

2 JPSEC: Security Part of JPEG2000 Standard



This paper gives an overview of JPSEC, the Security Part of JPEG2000 standard, which defines a framework to provide security services like confidentiality, access control, integrity protection, authentication and ownership protection. The FDIS specifications of JPSEC include 10 examples of informative tools, of which three examples were contributed by the Institute for Infocomm Research. Nevertheless, the framework is always ready to incorporate new tools in the future. In addition, this article also demonstrates how JPSEC could be used in some application scenarios.

Qibin Sun

Institute for Infocomm Research

Member, Multimedia Representation Technical Committee (MRTC)

Zhishou Zhang

Institute for Infocomm Research

1 Introduction

Over the last decade, driven by the advances of computer hardware, software and Internet, digital images have been widely used by individuals, government agencies and enterprises, due to their apparent advantages over traditional paper-based images. JPEG2000 [1] is one of the state-of-the-art coding standards published by the Joint Photographic Experts Group (JPEG) committee, which is under the joint auspices of ISO and ITU-T. It has various advantages over the current widely-used JPEG standard [2] in many aspects like compression efficiency, scalability and compression-domain editing. In particular, JPEG2000 supports lossy-to-lossless compression within the same bitstream. In contrast, JPEG standard uses separate bitstreams for lossy [2] and lossless [3] compression, respectively. Considering the above advantages of JPEG2000 standard, it is reasonable to expect the standard to prevail in the near future. Therefore, there are strong demands for security solutions to protect JPEG2000 images. Under this big picture, JPEG committee decided to create the security part (part-8) of the JPEG2000 standard, which is also known as JPSEC [4].

JPSEC defines a framework that provides security services for JPEG2000 images. Such security services include confidentiality, access control, integrity protection, authentication and ownership protection. This is achieved using various techniques like encryption, key generation and management, signature generation and verification, scrambling, and watermarking. Nevertheless, JPSEC is different from existing cryptography techniques which just treat the whole JPEG2000 bitstream as a message to be protected. The structures of JPEG2000 bitstream will be lost using existing cryptography techniques. One principle of JPSEC is that it must not limit the typical applications targeted by JPEG2000, i.e., a JPSEC bitstream (protected JPEG2000 bitstream) can still be used as normal JPEG2000 bitstream. For instance, the JPSEC bitstream still retains the rich structures like tile, layer, resolution, precinct and component.

Since the initiation of the project at the end of 2001, JPSEC has undergone different stages of the standardisation process, and JPSEC specification has reached the stage of Final Draft International Standard (FDIS) as at March 2006.

This article is organised as follows. Section 2 gives an overview of JPSEC. Section 3 illustrates the normative signalling syntax. Section 4 summarises the 10 JPSEC tools that were included as informative examples in the standard. Out of the 10 tools, three were contributed by the Institute for Infocomm Research. Section 5, demonstrates how JPSEC could be used in some applications. Finally, Section 6 provides the conclusion for this paper.

2 JPSEC Overview

In the framework defined by JPSEC, there are mainly four components at the high level, namely JPSEC bitstream syntax, JPSEC tools, Registration Authority (RA) and JPSEC applications. The bitstream syntax is normatively defined such that it could be interpreted by different JPSEC applications. JPSEC tool is a software or hardware process that implements JPSEC security services such as confidentiality and authentication. Each JPSEC application has a toolbox containing a set of JPSEC tools. Registration Authority is a central entity that maintains descriptions of registered JPSEC tools. Figure 1 depicts the relationships among these components.

