ITU-T

International Telecommunication Union
International Multimedia Telecommunications Consortium

JPSEC: Security for Digital Imagery in JPEG 2000

Susie Wee* & John Apostolopoulos

* Director, Mobile & Media Systems Lab
HP Labs

* Co-Editor of JPSEC

Joint ITU-T Workshop and IMTC Forum 2006 "H.323, SIP: is H.325 next?"
San Diego, 9-11 May 2006

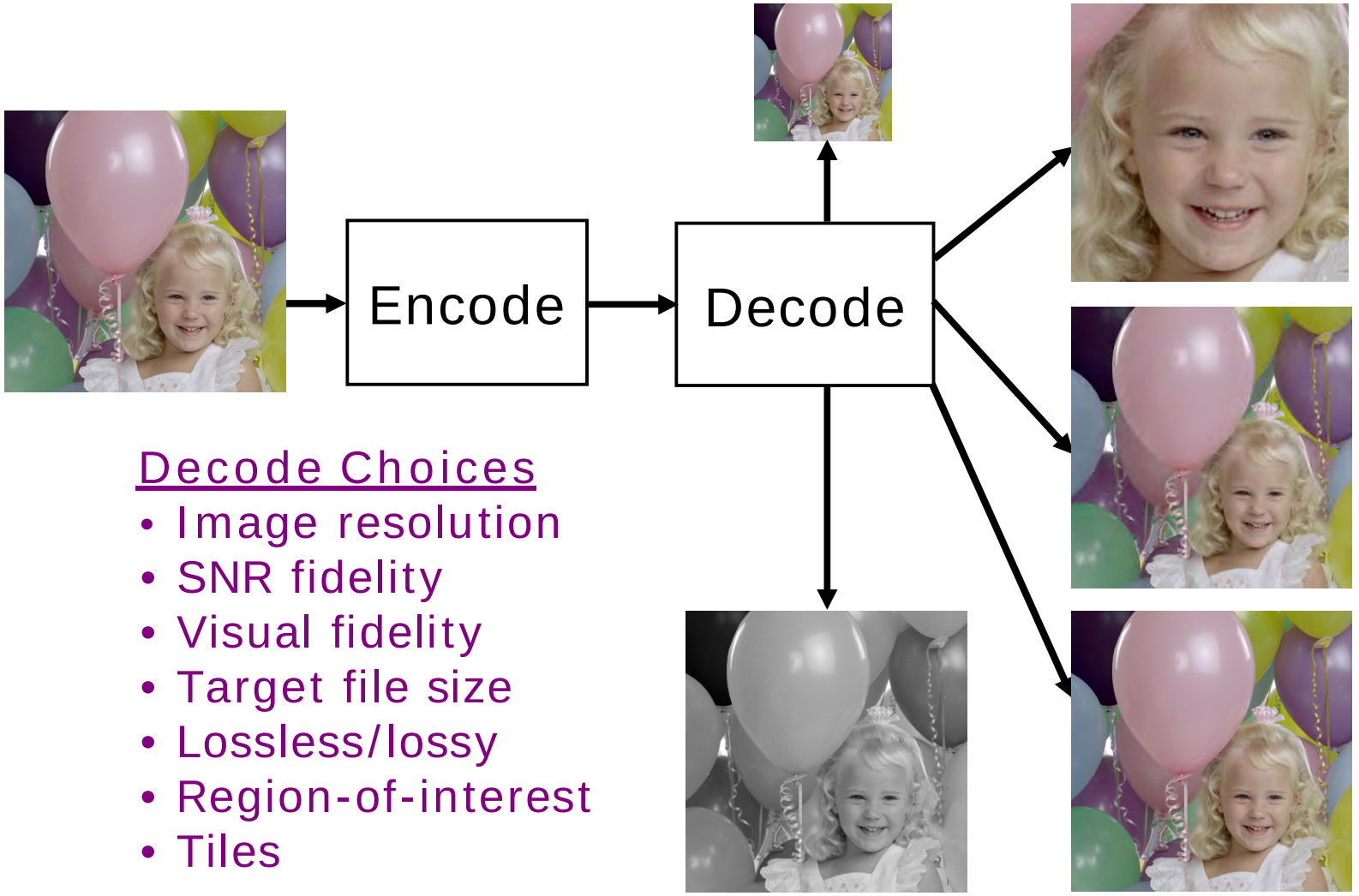
Introduction

- Digital imagery is an important area
- Emerging applications require adding security
  - Commerce of digital imagery
  - Secure web browsing
  - Secure media adaptation for diverse clients & networks
- JPEG 2000 is now creating the JPEG-2000 Security Standard
  - This is JPSEC!

JPEG 2000 family of standards

- Part 1: Core coding system
- Part 2: Extensions (adds more features to the core)
- Part 3: Motion JPEG 2000
- Part 4: Conformance
- Part 5: Reference software
- Part 6: Compound image file format (documents)
- Part 8: JPSEC on security
- Part 9: JPIP on interactive protocols and API
- Part 10: JP3D on volumetric imaging
- Part 11: JPWL on wireless applications
- Part 12: ISO Base Media File Format (=MPEG-4)

