A Method for Protecting and Controlling Access to JPEG2000 Images

Carlos Serrão[*a], António Serra[*a], Pedro Fonseca[*a], José Miguel Salles Dias[*a]
[a]UNIDE/ADETTI/ISCTE – Associação para o Desenvolvimento das Telecomunicações e Técnicas de Informática, Ed. ISCTE, Av. Das Forças Armadas, 1600-082 Lisboa, Portugal

ABSTRACT

The image compression standard JPEG2000 brings not only powerful compression performance but also new functionality unavailable in previous standards (such as region of interest, scalability and random access to image data, through flexible code stream description of the image). ISO/IEC JTC1/SC29/WG1, which is the ISO Committee working group for JPEG2000 standardization is currently defining additional parts to the standard that will allow extended functionalities. One of these extensions is Part 8 JPSEC – JPEG2000 security, which deals with the protection and access control of JPEG2000 code-stream. This paper reports the JPSEC activities detailing with the three core experiments which are in progress to supply the JPEG2000 ISO Committee, with the appropriate protection technology. These core experiments are focusing on the protection of the code-stream itself and on the overall security infrastructure that is needed to manage the access rights of users and applications to that protected code-stream. Regarding the encryption/scrambling process, this one deals with the JPEG2000 code stream in such a way that only the packets, which contain image data information are encrypted. All the other code-stream data will be in clear mode. This paper will also advance details of one of the JPSEC proposed solutions for the security infrastructure – OpenSDRM (Open and Secure Digital Rights Management) [16], which provides security and rights management from the content provider to the content final user. A use case where this security infrastructure was successfully used will also be provided.

Keywords: DRM, Registration Authority, encryption, protection tool

1 INTRODUCTION

While the increased availability of bandwidth resources is getting momentum in the current Internet, allowing the publishing of richer multimedia content over the network, also the level of threats to this publishing process is increasing. Main threats arise from the fact that if this type of content isn't properly protected, it can be freely used (by free, in this context, we mean that can be used without the payment of any fees to the content owner) or modified without regarding to the author´s own rights of such content.

Issues related to Intellectual Property Rights (IPR) first rose with the wide spread use of the MPEG-1/2 Layer 3 (MP3) Audio Standard, also known as the MP3 phenomenon (helped in some extend by the Naspter case), in which users have exchanged and acquired freely over the Internet music in digital format, without having to pay any royalties or fees to the music editors or to the music creators. In the present days, this is a problem that surpasses the borders of the music world, addressing also other audio-visual standards, such as video (MPEG-2 or MPEG-4) and other digital imaging standards. ISO standardization bodies, such as MPEG or JPEG, are raising their interest in the development of solutions that may help preventing these aspects.

In the case of digital imaging, the new image compression standard JPEG2000, is defining a new extension called Part 8 JPSEC,which is normalizing technology for the protection of the JPEG2000 code-stream. This new part is currently discussing on how to provide the necessary protection mechanisms to a JPEG2000 code-stream, which includes specific signaling, encryption, watermarking and a security infrastructure for dealing with digital image rights management.

This paper concentrates its attention in the crucial aspect of content rights protection: the security infrastructure for providing management of such rights in a digital world. It starts by providing a very short overview about the nature of JPEG2000 and which are its main characteristics. It then proceeds with the introduction of the JPEG2000 specific security extension Part 8, JPSEC. After this first introductory stage, the paper describes the proposal made in the issue of Digital Rights Management to the JPEG2000 Committee and, on how this proposal can be integrated in an open-

[*] {carlos.serrao, antonio.serra, pedro.fonseca, miguel.dias}@adetti.iscte.pt, phone +351217903064, http://www.adetti.pt

source Digital Rights Management (DRM) architecture. Finally an application example is provided and some conclusions are drawn from this work.

