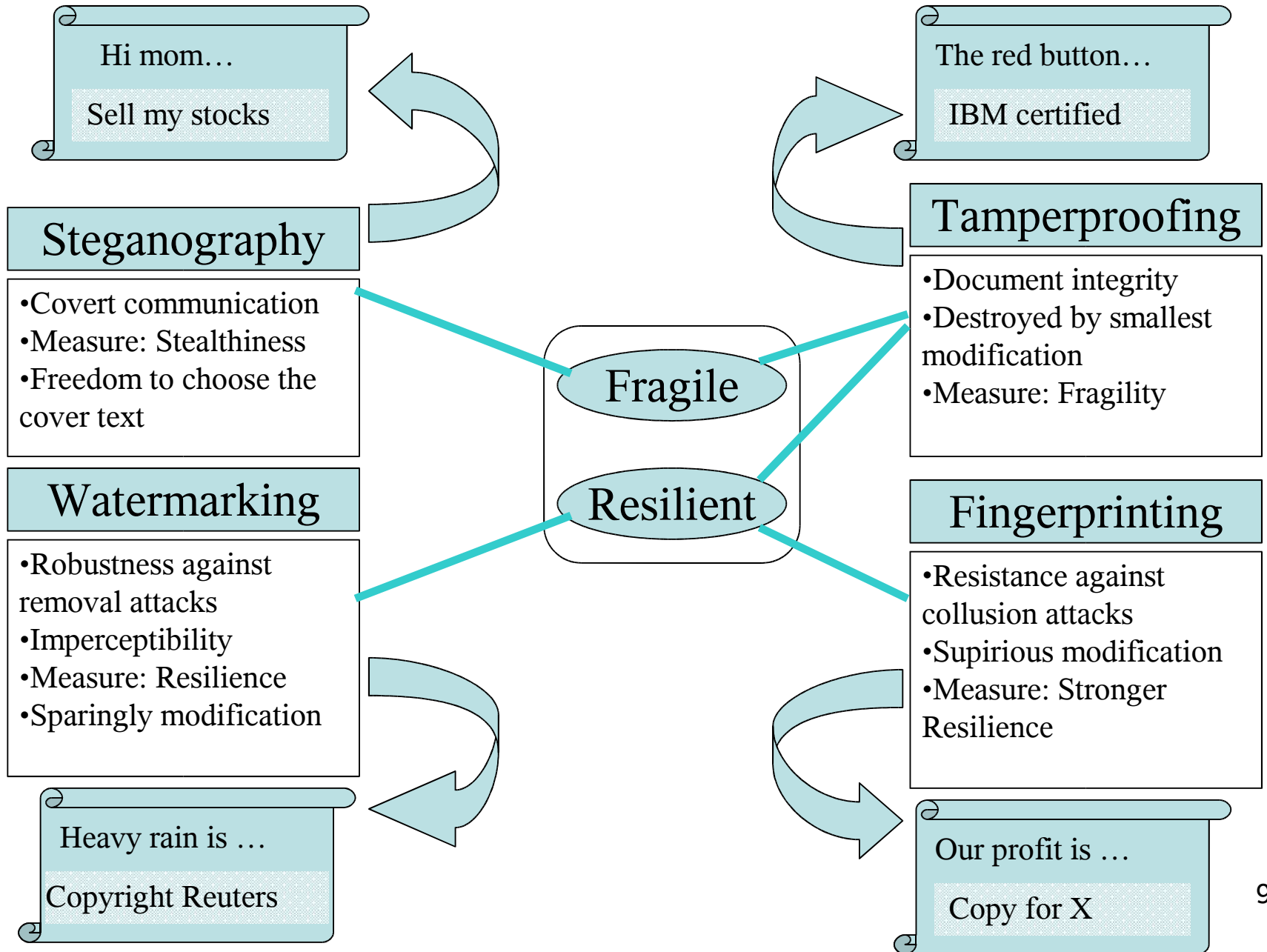
Warden



Discussions

- **Why do we need steganography in real life?**
- **How can we make use of it in solving real life problems?**