JPEG 2000 Application Paradigm



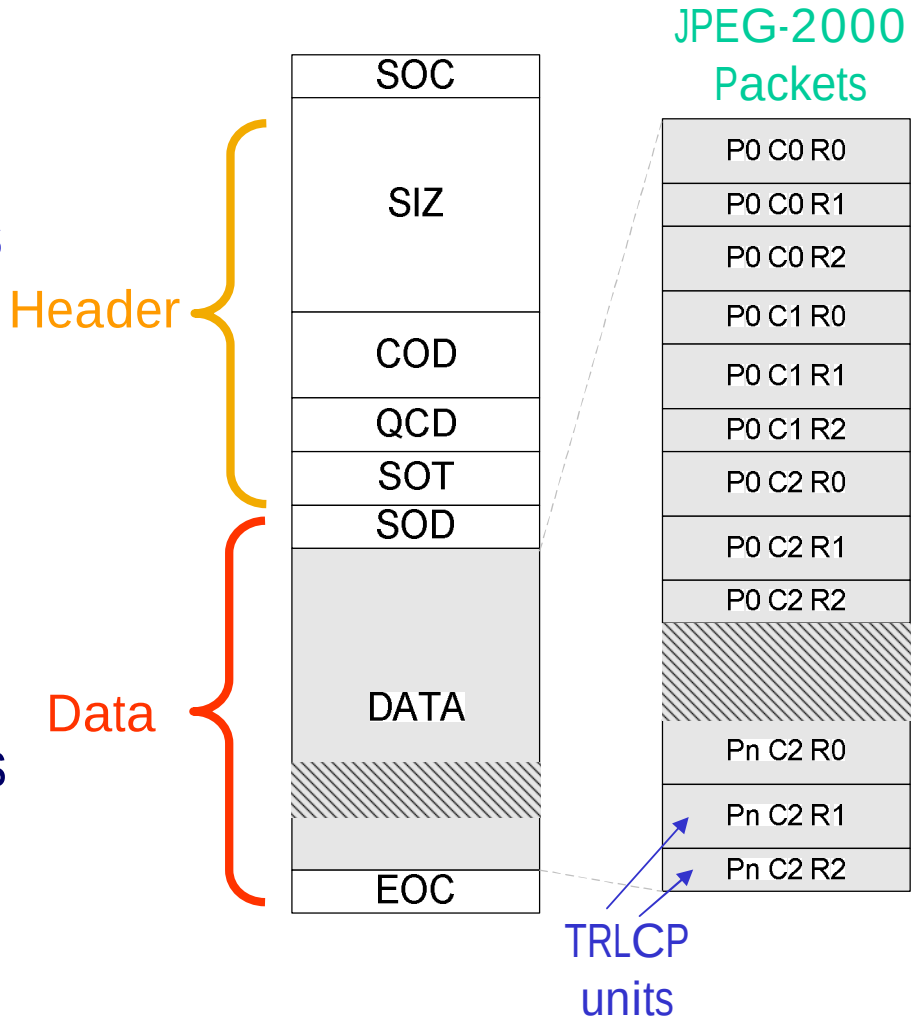
Decode Choices

- Image resolution
- SNR fidelity
- Visual fidelity
- Target file size
- Lossless/lossy
- Region-of-interest
- Tiles

JPEG-2000 image coding

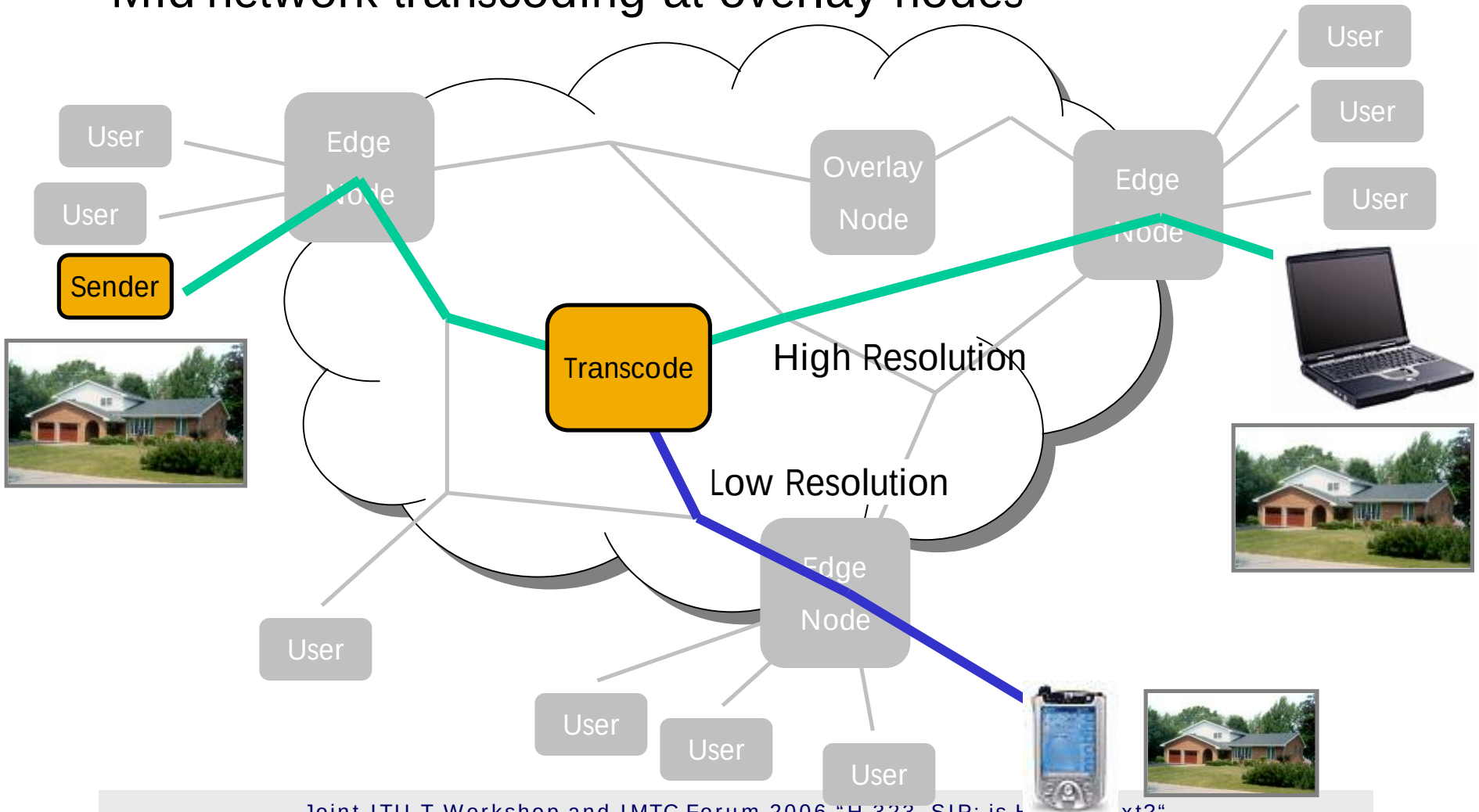
ITU-T

- Image structures
  - Tiles, Resolutions, Layers, Color components, Precincts
- Codestream structures
  - Header
    - SIZ, COD, QCD, etc.
  - Data
    - JPEG-2000 Packets: contain TRLCP units
      - Packet headers
      - Packet bodies