2 JPEG2000 OVERVIEW

The widespread usage of digital multimedia requires, from the image compression stand-point, higher performance and new features, such as interactivity. The JPEG2000 standard addresses these requirements by defining a flexible and scalable way of accessing compressed images. This new image compression standard fulfills many requirements that have arised from several types of applications (examples include medical imagery, color facsimile, earth observation images and remote sensing, internet use of digital images or scanning). The most important features of the current ISO JPEG2000 standard are [8]:

- Lossless and lossy compression.
- Low bit-rate performance.
- Improved signal to noise ratio and rate distortion metrics, as compared with other Standards such as JPEG.
- Progressive lossy to losseless transmission of the bit-stream and build-up of the image.
- Progressive transmission of the bit-stream, by:
    - Pixel accuracy or quality (controlled by signal to noise ratio and rate distortion metrics).
    - Pixel spatial resolution.
- Independent transmission of each of the multi-components of each pixel.
- Region-Of-Interest (ROI) coding and random access to ROIs, that can be decompressed with less distortion than the rest of the image.
- Random and independent access to precints, blocks or tiles that divide the image.
- Robustness to bit errors.
- Open architecture.
- Content-based description.

These characteristics are detailed in the next points:

- Lossless and lossy compression: some applications like Medical Imagery, Earth Observation or Archiving don't allow any loss of information in the image data, since all details in the image are of extreme importance. Other applications may allow to discard some "irrelevant" information to save storage space or bandwidth.
- Low bit-rate performance: the standard has high quality image compression at low bit-rates when compared to other standards like JPEG (Figure 1).
- Progressive transmission: a client application may ask for an image and define which part of the image it has more interest in, allowing the server to first select the data set from the code-stream that matches that part of the image and send it in a progressive way, increasing the quality as time progresses .
- Region-of-interest coding: an application may define a part of an image, which is to be lossless compressed, while the rest of the image may be lossy compressed.

- Random code-stream access: this feature allows a server application to select the data to send to the client in terms of quality layers, resolution level and component.
- Robustness to bit errors: the inclusion of error resilience markers in the code stream increases the PSNR in noisy channels.
- Open architecture: part 1 and 2 of the standard are free of fees allowing any one to implement is own JPEG2000 encoder/decoder.
- Contend-based description: the jp2 and jpx file formats uses XML boxes to include metadata about the image, author, etc [12].

Figure 1: Reconstructed images at 0.125 bpp with (a) JPEG and (b) JPEG2000

The digital rights protection for images in JPEG2000 is in development in part 8 of the standard (JPSEC – JPEG2000 Security). Part 8 will define the preferred encryption algorithms to be used in the protection of content as well the architecture for image delivery in a secure manner. At this moment the communications protocol to be used in client-server applications is almost finished, part 9 of the standard (JPIP – JPEG2000 Interactive Protocol), and is implementation on known and open standards in use on the Internet (HTTP) will allow the use of secure channels (HTTPS). Parts 10 (JP3D – JPEG2000 3D extensions) and 11 (JPWL – JPEG2000 Wireless) are also in development.

The following block diagram depicts how JPEG2000 works both in the coding and decoding operation (Figure 2).