Information Hiding



Watermarking

- **Hiding a message signal into a host signal, without any perceptual distortion of the host signal.**
- **The mark itself is “transparent” or unnoticeable for the human perception system.**
- **The roots of watermarking are considered to be in the study of “Steganography”.**

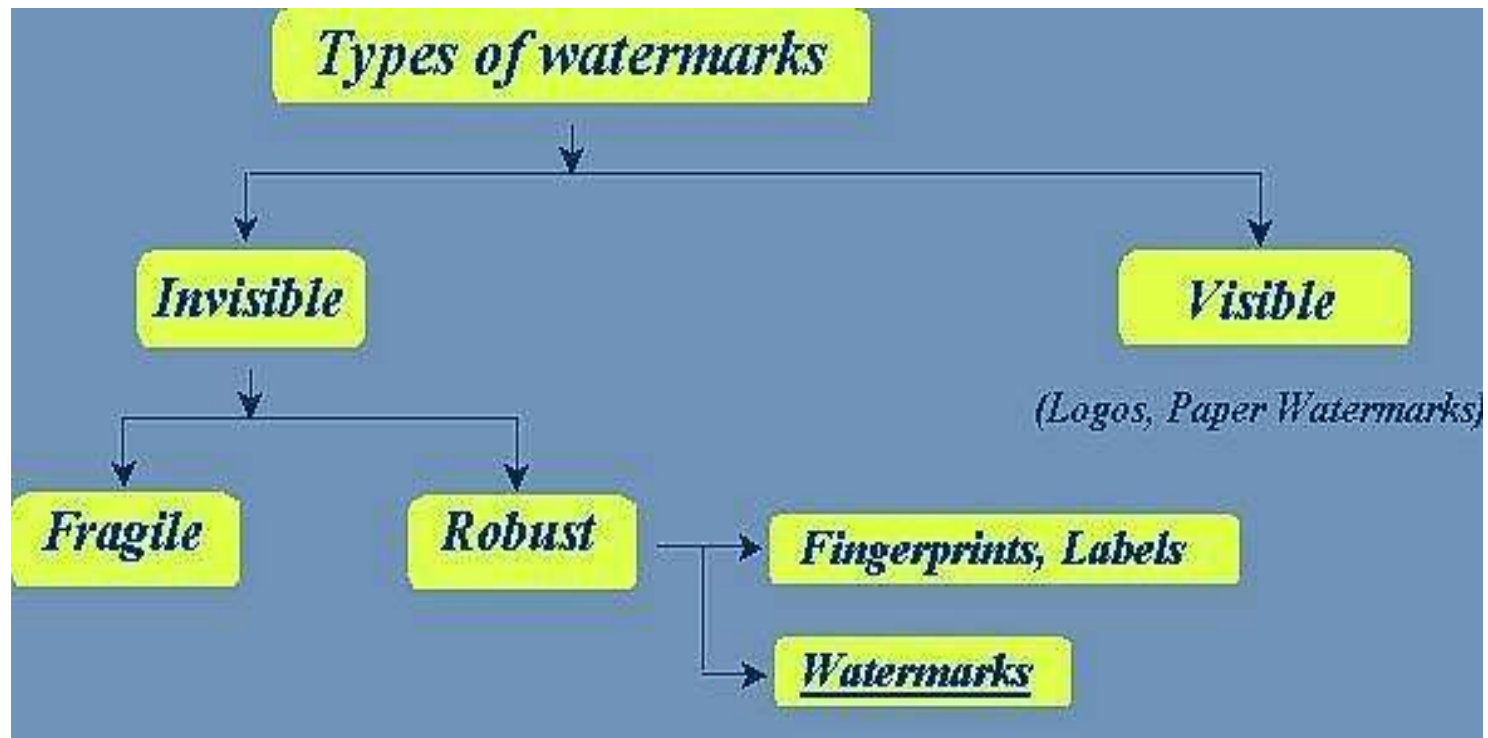
Rules of The Game for Watermarking

- This is not a “security through obscurity” game.
 - “*Navajo code breaking*”
- Only the **key** remains **secret**.
- Other information e.g. Insertion Algorithm, Databases, transformations are **public**.
- **Attacker** can apply transformations to the object.
- **Attack is successful** when watermark is broken.

