The Emerging JPEG-2000 Security (JPSEC) Standard

John Apostolopoulos[1], Susie Wee[1], Frederic Dufaux[2], Touradj Ebrahimi[2], Qibin Sun[3], Zhishou Zhang[3]
[1] HP Labs, Palo Alto, CA, USA
[2] Ecole Polytechnique Federale de Lausanne (EPFL), Lausanne, Switzerland
[3] Institute for Infocomm Research, Singapore

***Abstract*— The emergence of digital imaging applications are accelerating the need for security of digital imagery. The emerging international standard ISO/IEC JPEG-2000 Security (JPSEC) is designed to provide security for digital imagery, and in particular digital imagery coded with the JPEG-2000 image coding standard. This paper provides an overview of the JPSEC standard, including a description of its basic architecture and examples of its use.**

I. Introduction

Digital imagery is important in many applications today and one of the reasons for its success is the standardized compression formats provided by the JPEG and JPEG-2000 image coding standards. Security of digital imagery is gaining in importance and is necessary to enable the e-commerce of digital imagery. The emerging international standard ISO/IEC JPEG-2000 Security (JPSEC) [1] is designed to provide security for digital imagery, and in particular digital imagery coded with the JPEG-2000 image coding standard [2,3]. JPSEC is currently at Final Draft International Standard (FDIS) status, and is expected to become an international standard in early 2006.

This paper provides an overview of the JPSEC standard, including describing the security services provided, the JPSEC architecture, and a few examples of its use.

II. Overview of JPSEC

The JPSEC standard is designed to provide security for digital imagery. JPSEC is an open framework, and it can be extended in the future to support additional security services and security tools. Currently it focuses on the following media security services:

- Confidentiality via encryption and selective encryption: A JPSEC file can support a transformation of the (image and/or metadata) data (plaintext) into a form (cipher text) that conceals the data's original meaning. In selective encryption we mean that only parts of the image and/or metadata are encrypted, as opposed to the entire image and/or metadata.
- Integrity verification: A JPSEC file can support means of detecting manipulations to the image and/or metadata and thereby verify their integrity. This may be achieved by (1) cryptographic methods such as Message Authentication Codes (MAC), digital signatures, cryptographic checksums or keyed hashes, (2) watermarking-based methods (the standard does not define normative template for watermarking technology, although it supports non-normative tools using watermarking technology), or (3) a combination of the above.
- Source authentication: A JPSEC file can support verification of the identity of a user/party which generated the JPSEC file. This can be achieved through the use of digital signatures or message authentication codes (MACs).
- Conditional access: A JPSEC file can support a mechanism and policy to grant or restrict access to image data or portions of those. This could for instance allow one to view a low resolution (preview) of an image without being able to visualize or access a higher resolution version of the same image.
- Registered Content identification: A JPSEC file can be registered at a Content Registration Authority. It can support a method of matching the (claimed) image data/image content to the registered image data/image content, including information about where the file was registered as well as how to verify that the file corresponds to the identifier.
- Secure Scalable Streaming and Secure Transcoding: A JPSEC file or sequence of packets can support methods such that the same or different node can perform streaming and transcoding without requiring decryption or unprotecting the content [4,5]. For example, protected JPEG-2000 content is streamed to a mid-network node or proxy that in turn transcodes the protected JPEG-2000 content while preserving end-to-end security.

The JPSEC creator produces a JPSEC codestream with the desired security service, which can then be consumed by a JPSEC consumer. As discussed before, the JPSEC standard only specifies the codestream syntax and semantics, and not the creator or consumer. The next section provides a walk-through of one example JPSEC consumption process.

III. JPSEC ARCHITECTURE

The JPSEC standard has been designed to allow significant flexiblity and a high level of security through the use of protection tools and associated signalling that are applied to JPEG-2000 coded images. These protection tools include templates for decryption and authentication. We designed the JPSEC architecture for interlayer interaction between compression, security, file format, and packetization to provide the above desired attributes. Note that the incorporation of secure transcoding into the JPSEC standard led to significant changes to all of the above because of the required interlayer awareness.