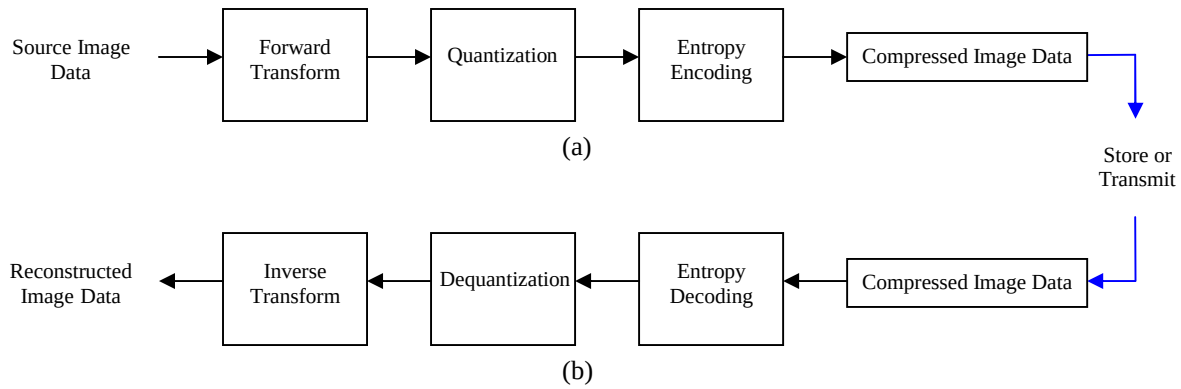

Figure 2 - Block diagram of JPEG2000 (a) encoder and (b) decoder

The standard is based on image tilling compression. Tilling is a technique that divides an image in small squares and applies to each independently the coding. This technique is very useful mainly for memory consumption issues on compression/decompression time. The core of JPEG2000 coding system is the EBCOT (Embedded Block Coding with Optimized Truncation) algorithm developed by David Taubman [8] who also wrote the first versions of the verification model. When encoding an image with JPEG2000, it is first applied a component transformation (RGB to YCbCr), and then the wavelet transform, to obtain the signal coefficients. After this stage, these coefficients are quantized and entropy encoded resulting on the compressed image for storage or transmission. On the decoder side, this process is reversed and the original image obtained.

3 PROVIDING JPEG2000 SECURITY

The part referring to the JPEG2000 security – JPSEC - was defined in WG1 N2388 document [9]. This document provides a good overview on how a JPSEC compliant solution should perform and what should be its scope. According to this document, the scope of security in JPEG2000, will cover the following aspects:

- **Metadata/image linkage integrity check mechanism**: a secure JPEG2000 bit stream will allow users to check for the integrity of the metadata (for instance those in the file format jp2, jpx, etc) associated to the image content. This includes mechanisms for verification of metadata integrity and metadata to image content link integrity [9, 11];

- **File encryption mechanism**: a secure JPEG2000 file will provide a flexible yet clear mechanism to allow for encryption of both metadata and image content. This includes partial encryption of the latter, or encryption with different strengths [9, 11];

- **Source authentication mechanism**: A secure JPEG2000 file will allow for verification of authenticity of the source [9, 11];

- **File integrity mechanism**: a secure JPEG2000 bit stream will allow for the verification of integrity of the content. This includes semi-robust integrity verification, as well as mechanisms to optionally identify locations in the image content where the integrity is put into question [9, 11];

- **Bit-stream conditional access mechanism**: a secure JPEG2000 code stream allows for conditional access to portions of it or to its associated metadata. This could allow for example, to view a low resolution (preview) of an image without being able to visualize a higher resolution [9, 11];

- **Specific recommendations on how to use JPX for security purposes**: JPEG2000 file format allows for previsions for identification of an image, or indications about the intellectual property behind its use. In most cases, these previsions are not defined in details but are more of an enabling mechanism. JPSEC will address some of the issues regarding identification, IP and IPR in a more detailed manner and will propose a recommended way of signaling such information [9, 11].

With these aspects covered, JPEG2000 by opposition to normal JPEG will have also a standardization mechanism to ensure the protection and security of the JPEG2000 code-stream.

Part 8 JPSEC is one of the parts of the standard that is still under discussion and some initiatives have already been started, in the provision of the appropriate security mechanisms to JPEG2000. These mechanisms will cover essentially three aspects: (a) conditional access, (b) security parameter signaling and (c) security infrastructure. As it was referred in the beginning of this document our focus will be in the conditional access and in the security infrastructure aspects of JPSEC.

3.1 PARAMETER SIGNALING

In the issue of security parameter signaling, a new code-stream marker is being defined (SEC) which will be located at the main header. The software tools dealing with JPEG2000 code-streams, will need to be able to detect and read this marker in order to be able to access to the protected code-stream. The existence of security information inside a code-

stream, is signaled by the SEC marker (0xFF94), followed by a list of protection methods. For each protection method, its included a globally unique registration identifier, which is understood in the context of an external Registration Authority, and a list of specific parameters for that protection method.