Media delivery to diverse clients over diverse networks

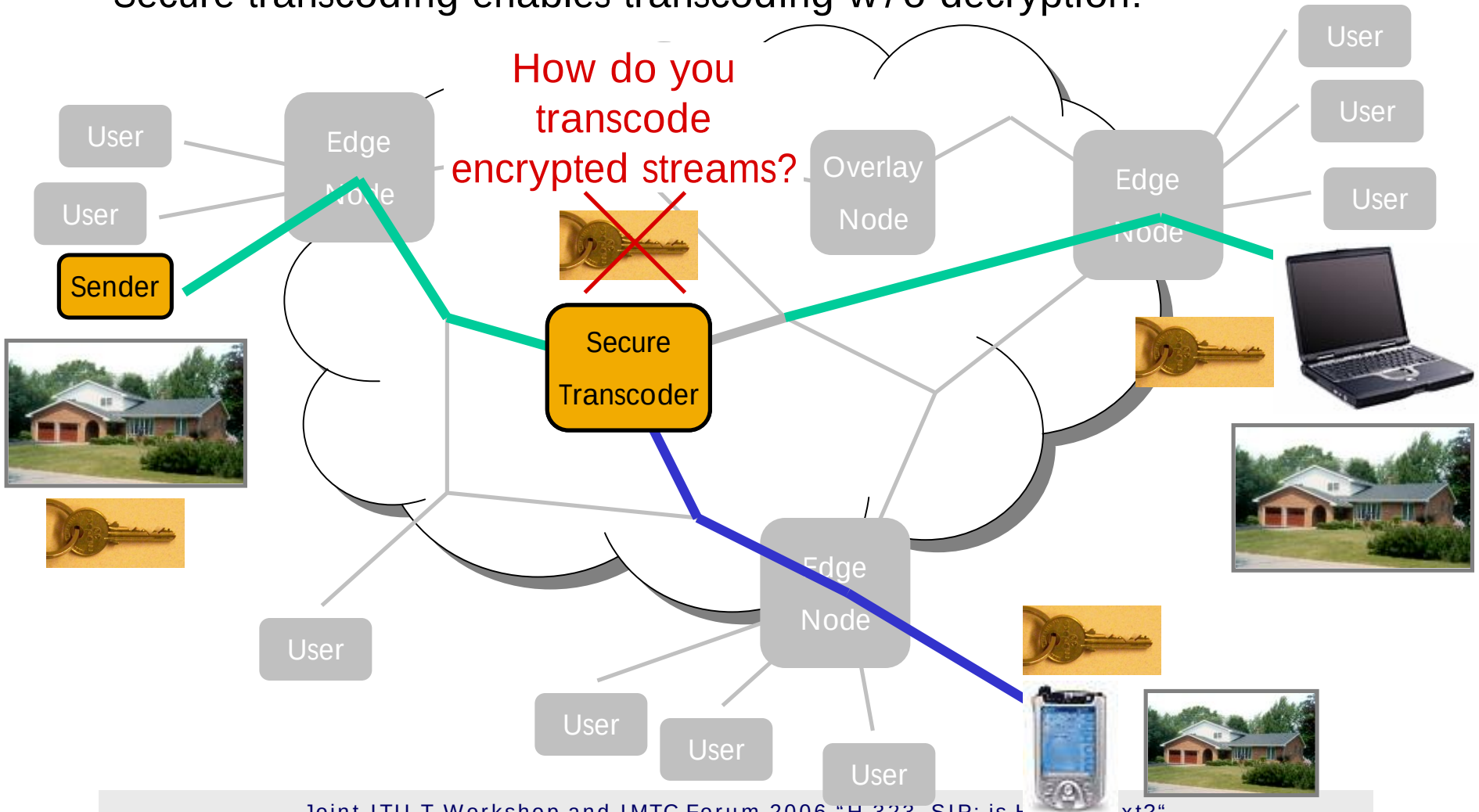
Mid-network transcoding at overlay nodes



Mid-Network Transcoding with End-to-End Security

[ICASSP, ICIP 2001]

Secure transcoding enables transcoding w/o decryption!



