Trusted Watermarks

Andreas Brett, Nicolai Kuntze, Andreas U. Schmidt

Fraunhofer Institute for Secure Information Technology SIT, Darmstadt, Germany

Introduction

- P2P: successful content distribution method
- especially for larger amounts of data
- allows for omitting expensive server infrastructures
- network load is balanced towards clients
- can thus be used in scalable video/audio on-demand systems
- but also introduces security issues
- e.g. content and device integrity have to be ensured

Objectives

- develop a video on-demand system based on P2P
- ensure content and device integrity
- modified Set-Top-Boxes are banned from sharing
- prevent copyright violation
- in a customer-friendly and non-restrictive manner

Methods

Trusted Computing for securing integrity

- incorporates Integrity Measurement Architecture (IMA)
- prevents adversaries from...
  a) modifying Set-Top-Boxes to retrieve unmarked content
  b) distributing forged content
  c) deploying own content (broadcast hijacking)

Digital Watermarking for protecting content from theft

- does NOT restrict content usage (unlike common DRMS)
- content is usable on any playback device
- but is marked with consumer-specific metadata
- allows to trace source of copyright violation

Details

- virtualization of a TPM-equipped System
- passing software TPM emulator to QEMU
- implementation of Trusted Computing Protocols
  1) AIK-Certification
  2) Remote Attestation
- verification of Set-Top-Box integrity (Integrity Measurement)
- distribution of AES encrypted video chunks
- specifically binding encryption and watermark keys to a Set-Top-Box's TPM
- client-side watermarking (personalized watermarks; reduced server load)
- demonstrative image watermarking method for MJPEG video formats

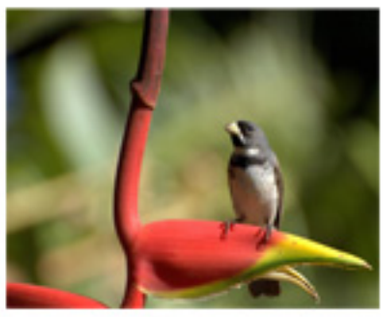

FIG. 1: SMOOTH-EDGE-DETECTION ALGORITHM

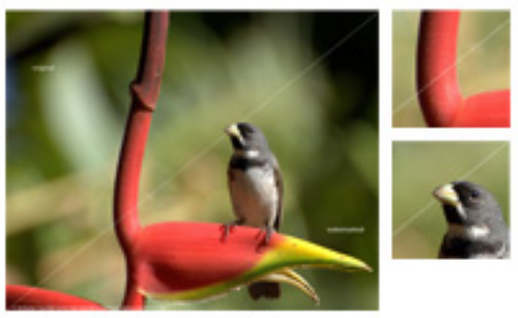

FIG. 2: WATERMARK PERCEPTIBILITY

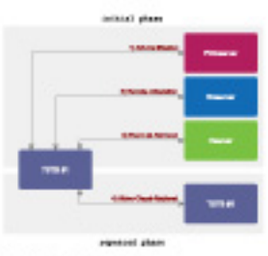

FIG. 3: PROTOCOL FLOW

FIG. 4: USAGE SCENARIO

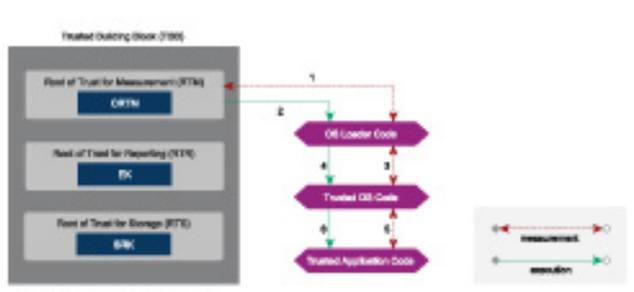

FIG. 5: TRANSITIVE TRUST

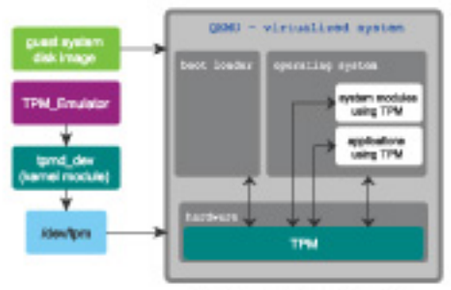

FIG. 6: TPM VIRTUALIZATION

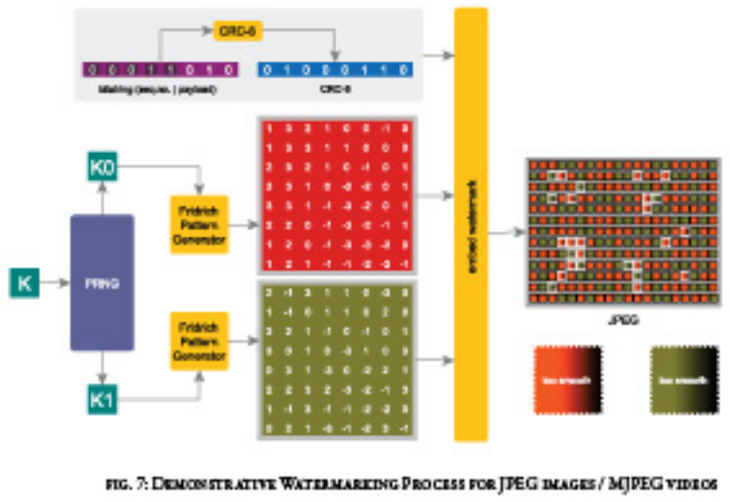

FIG. 7: DEMONSTRATIVE WATERMARKING PROCESS FOR JPEG IMAGES / MJPEG VIDEOS

Conclusions

We have shown a solution to improve media distribution by...

a) rerouting server load towards clients (reduced costs)

b) preventing copyright violation / fraud (marked content)

c) enhancing customer-experience at the same time (non-restrictive content)

Fraunhofer Institute for Secure Information Technology SIT

Dr. Andreas U. Schmidt

Dipl. Inform. Nicolai Kuntze

http://www.sit.fraunhofer.de

Fraunhofer Institut Sichere Informations-Technologie