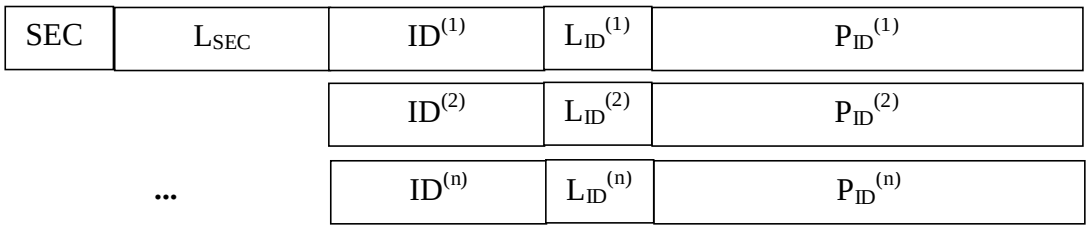

Figure 3 The SEC marker segment in the JPEG2000 code-stream

Mnemonic	Size (in bytes)	Values	Description
SEC	2	0xFF94	SEC marker
L_{SEC}	2	$[0,2^{16}-1]$	Length of SEC marker segment
$ID^{(i)}$	4	$[0,2^{32}-1]$	Registered ID for protection method i
$L_{ID}^{(i)}$	2	$[0,2^{16}-1]$	Length of $P_{ID}^{(i)}$
$P_{ID}^{(i)}$	variable	Unspecified	Parameters for protection method i

Table 1 Format of the security parameters

Each of the security parameter semantics is relative to the specific protection method, which is proprietary and not standardized, and is enforced by a given protection tool that uses a specific encryption, watermarking or scrambling algorithm to protect the JPEG2000 code-stream [10, 13, 14].

3.2 CONDITIONAL ACCESS

The main objective of Part 8 is to identify and implement a complete JPEG2000 system that will allow the conditional access to portions of the code-stream and, possibly, of the file formats. This system should have in mind the following requirements:

- **Functionality**: selective access to the following parts of the code-stream: whole stream, tiles, resolutions, quality layers, precincts, components, regions of interest, code-blocks; selective access to the metadata in the file format.
- **Robustness**: How secure is the solution ?. it should be difficult to break the solution.
- **Efficiency and complexity of the solution**. What is the required overhead in terms of processing time, storage usage and data expansion ? The ystem should bear in mind the trade-off between efficiency and complexity.
- **Flexibility**: the solution should be expanded to the different JPEG2000 file formats

Several alternatives are possible in the design of each of the components mentioned above. Part 8 is still under development and discussion, although, as mentioned, some proposals have already been submitted to the JPSEC group of the ISO Committee. Also, a core experiment was setup to test the proposed solutions [16].

3.3 SECURITY INFRASTRUCTURE

The most recent discussions held in JPSEC in terms of security infrastructure indicate the existence of a Registration Authority (RA) that will be capable of registering protection tools. To each of the protection tools the RA will assign a globally unique registration identifier (32 bit long) which then is used in the SEC marker inside the code-stream.

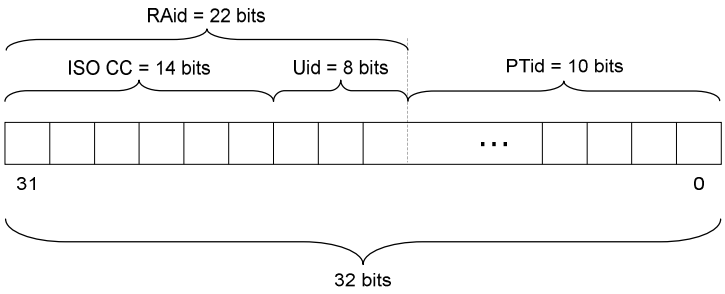

Figure 4 Registration Authority unique identifier

As proposed, the RA identifier will be composed of two parts: Registration Authority identifier (RAid) and the Protection Tool identifier (PTid). The RAid identifies the RA and is assigned by a JURA-like authority [18], managed and controlled by ISO JPEG. This RAid is 22 bits long (14 bits for the ISO country code and the remaining 8 bits (2^8) for the identification within the country). The PTid is 10 bits long allowing the registration of 2^{10} different protection tools within a RA. The maximum number of possible protection tools registered by this scheme is: COUNTRY_CODE x 2^8 x 2^{10}. An example of a complete protection tool identifier could be PT3210, meaning that the tool was registered with number 10 within the RA which identifier is PT32.