JPSEC provides security services for JPEG-2000 by defining a number of protection tools that can be applied to JPEG-2000 bitstreams. A JPSEC system consists of a JPSEC creator, JPSEC bitstream, and JPSEC consumer. The JPSEC creator can apply one or more protection tools to an image. The resulting JPSEC bitstream contains signaling information for the protection tools and the modified data that may have resulted from their application. The signaling information is placed in a SEC (security) marker segment that is added to the JPEG-2000 header, and it includes the parameters that a JPSEC consumer needs to interpret and process the protected stream. The JPSEC bitstream contains three general types of information to describe to the JPSEC consumer the *what*, *where*, and *how* of the applied security services.

A. What security service is provided?

The JPSEC syntax has three types of security tools: template tools, registration authority tools, and user-defined tools. The *template tools* are defined by the normative part of the JPSEC standard. They have an identifier that specifies which protection method template is used. JPSEC provides templates for decryption, authentication, and hashing. The *registration authority* tools are registered with and defined by a JPSEC registration authority and have a registration authority ID number that is specified in the syntax. The *user-defined tools* are defined by a user or application. JPSEC reserves a set of ID numbers that can be used by private applications. However, ID collisions may occur if the same ID number is used by different JPSEC applications, so the user must be careful in defining the use and scope of these streams. Both the registration authority and user-defined tools enable the application of proprietary protection methods, for example, new techniques or classified government security techniques can be applied in this fashion. The remainder of this discussion focuses on JPSEC template tools as defined by the normative part of the standard.

B. Where is the security tool applied?

JPSEC uses a Zone of Influence (ZOI) to describe where the security tool is applied. The ZOI functionally describes how to apply tools to the stream, and it can also include valuable metadata about the coded and protected image. The Zone of Influence (ZOI) describes the coverage area of each JPSEC tool. This coverage area can be described by image-related or non-image-related parameters. Image-related parameters can specify parameters such as resolution, image area, tile index, quality layer, or color

Decryption Template	
Block cipher	
Cipher	AES, 3DES
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

Table 1: Decryption and authentication templates.

component. For example, the ZOI can specify that the lowest resolution component of the image is encrypted. Non-image-related parameters can specify areas such as byte ranges or packet indices. For example, the ZOI can specify that the JPSEC stream is encrypted from bytes 198 through 1368. In cases where image related parameters and non-image related are used together, the ZOI describes the correspondence between these areas. For example, the ZOI can be used to indicate that the resolutions and image area specified by the image related parameters correspond to the byte ranges specified by the non-image related parameters. This feature allows the ZOI to be used as metadata that signals where certain parts of the image are located in the JPSEC bitstream. This is especially useful when encryption is used because the image data is no longer accessible in the protected JPSEC stream, thus, it may be impossible to determine where the various image data boundaries lie in the encrypted JPSEC stream.

C. *How is the security tool applied?*

While the identifier describes what security services are used, and the zone of influence describes where the security tool is applied, further details are needed to instruct a JPSEC consumer how to consume the protected stream. JPSEC uses template and processing parameters for this task. The template parameters describe the detailed parameters of the template tool. For example, while the IDs indicate that decryption and authentication are to be applied, the template parameters would indicate that the JPSEC consumer should use AES decryption in counter mode for decryption and HMAC with SHA-1 for authentication. Example template parameters are shown in Table **1**, along with additional information expressed by the templates.

In addition to specifying the template parameters, JPSEC also specifies the processing parameters, including the processing domain and granularity, that describe how the tools are applied. For example, the processing parameters can instruct a JPSEC consumer to apply the specified decryption method with a granularity of a resolution layer and to the domain of packet bodies only. With this information and the access keys, a JPSEC consumer can correctly decrypt and decode the portions of the data that it is allowed to access.