Requirements of Watermarking

- **Robustness**
 - Watermark cannot be destroyed by modifying the watermarked object
- **Security**
 - Watermark payload must remain secret
 - Unauthorized embedding should be prohibited
- **Imperceptibility**
 - Watermark is not perceptible.

Watermarking for a Reason

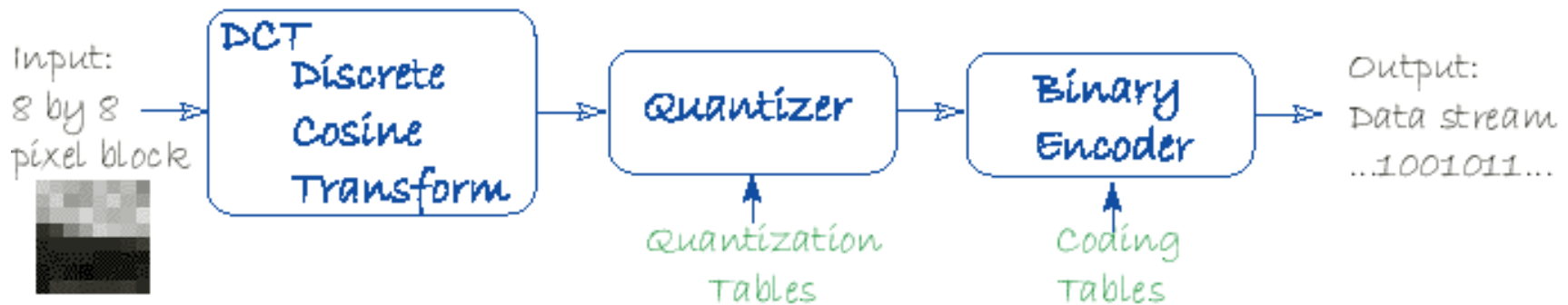


Discussions

- **Why do we need watermarking in real life?**

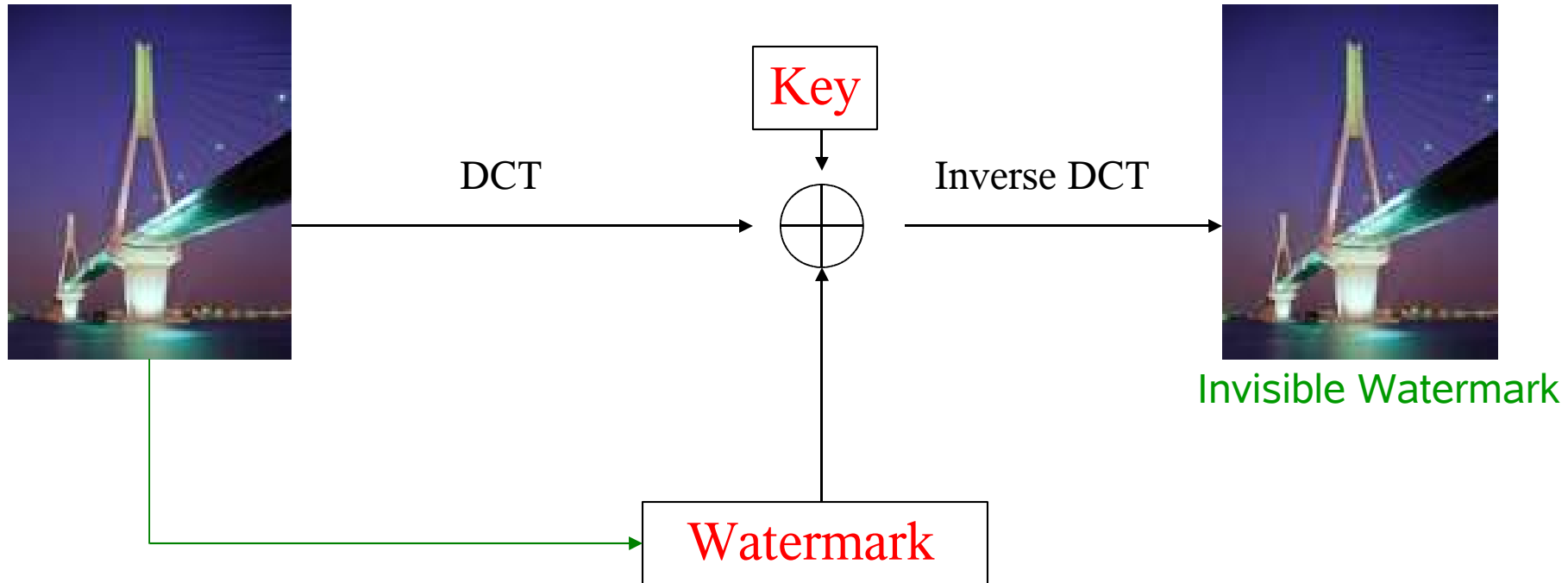
Image Watermarking

Image Processing (JPEG)



- **JPEG divides up the image into 8 by 8 pixel blocks**
- **Calculates the Discrete Cosine Transform (DCT) of each block**
- **A quantizer rounds off the DCT coefficients according to the quantization matrix**
 - This step produces the "lossy" nature of JPEG, but allows for large compression ratios.
- **For decompression JPEG recovers the quantized DCT coefficients from the compressed data stream and takes the inverse transforms and displays the image.**

Inserting Watermark Bits to an Image



Example of a Visible Watermark



Attacks and Benchmarks

- **Statistical Attacks**
 - Chi-square attack, RS analysis etc.
- **Additive Attack**
 - Adding another watermark on the watermarked object
- **Mosaic Attack**
 - Slicing up the image into pieces
- **StirMark Benchmark 4 :**
 - includes several attacks and in particular the random geometric distortions that still defeat many schemes!
- **Watermark Evaluation Testbed**
 - www.datahiding.org

Natural Language Text Watermarking

Natural Language Text Watermarking I

- **Watermark is inserted using appearance of text elements**

space (e.g., line and word distances)