Before a RA can register and issue protection tools identifiers, it must obtain at a JPEG managed infrastructure (JURA-like) a RAid. This process occurs through the filling of an appropriate application to a JPEG authority. Specific information about the candidate RA is verified and a RAid is issued and registered. A web-service interface will be available at the JPEG authority to allow the public information query on a specific RA.

A specific RA may operate in the following manner:

- A Protection Tool creator (PTc) registers a protection tool (PT) at a RA. This process may involve or not the actual upload of the PT to the RA. The RA issues a unique id to the PTc and PT;

- An Image Producer (IMp) that whishes to protect its JPEG2000 images can use directly a previously agreed protection method (closed model), which inserts in the image code-stream the identifier of the protection tool issued by an RA. This may happen in the case of commercial relationship between the IMp and a specific PTc. If such previous agreement doesn't exist, the IMp may list the available tools at the RA and list the characteristics of the tools (open model). The IMp can download from the RA a protection tool which inserts in the image code-stream the identifier of the protection tool issued by the RA;

- When the protected images are delivered to final users, the applications will either have already installed the protection tools that will control the access to the image (closed model) or they will be able to identify from the code stream marker the place where they can download the tool (open model).

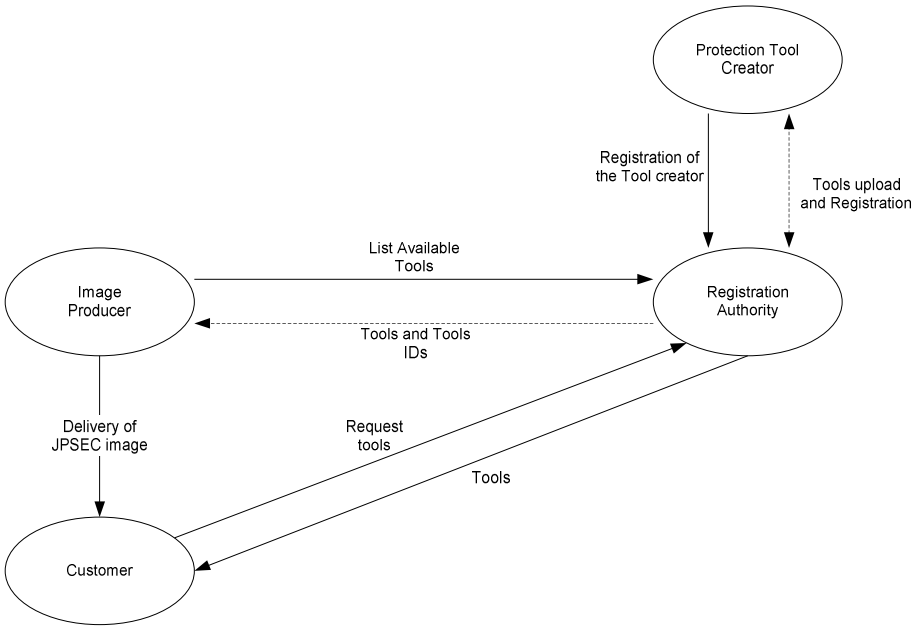

Figure 5 Protection tools RA operation

The security features described in this section can be achieved using a technological solution called Digital Rights Management (DRM). Although the JPSEC is somewhat vague in terms of concrete protection methods that will be applied to JPEG2000 code-streams and how will the IPR be managed, one specific protection method can be proposed for ensuring the protection, access control and management digital rights information within JPEG2000 images. The following section will provide description of this method based on DRM technology.