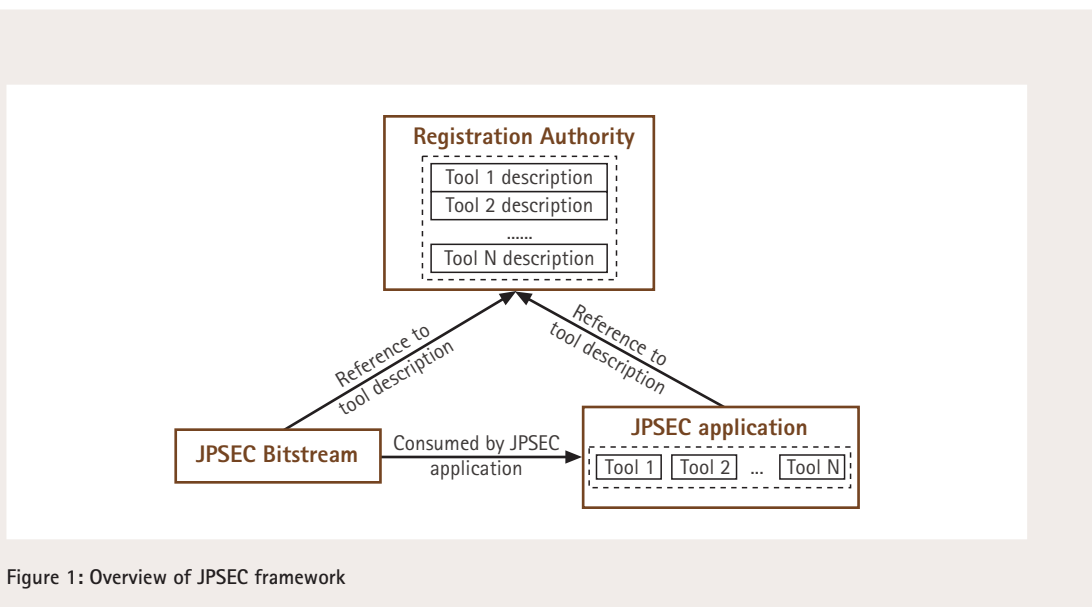


Figure 1: Overview of JPSEC framework

JPSEC bitstream can be created and consumed in a number of ways. A few illustrative examples are shown in Figure 2. JPSEC bitstreams can be created from an original image, from JPEG2000 bitstream, or from another JPSEC bitstream. In the first case, the encoding and protection operations are performed at the same time, so the tool has access to the original image content. This may be important for some JPSEC tools that are based on image content instead of bitstream. In the second case, the JPSEC bitstream is created from JPEG2000 bitstream. This may occur when performing encryption on a database of JPEG2000 images. Finally, the JPSEC bitstream may be created from another JPSEC bitstream. This may arise when multiple JPSEC tools are applied to the same content, but at different times or by different entities. In this case, the ordering in which the tools are applied during the creation must be opposite to that during the consumption.