formulas

text: "Die Verallgemeinerung des ..."

figures and tables

PDF specific: hyperlinks

- **Easy to remove using Optical Character Recognition techniques**

Natural Language Text Watermarking II

Discussion

- **Why do we need NL watermarking?**
- **Why is it tough?**

Excerpts from Prof. Ed J Delp:

Important Application Domains

- **Authentication**

- People, data, and physical objects
- Surveillance
- Biometrics
- “things” (rfid)

- **Forensics**

- Data, e.g. Medical Imaging
- Forgery of “events”
- Content tracking

Excerpts from Prof. Ed J Delp:

Application Domains (Cont.d)

- **Privacy**
 - Remote Sensing
 - Databases (degradable content)
 - Mobile Systems and Sensor Networks
 - Sensors are everywhere
- **Data Hiding - Data Channel**
 - Meta-data binding
 - Steganography
 - Auxiliary Channel for “measurements”

Keywords and Quick References

- **Keywords:**
 - **Information hiding, data hiding, steganography, steganalysis, covert communication, digital watermarking, fingerprinting, traitor tracing, broadcast monitoring, meta-data binding**
- **A few links to start reading about watermarking:**
 - <http://stargate.ecn.purdue.edu/~ips/> (Viper Lab)
 - http://www.research.ibm.com/image_apps/watermark.html (IBM Labs)
 - <http://www.petitcolas.net/fabien/steganography/> (Fabien Petitcolas Microsoft)
 - <http://www.watermarkingworld.org/>
 - <http://www.wipo.int/> (World Intellectual Property Organization)
 - <http://www.digimarc.com/watermarking/techOverview.asp> (Digimarc)
 - <http://www.datahiding.org> (Watermark Evaluation Testbed Purdue University)

Questions and Ideas