4 OPEN AND SECURE DIGITAL RIGHTS MANAGEMENT

DRM is the chain of hardware and software services and technologies governing the authorized use of digital content and managing any consequences of that use, throughout the entire life cycle of the content [7].

DRM technology has been developed to protect the commerce, intellectual property ownership and privacy rights of digital content creators and owners as it travels through the chain, from producer to distributor to consumer and, even further, from consumer to other consumers (by consumer, we mean any recipient of the content). It persistently protects and governs content based on usage rules specified by the content owner and rights held by the consumer. DRM can be used to control and track authorized access and use for marketing, sales, royalties, penetration, and accountability reasons. For these reasons, DRM can be an important component of an organization's business strategy [7].

Different types of organizations may have different motives for protecting and managing their digital content. Content owners and service providers may want to control access to their content in order to generate revenue from its sale, while an enterprise may want to share content but not sell it. In an enterprise, where content is shared but not sold, access to content is generally controlled through username/password authentication. This, however, does not control the policy or what users can do with the content once they have access to it. DRM provides three benefits: 1) persistent protection of content through encryption, 2) expression and association of usage rules with content, and 3) enforcement of the usage rules.

The proposed DRM solution is called Open and Secure Digital Rights Management (OpenSDRM) and is an open-source approach to DRM technology, currently being used for IPR protection and management in some Research and Development projects in the JPEG2000 and MPEG.

4.1 OPENSDRM ARCHITECTURE

The OpenSDRM architecture (Figure 6) is adaptive [15], which means that it can be configured for use with several business models and different types of content. OpenSDRM deploys a traditional DRM solution for content rights protection and can be applied for publishing and trading of digital multimedia content. Additionally, the security architecture proposed started from the OPIMA international specifications, MPEG-4 IPMP Extensions [2, 3] and the emerging MPEG-21 IPMP architecture [1, 4, 5, 6] as well as with some of the proposals for JPEG2000 standard Part 8 – JPSEC – JPEG2000 security [15].

This DRM solution is composed of several optional elements covering the content distribution value chain, from content production (content author or producer) to content usage (final user). It covers several major aspects of the content distribution and trading: content production, preparation and registration (Content Preparation Server, Registration Server), content protection (Registration Server, License Server, Intellectual Property Management and Protection - IPMP tools server and Authentication Server), interactive content distribution (Media Delivery Server), content negotiation and acquisition (Commerce Server, Payment Gateway), strong actors and users authentication (Authentication Server) and conditional visualization/playback (Media Application, IPMP tools Server, License Server) [15].

Although some of the components (sometimes actors) are external to the architecture, they play a major role in the overall system.