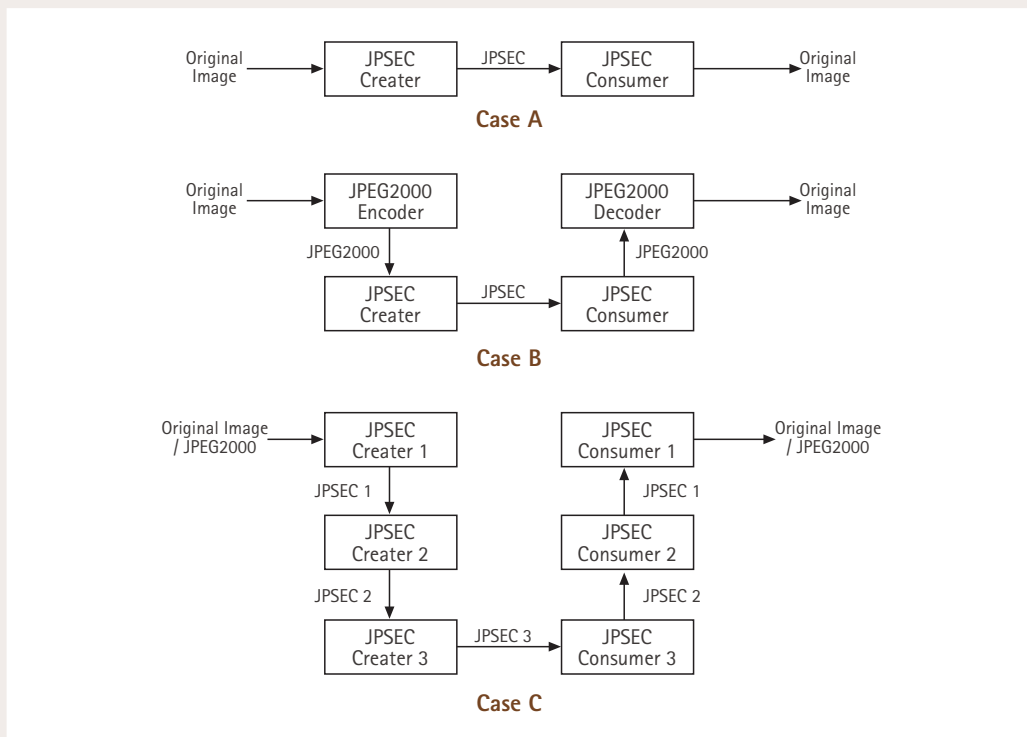


Figure 2: Creating and consuming JPSEC bitstream

JPSEC tools can be classified into two categories: template protection tool and RA protection tool. The template protection tools use the syntaxes that are well defined in protection templates in the JPSEC standard, no proprietary parameter is allowed. Their behaviours are uniquely specified by those security parameters. For example, given two template protection tools A and B, a JPSEC bitstream can be processed by either tool A or tool B with the same outputs, provided that both tools support the signalled security parameters. However, the RA protection tools use proprietary syntax for their security parameters, and each RA protection tool has a unique behaviour specified by a unique identifier assigned by the RA. Each RA protection tool has to be registered with the RA, which maintains all tool descriptions including information like ownership of the tool, parameter format and semantics, usage guideline, URL, and so on.

JPSEC is an open framework that is always ready to incorporate new tools in the future. This is achieved by normatively defining the registration process for a new JPSEC tool. The registration consists of three steps: submission of the registration documents, review by JPSEC authorities and notification. In cases where the final decision is negative, the registrant still has a chance by making an appeal in the JPEG committee meeting. In July of 2004, JPEG committee issued a 'Call for Expression of Interest in JPEG2000 Registration Authority' [5] to invite organisations or companies to implement functionalities of RA.

Each JPSEC application has a toolbox containing a set of JPSEC tools. Upon receiving a JPSEC bitstream, a JPSEC application has to read into the stream syntax and identify the JPSEC tools required to process the received bitstream. If the identified tool is not in its toolbox, it has to contact the RA to download detailed information and add this tool into its toolbox. After that, the JPSEC application just invokes the identified tool to process the received JPSEC bitstream.

3 JPSEC Syntax

JPSEC bitstream is nothing more than a JPEG2000 bitstream, which might have been partially encrypted, scrambled or watermarked in order to provide security services such as authentication or confidentiality. In addition to that, JPSEC bitstream also contains two additional marker segments: Security Marker (SEC) segment and In-Codestream Security Marker (INSEC) segment. These two segments complement each other in signalling sufficient security parameters of the JPSEC bitstream. The next two sub-sections explain these two marker segments respectively.

3.1 SEC Marker Segment

The SEC segment is located in the main header of JPSEC bitstream, and it signals general security parameters of the applied JPSEC tools. Figure 3 gives the overall syntax of the SEC segment when N JPSEC tools have been applied. The segment starts with the two-byte **SEC** marker $0xFF65$. L_{SEC} is the length of the SEC segment, including the two bytes for L_{SEC} , but not the two bytes for the SEC marker itself. Z_{SEC} is a SEC marker segment index, since there may be multiple SEC segments in one JPSEC bitstream. P_{SEC} is a parameter that describes the security parameters relevant to the entire JPSEC bitstream, not specific to an applied tool. The next N **tool syntaxes** correspond to the N applied tool instances. For instance, the first **tool syntax** is for the last applied tool instance, and the last **tool syntax** is for the first applied tool instance. Some tool instances could use the same tool, for example, the same tool can be applied three times, generating three tool instances. In order to consume such JPSEC bitstream, the N **tool syntaxes** have to be processed in the order of appearance. In addition, when multiple SEC segments appear in the main header, they are also processed in order of appearance.