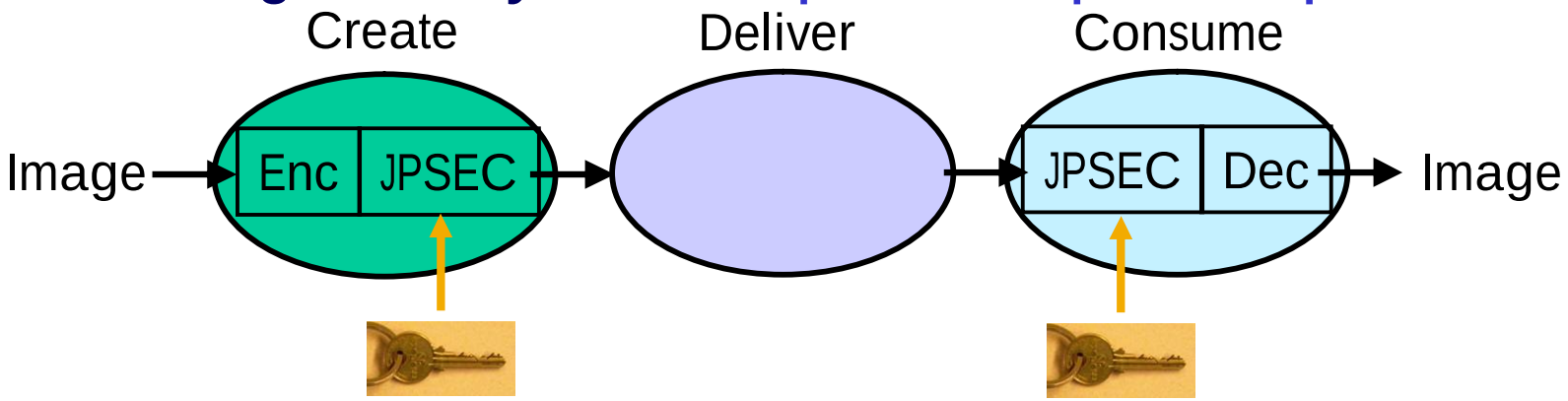
ITU-T

Data vs. Media Security

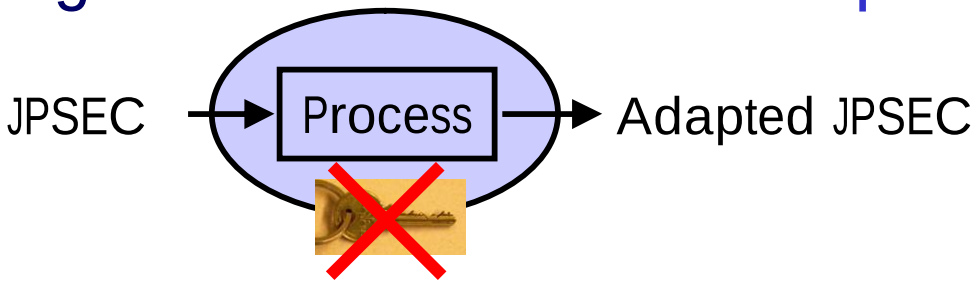
- Question: How do we secure digital images?
- Conventional approach: Apply traditional data security to media
  - Problem: Lose all media attributes, e.g., the ability to access a portion of the media
- Our solution: Jointly design security, compression, & delivery to preserve media features