IV. Example JPSEC Use Cases

A. *Multi-level Access Control*

Security protection tools may be applied to an image using one key or multiple keys. The advantage of using multiple keys is that they can provide multiple levels of access control. For example, different access rights may be provided to different individuals by providing each individual with an appropriate key. These access rights may correspond to different qualities of the image, e.g. given JPEG-2000's various forms of scalability, one can provide access to different resolutions, quality levels (pixel fidelity), spatial regions or regions of interest [6].

The multiple keys may be independent of each other, but this can lead to the requirement for a large number of keys complicating tasks such as key distribution. Another common approach is for the keys to be related in a structured manner, e.g. they may be recursively computed from a master key using a hash tree: Given a master key k, a sequence of keys may be computed by applying a one-way hash function H(), where $k_{i+1} = H(k_i)$. For example, with a 2-level wavelet decomposition 3 resolution levels are available {Low, Med, High}. By encrypting these three levels with the three keys $\{k_2, k_1, k_0\}$ where $k_1 = H(k_0)$ and $k_2 = H(k_1) = H(H(k_0))$, a user with k_0 can generate k_1 and k_2 and thereby decrypt all three resolution layers to get the High resolution image, a user with k_1 can generate k_2 and thereby decrypt two resolution layers to get the Med resolution, and a user with k_2 can only decrypt one resolution layer to get the Low resolution version of the image, as illustrated in Figure 1. Note that while this brief discussion for simplicity focused on a 1-D hash chain for key generation, general tree structures (including non-binary, unbalanced, and M-D trees) are straightforward extensions and provide very valuable flexibility and richness for access control. In this manner, *one copy of encrypted media content provides multiple levels of access control where the access depends on the key of the accessor.*

B. *Selective or Partial Encryption of Image Content*

The JPSEC tools may be used to selectively encrypt different semantically meaningful portions of an image. For example, in Figure 2 a portion of JPEG-2000 coded image is selectively left unencrypted, while the remaining portions are encrypted. An end-user without the key can still see part of the image content and therefore decide whether to purchase it or not. If the end-user purchases the content he/she receives the key which can then be used to decrypt and decode the entire image.

An important note here is that this encrypted JPEG-2000 bitstream was decoded using a JPEG-2000 decoder, and not a JPSEC decoder, i.e. the encrypted bitstream in this example was designed to be usefully decoded by a JPEG-2000 decoder which does not have the key or have knowledge about what was encrypted. This functionality is quite useful as it enables conventional JPEG-2000 decoders to make use of JPSEC protected content.

V. Summary

JPSEC is an emerging standard for the security of digital imagery, which is currently at Final Draft International Standard (FDIS) status and is expected to progress to International Standard (IS) status in early 2006. JPSEC provides a significant amount of flexibility which can be used to create a rich and diverse range of secure digital image (and video) applications. This paper provided an overview of the JPSEC standard as well as a number of illustrative examples of its use.

Acknowledgement: The authors would like to thank all the individuals who participated in the development of JPSEC. EPFL is partially supported by the European Project WCAM http://www.ist-wcam.org (IST Contract 507204) funded under the European Commission IST 6th Framework Program.

References

[1] *JPSEC Final Draft International Standard, ISO/IEC JTC1/SC29/WG1/N3820,* T. Ebrahimi, C. Rollin, S. Wee, eds., Nov. 2005.

[2] D. Taubman, M. Marcellin, *JPEG2000: Image Compression Fundamentals, Standards, and Practice,* Kluwer Academic Publishers, Boston, MA, 2002.

[3] A. Skodras, C. Christopoulos, T. Ebrahimi, The JPEG 2000 Still Image Compression Standard, IEEE Signal Processing Magazine, September 2001.

[4] S. Wee, J.Apostolopoulos, “Secure scalable streaming enabling transcoding without decryption”, *IEEE ICIP*, Oct. 2001.

[5] S. Wee, J. Apostolopoulos, “Secure Transcoding with JPSEC Confidentiality and Authentication”, *IEEE ICIP*, Oct 2004.