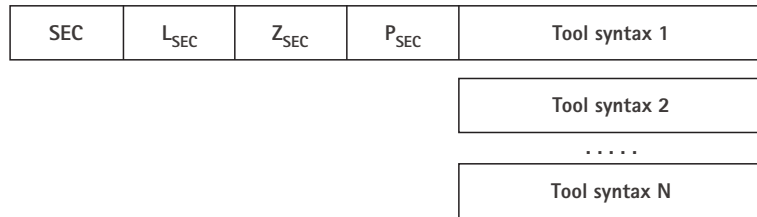


Figure 3: SEC marker segment syntax

Figure 4(a) gives the **tool syntax** of template protection tool, and all fields are normatively defined in JPSEC standard. The field ***i*** is a unique identifier of the applied tool instance within the JPSEC bitstream. This field can be used to associate with INSEC segments that scatter in JPEG2000 bitstream. The field **ZOI**, or Zone Of Influence, has a powerful syntax to signal the covered areas in terms of both image related parameters (such as tile, resolution, precinct, layer, component and region of interest) and non-image related parameters (such as byte range). More details can be found in Section 5.4 of JPSEC standard [4]. **L_{ZOI}** is the length of **ZOI** in bytes. In addition, JPSEC also defines some templates to accommodate the parameters that are common to specific JPSEC security services. For example, there is an encryption template for confidentiality service, authentication template for authentication service, and integrity template for integrity protection service. Depending on the targeted service of the tool, the field **T** in Figure 4(a) contains one of the defined templates. The field **PD** is to indicate at which domain this tool is based on. The possible domains include wavelet coefficient, quantised wavelet coefficient and bitstream domain. For instance, if a tool provides confidentiality by scrambling wavelet coefficients, it is based on wavelet coefficient domain; if this is done by scrambling the bytes in the bitstream, it is based on bitstream domain. The field **L** is the length of **T** and **PD** in bytes. Finally, the field **G** is to indicate the unit of protection, which can range from tile to codeblock.



a) Syntax for template protection tool



b) Syntax for RA protection tool

* Fields with grey colour have variable length

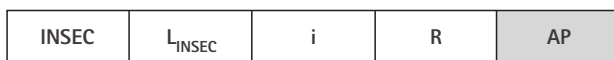
Figure 4: Tool syntax

The tool syntax of the RA protection tool, as shown in Figure 4(b), has two things different from that of the template protection tool. One difference is that it has a unique ID assigned by Registration Authority. The other difference is that the syntax of the field **P** is not specified in the normative part, in contrast to the **T**, **PD** and **G** fields in template protection tool syntax. Each RA protection tool may have its own syntax for the **P** field, which must be registered with Registration Authority. Therefore, the RA protection tool has more freedom to define proprietary syntax according to its own needs.

3.2 INSEC Marker Segment

The SEC segment in the main header contains the general security parameters that are applicable to the whole bitstream. However, some other parameters are applicable only to a small portion of the bitstream. For example, when a JPSEC tool encrypts each packet using a different key, the key parameter is only applicable to one particular packet. In this case, it is more efficient to signal this type of parameters at the location that is immediately proceeding or following the associated portion. The INSEC segment is created for this purpose.

The INSEC segment can be placed anywhere in the bitstream coded data. It makes use of the fact that the arithmetic decoder of JPEG2000 stops reading bytes from the bitstream when it encounters a termination marker (i.e. two bytes with a value greater than 0xFF8F). This interesting feature is used to add extra bytes in the bitstream without affecting the syntax compliance. Figure 5 shows the syntax of INSEC segment. The **INSEC** marker is 0xFF94, **L_{INSEC}** is the length of INSEC segment in bytes. The field **i** is used to associate this INSEC segment with a tool instance in the main header. The field **R** indicates the portion of bitstream to which this segment is applicable, i.e., the portion starting from proceeding INSEC to current INSEC, or from current INSEC to the following INSEC. The field **AP** contains other useful parameters like decryption key.



** Fields with grey colour have variable length*

Figure 5: INSEC marker segment syntax

4 Available JPSEC Tools

Currently, the JPSEC standard includes 10 JPSEC tools as informative examples in Annex B of JPSEC FDIS [4]. This section summarises these 10 tools, and more details can be found in the FDIS [4] and the given references. Note that a tool may be able to provide more than one security services.

Out of these 10 example tools, three tools are for integrity protection and authentication service, including a unified authentication framework [6, 7], authentication method that enables secure scalable streaming and secure transcoding [8, 9] and scalable authentication method [10]. All these three tools are able to retain the rich

structures of JPEG2000 bitstream. But the first tool [6, 7] integrates both fragile (based on bitstream data) and semi-fragile authentication (based on image content), thus, it can be used to protect JPEG2000 images in a broader range of applications like medical imaging, image streaming, image editing, etc.

Another three example tools are for confidentiality service: selective packet-based encryption [11], encryption that enables secure scalable streaming and secure transcoding [8, 9] and encryption that prevents marker emulation [12]. All these three tools support scalable encryption of JPEG2000 bitstream. However, the second tool [8, 9] achieves two seemingly conflicting goals simultaneously: end-to-end security and transcodability. The protected bitstream can be transcoded or adapted by a third-party entity without unprotecting or decrypting the bitstream. The third tool [12] is able to prevent marker emulation, thus, the encrypted bitstream is compliant with JPEG2000 Part-1 standard [1].