JPSEC Basic Design Principle

- JPSEC goes beyond simple end-point operations

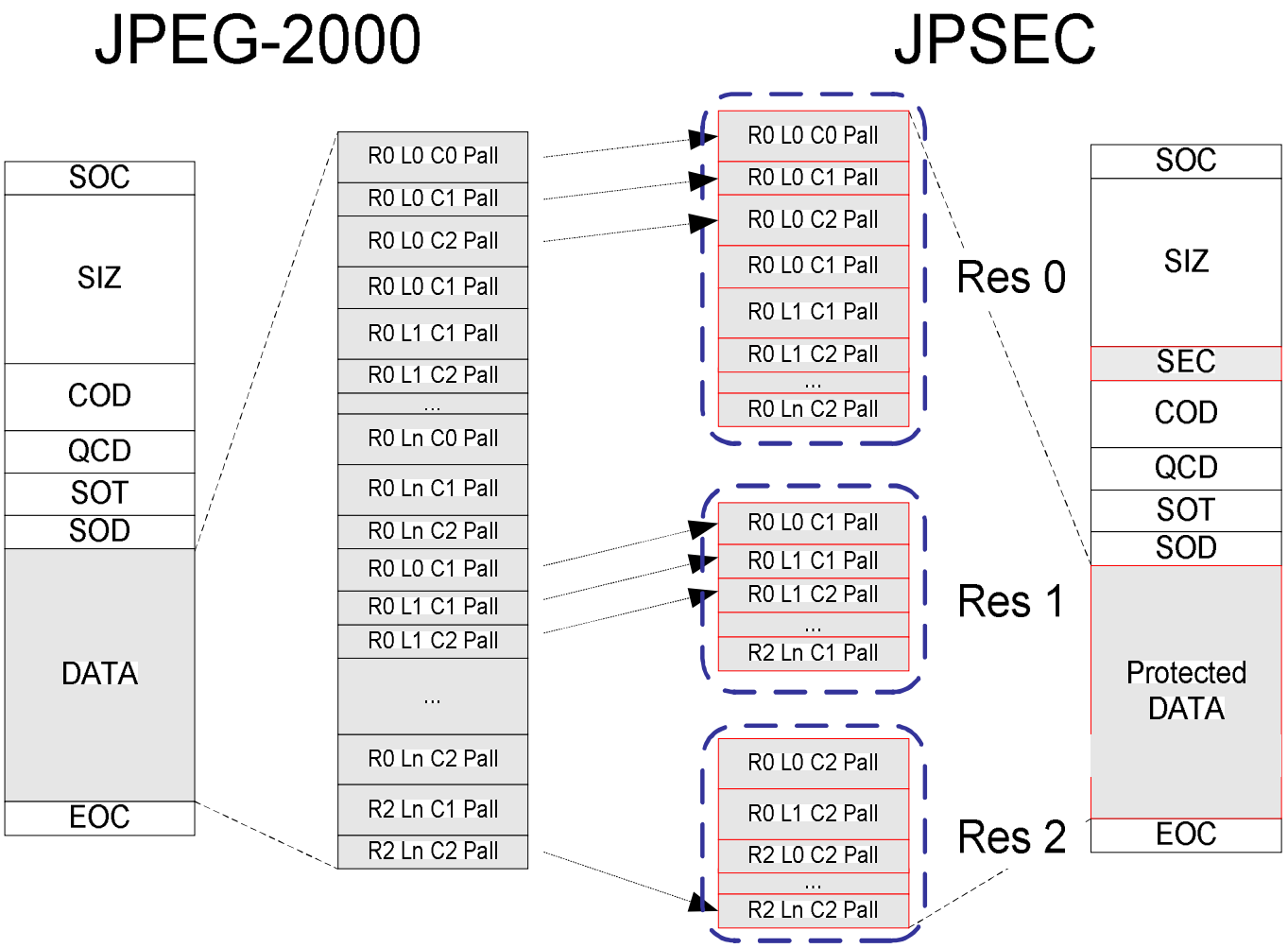


- JPSEC is designed for intermediate operations



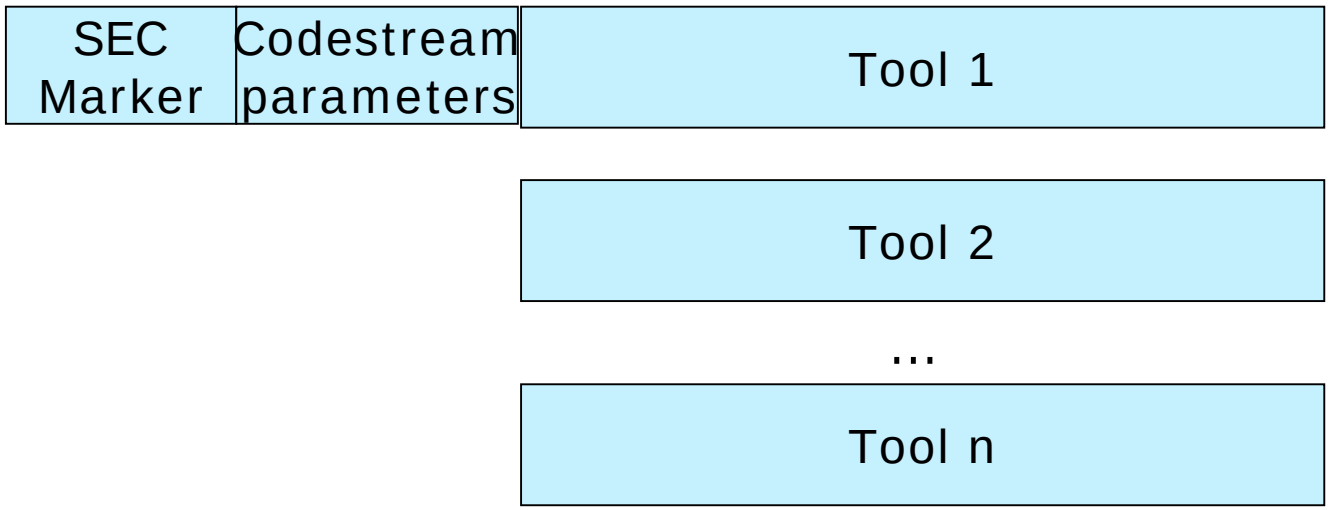
- Leads to deeper & richer design goals
- Impacts all security services & overall design

JPEG-2000 to JPSEC



JPSEC creation & consumption
SEC Marker Segment

Security is achieved with
JPSEC Protection Tools signaled in the codestream.



JPSEC tool types

- JPSEC Template Tool
  - Syntax defined by JPSEC standard (normative)
  - Protection method templates specify parameter syntax
- JPSEC Registration Authority Tool
  - Syntax defined by registration authority (non-normative)
- JPSEC Private Tool
  - Syntax defined by private application (non-normative)

JPSEC Architecture & Syntax

- What security service is applied?
  - Protection tool type
- Where is the security service applied?
  - Zone of influence (ZOI)
- How is the security tool applied?
  - Tool parameters

- Designed to be simple, efficient, highly flexible & extensible to support rich sets of capabilities & applications

What?
JPSEC Template Tools

- Protection method templates
  - Decryption template
    - Block cipher
    - Stream cipher
    - Asymmetric cipher
  - Authentication template
    - Hash-based authentication
    - Cipher-based authentication
    - Digital signature
  - Integrity template

Where?
Zone of Influence (ZOI)

- ZOI specifies tool's area of influence
- Image-Related Descriptions
  - Region, tile, resolution, component, quality level, etc.
- Bitstream-Related Descriptions
  - Byte range, packet, Distortion, TRLCP tag
- Used together to describe correspondence

ZOI is a powerful tool that enables low-complexity & highly flexible media security by providing metadata for the protected data