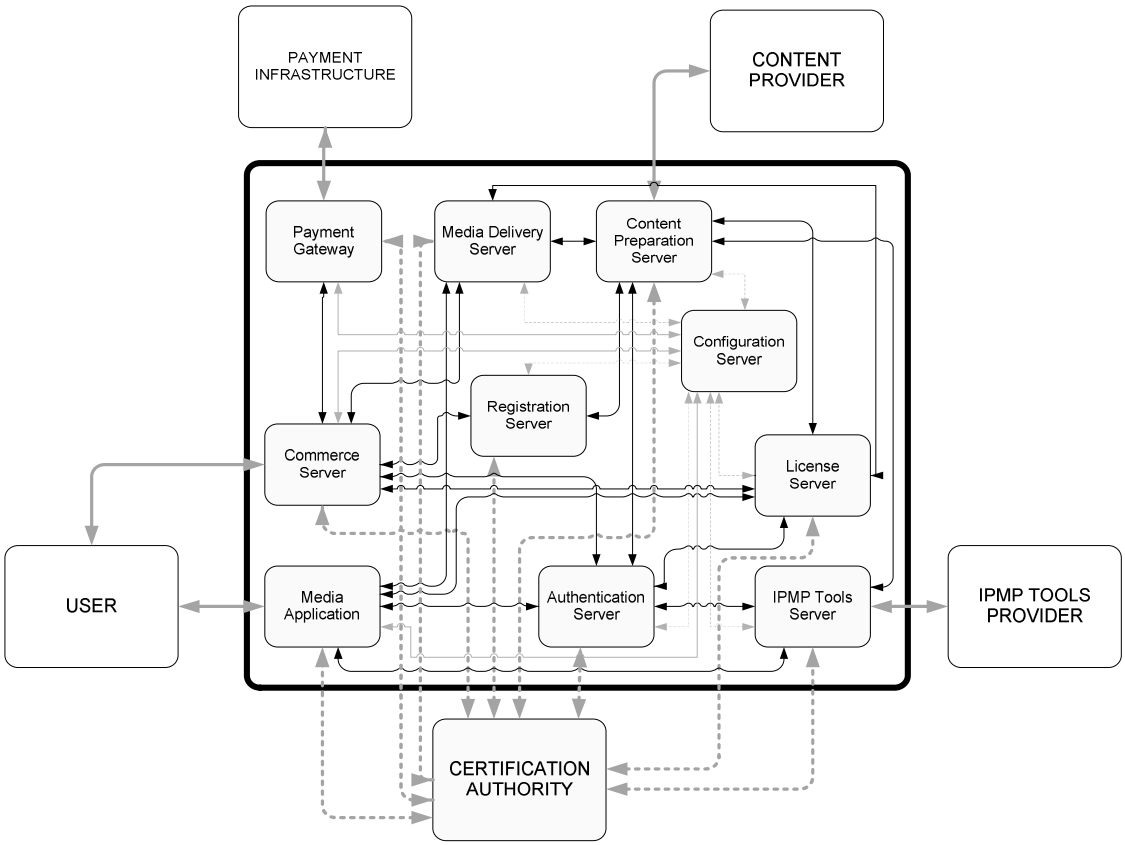

Figure 6 OpenSDRM overall architecture

Among the external actors and components are the Certification Authority, the IPMP tools Provider, the Content Provider, the Payment Infrastructure and the final User. These external components and actors interact externally with the OpenSDRM architecture:

- **User**: the User represents a person who wishes to operate a way of enjoying some part of the content (this content may or may not be protected, however the way to access and display such content may require the use of protected devices, software and licenses). The user will make requests to OpenSDRM in order to: identify him, download licenses and play multimedia content. The requests will be made via a Graphical User Interface, for example, using a web browser or any other specific application (EPG, Media Application). OpenSDRM will provide an appropriate response to the User, for example, by playing the multimedia content. In a final analysis the User interaction with OpenSDRM will always result in one of two things: either the user can play the content and enjoy it or he can't; being then informed of the reason for this prevention.

- **IPMP Tools Provider (ITP)**: the IPMP Tools Provider is any organization that produces tools for encryption, scrambling, watermarking and others that can be applied to content protection (protection tools). These tools will be made available to OpenSDRM for use in content rights protection. The IPMP Tools Provider requests to the OpenSDRM platform the tools upload. The IPMP Tools Provider indicates how the IPMP tool is to be uploaded. An IPMP Tools Provider needs to be registered on the OpenSDRM platform to be able to upload the tools. These tools will need to comply with some guidelines. These guidelines and a subscription translates into a business relation that must exist between a given Content Provider and the IPMP Tools Provider, since mostly, a given producer and/or distributor of content may want to choose which type of protection the content will have and which tools can be applied to the content and from which provider.

- **Content Provider (COP)**: the Content Provider is any multimedia content provider that feeds OpenSDRM with content and/or metadata. The Content Provider uploads the content indicating how it is to be uploaded. The content can be complex multimedia content that is ready for distribution, or simple content, for example JPEG images, that can be edited and combined with other content. A Content Provider must be registered on the OpenSDRM platform in order to be able to use it. This implies the existence of some business relation between the actual author of content and the content distributor (for instance, songwriters or bands and editing companies).