There are five example tools for access control services: flexible access control scheme [13], key generation for access control [14], wavelet and bitstream domain scrambling for access control [15], progress access [16] and access control based on data splitting and luring [17, 18]. Basically, the first [13], second [14] and fourth [16] tool are quite similar in that they all rely on the same key generation technique. The third [15] tool controls the access by scrambling the sign bit of wavelet coefficients or by scrambling the bytes in the JPEG2000 bitstream, which is light-weight method in terms of computation complexity. With the last tool [17, 18], a small portion of the original bitstream is extracted into a control file and replaced by random noise. The control file, which could be quite large in size, is used as a key to access the original data. Furthermore, the tool is vulnerable to collision attack, and original bitstream could be recovered by comparing different protected version of the same bitstream.

Moreover, JPSEC standardises an open framework for protecting JPEG2000 images. In the future, when more advanced technique is invented, it can always be incorporated into JPSEC framework by registering a new tool with the Registration Authority.

5 JPSEC Applications

The security services provided by JPSEC are vital to many applications where digital images are heavily involved. Generally speaking, digital images can be classified into three categories. The first category of images has very important content; the owner wants to keep it confidential or control access to the image. For example, when a reporter captures a very important photo, he may want to encrypt this photo before sending it back to his headquarter, as he does not want his competitor to see the content of this photo. For this category of images, it is necessary to apply JPSEC tool for confidentiality and access control services.

The second category of images may not have important content, but their integrity and authenticity are much more important. One such example is the digital surveillance, where it is important to tell the integrity and authentication of the received images. In case the image is modified by a malicious attacker, the receiver should be able to detect it. For this category of images, it is necessary to apply JPSEC tools providing integrity protection and authentication services.

The third category has the attributes of the above two categories, i.e., image content is important, and its authenticity and integrity are important, too. One such example is the image transmission in the military battlefield, where the enemy may try to access, modify or forge the digital images. In this situation, it is necessary to apply JPSEC tools providing confidentiality, access control, integrity protection, and authentication services.

The above applications of JPSEC can be summarised by a common JPEG2000 image distribution application, as depicted in Figure 6, where the images are distributed from the image owner or publisher to the end-receivers in three steps, namely JPSEC bitstream creation, JPSEC bitstream delivery and JPSEC bitstream consumption.

The first step, JPSEC bitstream creation, is accomplished by the JPSEC creator, which is in charge of generating JPSEC bitstream by applying various JPSEC tools. This step is normally done by the image owner or publisher. The JPSEC creator takes inputs like the covered area to be protected, required security services and the related security parameters (like encryption key, encryption algorithm, etc). Based on the tool descriptions downloaded from RA and the inputs, JPSEC creator decides which tool(s) should be applied to provide the required security services and in which order to apply them. The output of JPSEC creator is the JPSEC bitstream.

The second step, JPSEC bitstream delivery, is to transfer the JPSEC bitstream from the image owner or publisher to the end-receivers via a network or media like CD-ROM. During the transfer, the JPSEC bitstream may be transcoded or adapted to suit the dynamic network situation or end-receiver's capabilities. For example, if the end-receiver is a PDA with very low resolution and limited bandwidth, the JPSEC bitstream may be transcoded to a lower resolution and lower bit-rate. The transcoder could be normal JPEG2000 transcoder or JPSEC-aware JPEG2000 transcoder. In any case, it is desirable that the transcoded version of the JPSEC bitstream could still be protected.

The final step, JPSEC bitstream consumption, is to process the received JPSEC bitstream, which might have been transcoded by some intermediate entities. The JPSEC consumer first needs to identify the applied tool(s) by reading the SEC marker segment in the main header. After that, JPSEC consumer invokes those tools in order to render the received JPSEC bitstream. The output of JPSEC consumer includes the reconstructed image (like decrypted image) and security outputs (like verification result).