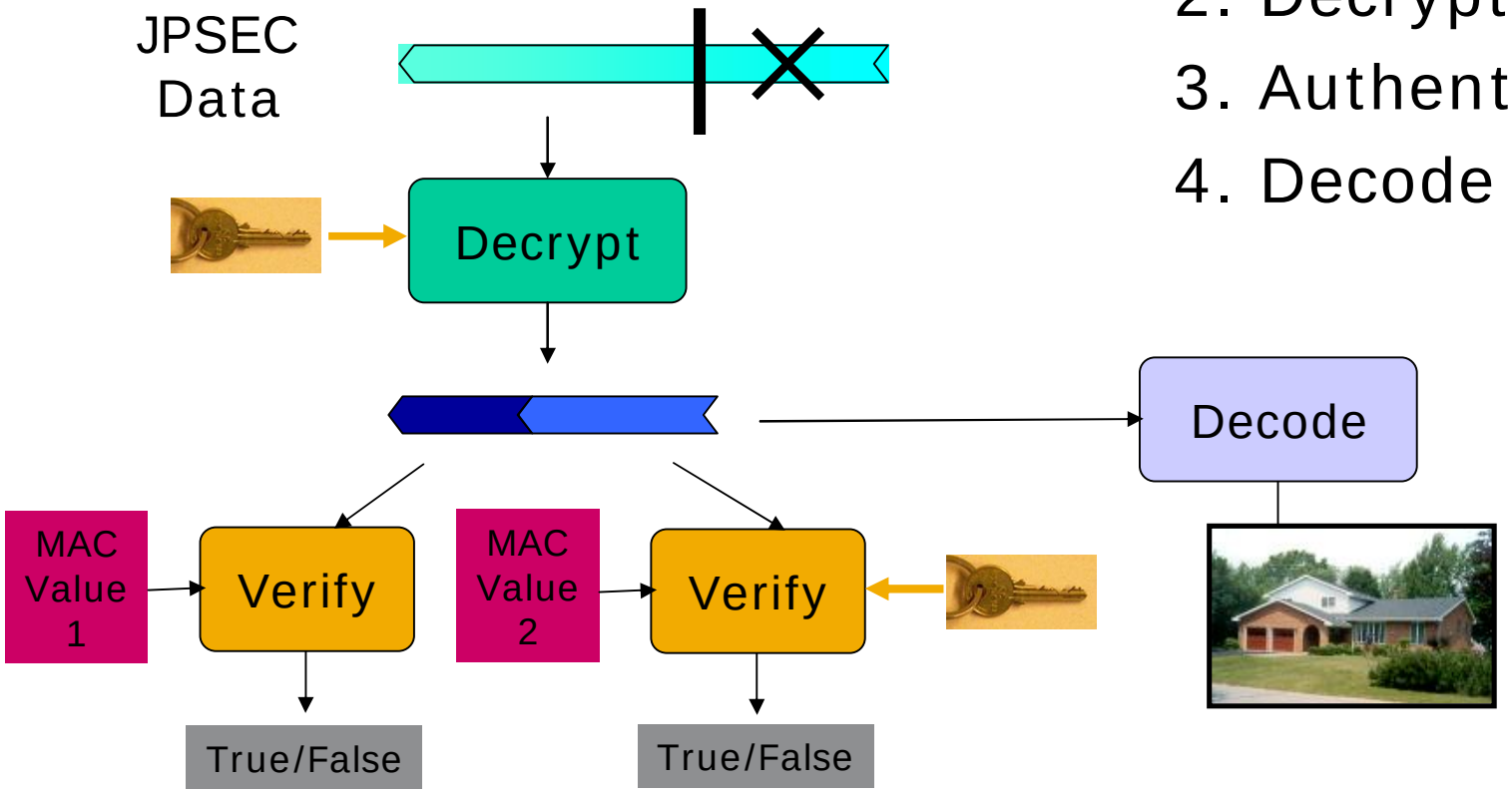
How?
Protection Template Options

Decryption Template	
Block cipher	
Cipher	DES, 3DES, AES
Block cipher mode	ECB, CBC, CFB, OFB, CTR
Padding mode	Ciphertext stealing, PKCS#7
Block size	Cipher dependent
Key template	Application dependent
Initialization vector	Variable
Stream Cipher	
Cipher	RC4
Key template	Application dependent
Initialization vector	Variable
Asymmetric Cipher	
Cipher	RSA
Key template	Application dependent

Authentication Template	
Hash-based authentication	
Method	HMAC
Hash function	SHA-1,RIPEMD 160,SHA256
Key template	Application dependent
Size of MAC	Variable
MAC value	Signal dependent
Cipher-based Authentication	
Method	CBC-MAC
Block cipher	Cipher ID
Key template	Application dependent
Size of MAC	Variable
MAC value	Signal dependent
Digital Signature	
Method	RSA, Rabin, DSA, ECDSA
Hash function	Hash ID
Key template	Application dependent
Digital signature	Signal dependent

Example: Transcode, Decrypt & Authenticate

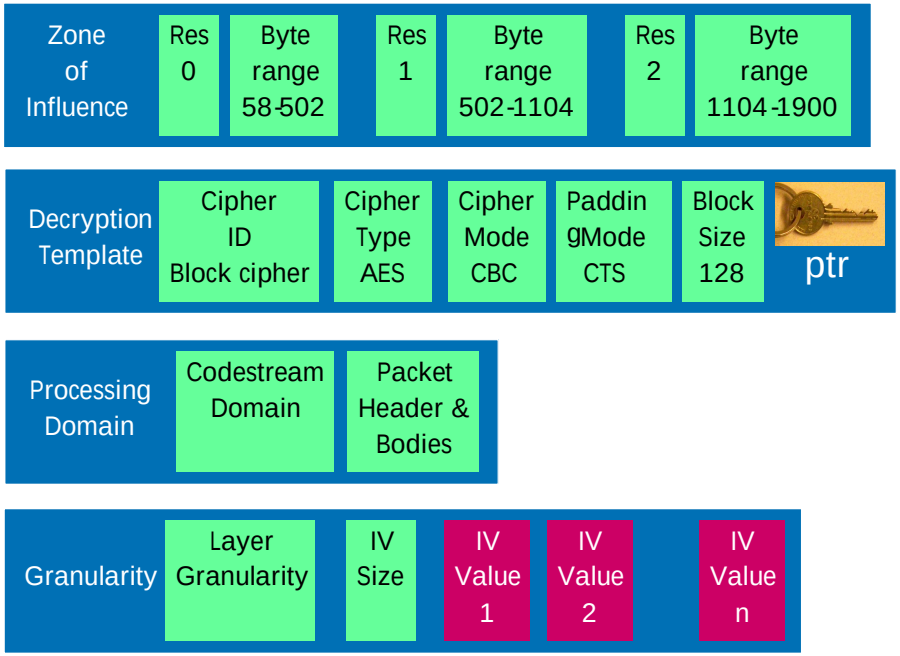
1. Transcode
2. Decrypt
3. Authenticate
4. Decode



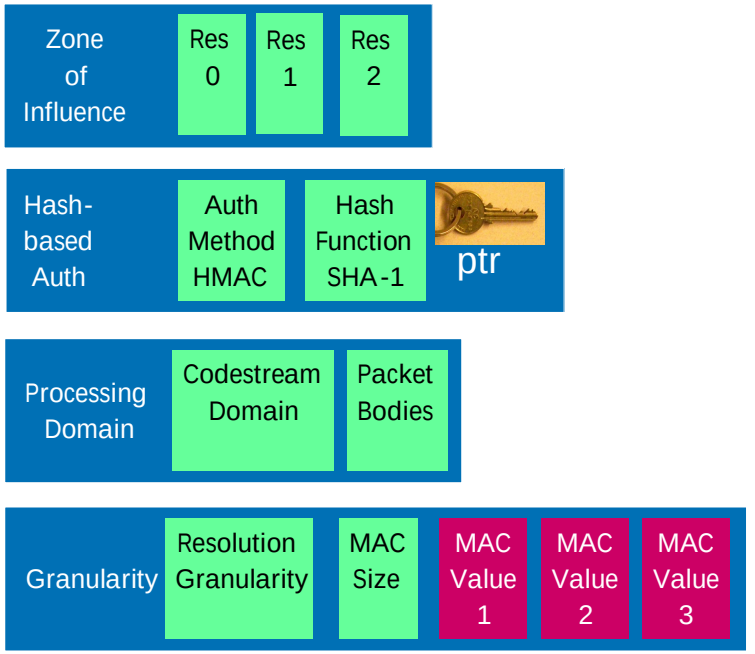
What, Where, How: JPSEC Protection Templates