[6] Y. Wu, D. Ma, R. Deng, “Progressive Protection of JPEG2000 Codestreams”, *IEEE ICIP*, Oct 2004.

[7] Z. Zhang, Q. Sun, G. Qiu, Y.Q. Shi, and Z. Ni, “A unified authentication framework for JPEG2000,” *IEEE ICME*, 2004.

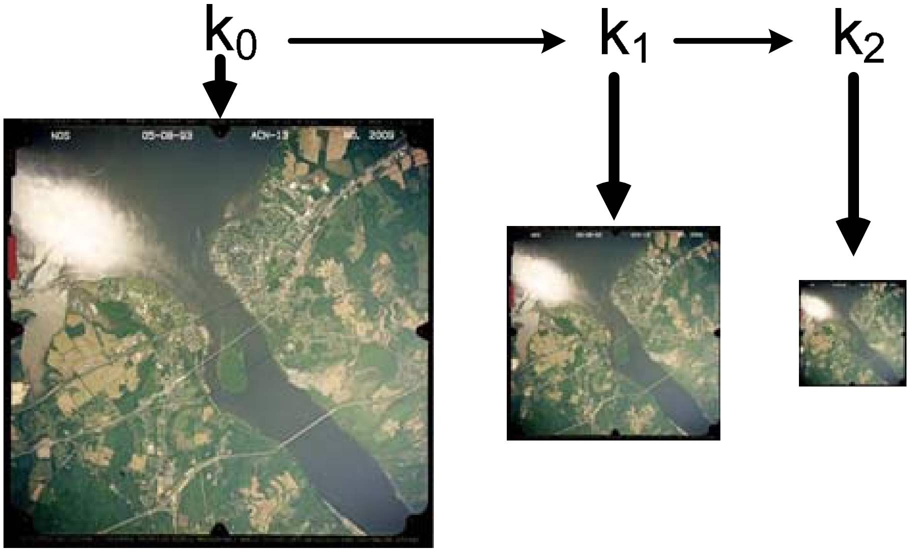

Figure 1 Multi-level access control: Given one encrypted image, the user with key k_0 can access the high, medium, or low resolution images; user with key k_1 can access medium or low; while user with key k_2 can only access lowest resolution.

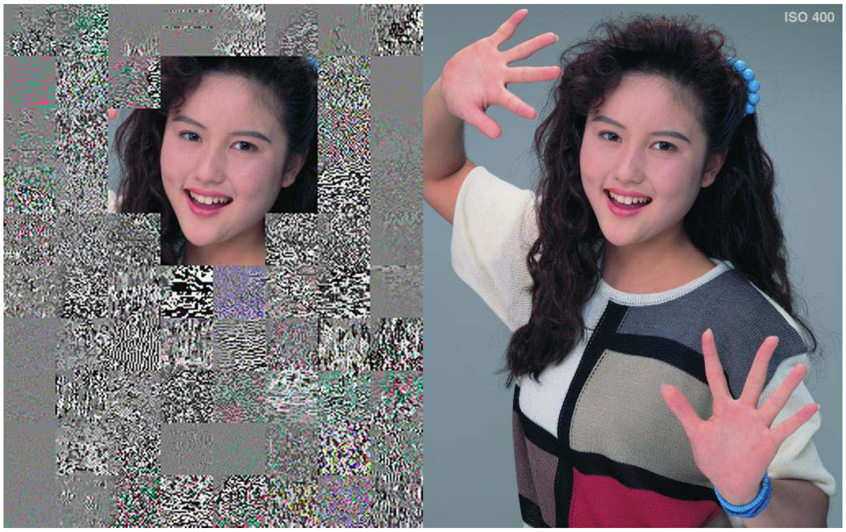

Figure 2 Selected spatial regions are left unencrypted while the remaining regions are encrypted. A JPEG decoder (w/o the key) decodes the left image while a JPSEC decoder with the key recovers the right image.