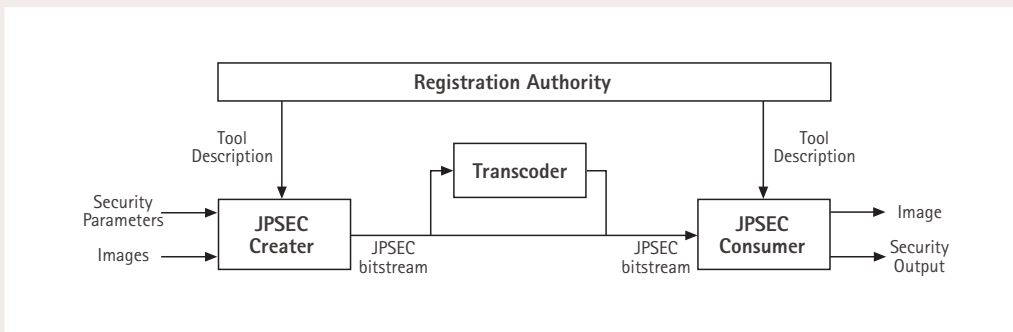


Figure 6: JPEG2000 image distribution application scenario

6 Conclusion

This article has given an overview of the JPSEC framework consisting of JPSEC application, JPSEC tool, Registration Authority and bitstream syntax. The four components work hand-in-hand to deliver various security services. The bitstream syntax is normatively defined for the signalling of the security parameters, thus providing a common language interface among the different entities of the framework. The JPSEC standard includes 10 informative tools, as summarised in Section 4. At the time of this article, no tool for ownership protection service is available. This article also demonstrates how JPSEC could be used in some application scenarios.

7 Acknowledgements

The authors thanked ITSC/MRTC Singapore, especially Mr Lee Chak Joo, for their enthusiastic guidance and support.

8 References

- [1] Information Technology - JPEG2000 Image Coding System, ISO/IEC International Standard 15444-1, ITU Recommendation T.800, 2000.
- [2] Information technology - digital compression and coding of continuous-tone still images - part 1: Requirements and guidelines, ISO/IEC International Standard 10918-1, ITU-T Rec. T.81, 1993.
- [3] Information technology - lossless and near lossless compression of continuous-tone still images, ISO/IEC International Standard 14495-1 and ITU Rec. T.87, 1999.
- [4] JPSEC Final Draft of International Standard, ISO/IEC/JTC 1/SC29/WG1/N3853, February 2006.
- [5] Call for expression of interest in JPEG2000 Registration Authority, ISO/IEC JTC 1/SC29/WG1/N3359.
- [6] Z. Zhang, G. Qiu, Q. Sun, X. Lin, Z. Ni and Y-Q. Shi, A unified authentication framework for JPEG2000, in IEEE International Conference on Multimedia and Expo (ICME), 2004.
- [7] Z. Zhang, G. Qiu, Q. Sun and X. Lin, Z. Ni and Y-Q. Shi, A Unified Authentication Framework for JPEG2000, ISO/IEC/JTC 1/SC29/WG1/N3211, March 2004.
- [8] S. Wee and J. Apostolopoulos, Secure transcoding with JPSEC confidentiality and authentication, to appear in IEEE International conference on image processing (ICIP), 2004.
- [9] S. Wee and J. Apostolopoulos, HP's updated proposal on 'Secure Scalable Streaming and Secure Transcoding for JPSEC', ISO/IEC/JTC 1/SC29/WG1/N3251, March 2004.
- [10] Y. Wu, D. Ma and R. Deng, ImTrust: Design and Implementation, ISO/IEC/JTC 1/SC29/WG1/N3075.

- [11] Y. Sadourny and V. Conan, 'Description of THALES Communication Proposal on JPEG-2000 Codestreams Encryption', ISO/IEC/JTC 1/SC29/WG1/N3078, October 2003.
- [12] J. Hayashi and K. Iwamura, Encryption tool for JPEG 2000 access control, ISO/IEC/JTC 1/SC29/WG1/N3205, March 2004.
- [13] D. Ma, Y. Wu and R. Deng, ImAccess: Flexible Access Control to JPEG2000 Image Codestreams, ISO/IEC/JTC 1/SC29/WG1/N3001, June 2003.
- [14] J. Hayashi and K. Iwamura, Key generation tool for JPEG2000 access control, ISO/IEC/JTC 1/SC29/WG1/N3206, March 2004.
- [15] F. Dufaux, Y. Abdeljaoued, F. Aspert and T. Ebrahimi, EPFL's Proposal for JPSEC Core Experiment v2.0, ISO/IEC/JTC 1/SC29/WG1/N3209, March 2004.
- [16] J. Hayashi, K. Iwamura, Y. Wu, D. Ma and R. Deng, Progressive Access to JPEG 2000 Codestream, ISO/IEC/JTC 1/SC29/WG1/N3204, March 2004.
- [17] J. Caporossi, Protection of JPEG2000 data: the Medialiving technology, ISO/IEC/JTC 1/SC29/WG1/N3207, March 2004.
- [18] J. Caporossi, The Medialiving core experiment 2.0, ISO/IEC/JTC 1/SC29/WG1/N3208, March 2004.