- Example: Securely access & authenticate 3 resolution layers

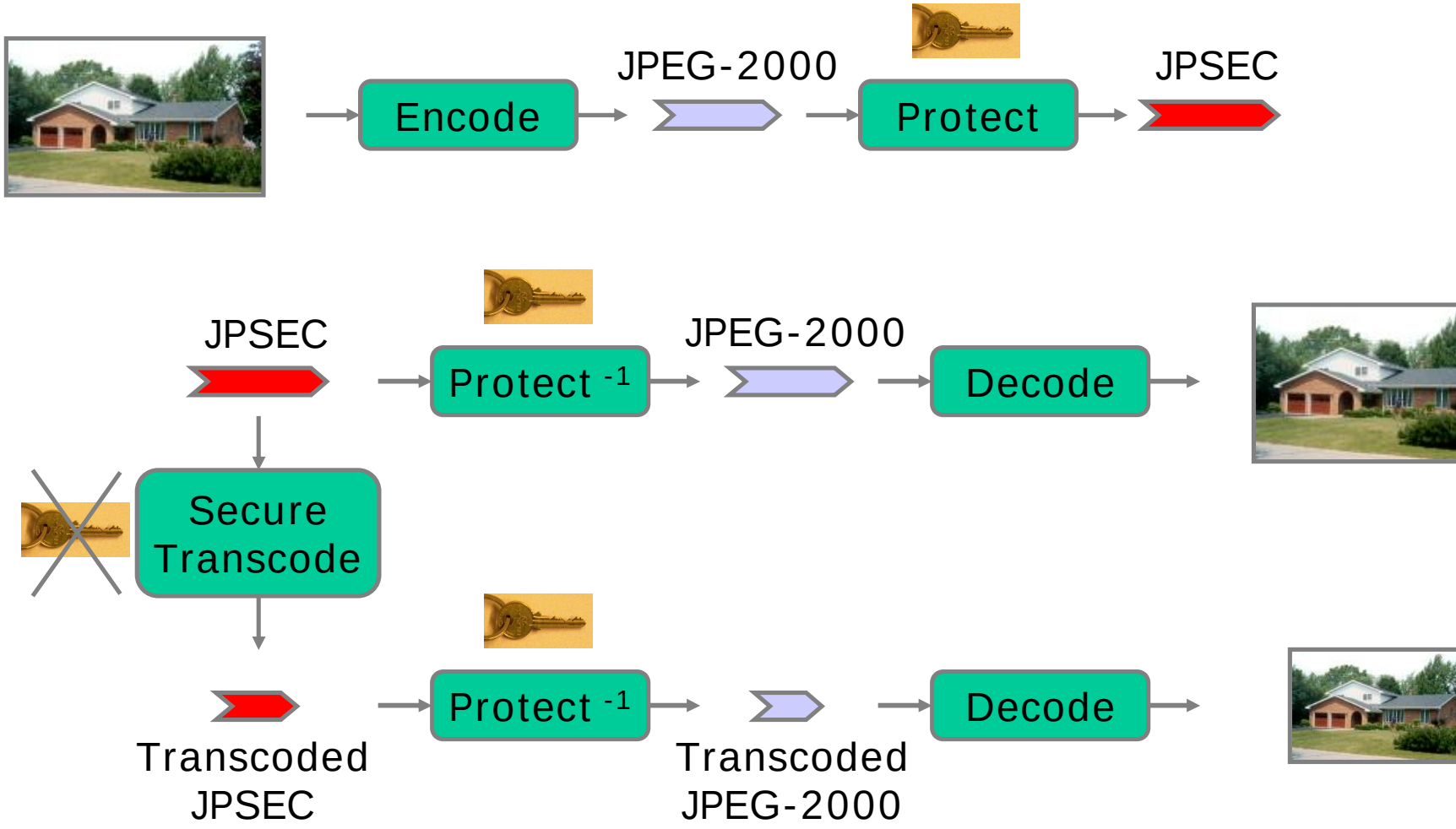
Decryption Template



Authentication Template



JPSEC with Secure Transcoding



Results: JPSEC transcoded images

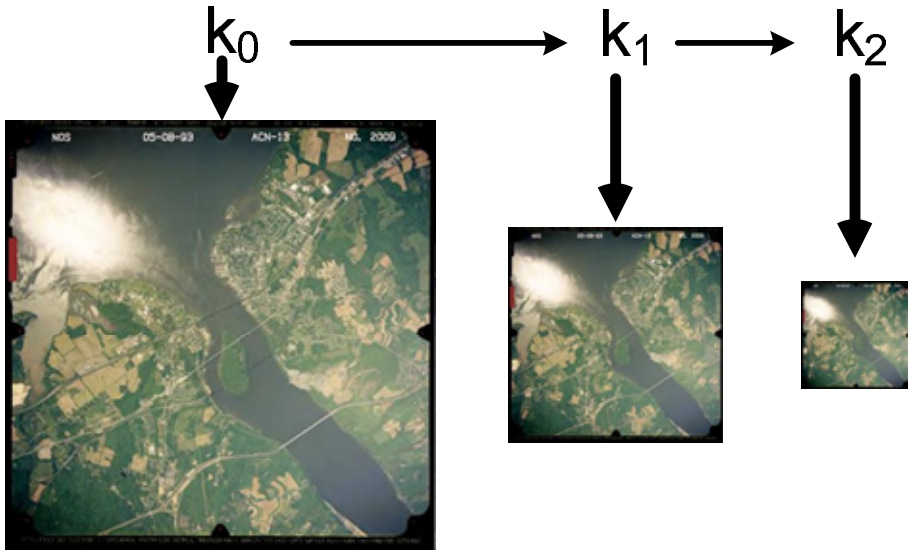
JPSEC Security Service Requirements

1. Confidentiality ← Media aware
2. Integrity verification ← Media aware
3. Authentication ← Media aware
4. Access control ← Media aware
5. Registered content identification
6. Secure scalable streaming & secure transcoding

New (non-conventional) security service

ITU-T

Use Case 1:
Multi-level Access Control



- Access resolution, quality, spatial region
- Multiple independent or structured keys
- One copy of encrypted media provides multiple levels of access control --- access depends on user's key

Use Case 2:
Selective & Partial Encryption

Marked Image

Spatial Pattern of Marking

Decoding without key

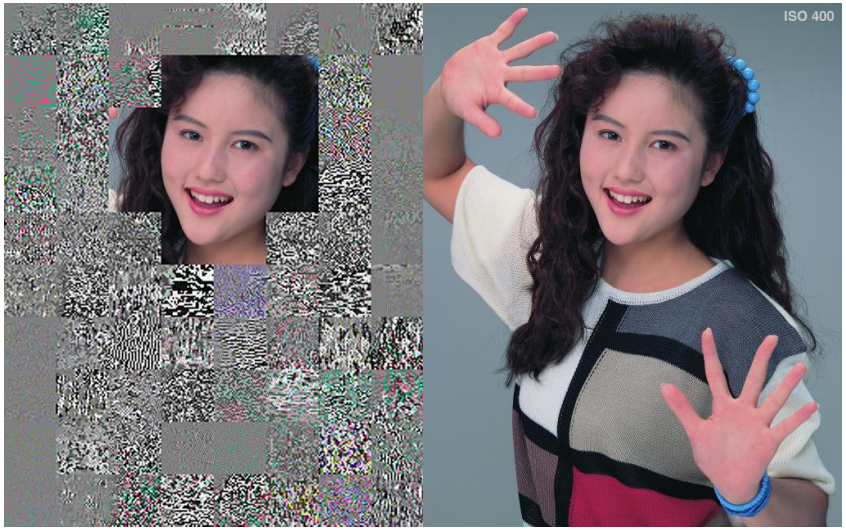
- Marked image sufficient for understanding image content & deciding whether to purchase key to unmark the image

ITU-T

Use Case 3:
Selective Encryption

IMTC

Selectively encrypted JPEG-2000 Image (decoding w/o key)

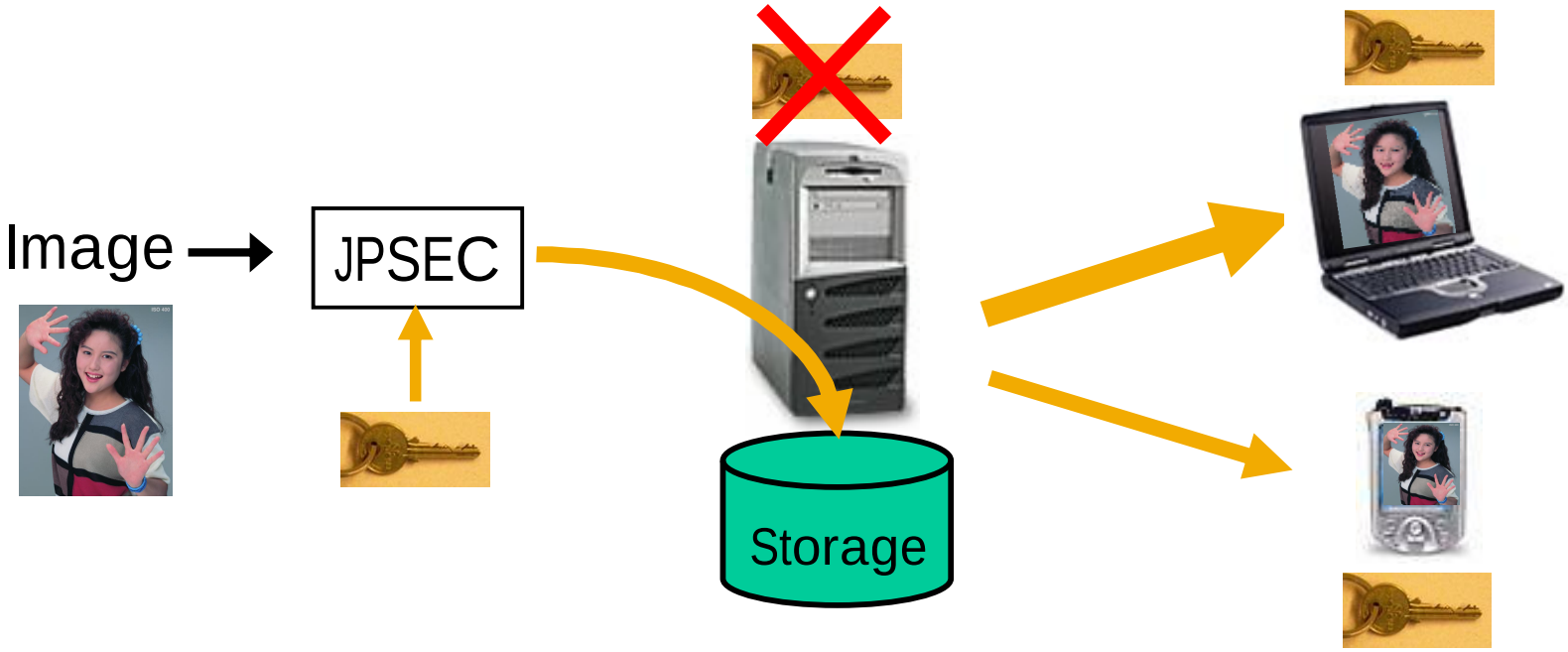


Decrypted Image (with key)

- Selected portions hidden with encryption
- End-user w/o key can still see image contents and decide whether to purchase
- Encrypted JPEG-2000 bitstreams decoded by JPEG-2000 decoder without key

ITU-T

Use Case 4:
Secure Storage & Transcoding



- Encrypt, store, securely adapt for different devices
  - Server stores encrypted content
  - Server adapts/transcodes without decryption
- Secure Scalable Streaming technology

JPSEC Status

- JPEG-2000 security standard (JPSEC)
- New requirement: Secure scalable streaming and secure transcoding
- Status: Final Draft International Standard
- Likely to reach International Standard in Summer 2006

ITU-T

Acknowledgements

- The authors would like to thank the members of the JPSEC Ad-Hoc Group and the JPEG working group for their continual support.