- **Payment Infrastructure (PYI)**: the Payment Infrastructure facilitates OpenSDRM e-commerce features by providing services for handling electronic payments. The Payment Infrastructure will be any infrastructure capable of handling payments. OpenSDRM sends a request to the Payment Infrastructure requesting authorization for a payment. The Payment Infrastructure sends a reply to OpenSDRM indicating whether the payment is authorized or refused. Ideally, the interface between OpenSDRM and the Payment Infrastructure would be generic and independent of the payment method, allowing therefore a multiplicity of payment systems.

- **Certification Authority (CAU)**: the Certification Authority is responsible for receiving requests for, and issuing credentials to entities. These credentials will be used by entities to authenticate themselves to each other, allowing the establishment of secure and authenticated communication channels between them. All the components in the OpenSDRM architecture communicate using the channel security provided by the SSL/TLS protocol. This Certification Authority may be internal to OpenSDRM, and therefore entirely managed by some entity, or it may be an external commercial Certification Authority such as Verisign or Thawte. Either way this will not affect the performance or security of the architecture.

OpenSDRM is also composed by a set of internal components and corresponding interfaces (Figure 6). These components include: Media Application, Media Delivery Server, Commerce Server, Authentication Server, License Server, IPMP Tools Server, Registration Server, Content Preparation Server and the Payment Gateway. Each of these components is described next:

- **Content Preparation server (CPS)**: this server component is responsible for the content preparation. It receives raw content from a specified source or sources and encodes it on a specified format, adds metadata and protects it. If further metadata needs to be added, it is stored on the Registration Server. This server component will interface with: (a) Media Delivery server: this interface will be used to store the content to be delivered to Users in the Media Delivery Server; (b) Authentication server: this interface will be used to identify the content provider in the Content Preparation Server; (c) Registration server: this interface will be used to register uniquely the content being created and associate it with a unique registration number. It will

also register content associated metadata to be consulted afterwards by the Commerce Server; (d) License server: this interface will be used to register the cryptographic keys that were used to protect the content during the production phase. This interface may also be used to establish some pre-conditions that need to be present from the first phase of existence of the content (generic license); (e) IPMP Tools server: this interface will be necessary to present to the content producer the IPMP tools that are available on the system that can be used to protect the content (it also provides a description of the tool, capabilities and the means of obtaining it).

- **Commerce server (COS)**: the Commerce server is a server component responsible for trading the content with the users. Normally, content is chosen via web browser, some very generic metadata might be consulted, information about the price is also available, and especially the content usage conditions might be established. The user must be authenticated to this component through the Authentication server and the licenses for the content are also produced online based on this user authentication and the conditions he chose. This component will interface with the: (a) Media Delivery server: this interface will allow the Commerce Server to alert and prepare the Media Delivery server to start sending the content acquired by the user; (b) License server: this interface will be used by the Commerce Server to request the License Server to produce a new license for a particular content; (c) Registration server: this interface is important for the Commerce Server, since it will allow the Commerce server to obtain all the necessary information about a particular piece of content; (d) Authentication server: this interface is useful because it will allow the Commerce Server to authenticate the Users that will acquire content from it;

- **Media Delivery server (MDS)**: the Media Delivery server is a server component responsible for exchanging parts of the content with the client. This Media Delivery server will implement a specific protocol (download (FTP, HTTP, JPIP or other), streaming (RTSP, other), broadcast) to exchange protected content with the client application. This server component will interface with: (a) Content Preparation server: after the production of the content at the Content Preparation Server it is uploaded (online or offline) to the Media Delivery Server; (b) Commerce server: this interface is used by the Commerce Server to notify the Media Delivery Server that a User will need to access a particular piece of content in a pre-determined way.

- **Registration server (RGS)**: the Registration server is a server component whose role is to assign unique identifiers to content and to register metadata information for that specific content. One of the goals of this architecture is to be as close as possible to standards and therefore for this unique ID, it follows the MPEG-21 directives about Digital Item Identification (DII), using a reduced version of the MPEG-21 DII Digital Object Identifiers (DOI) [5, 6]. This server component will interface with: (a) Content Preparation server: this interface allows the Content Preparation Server to request a unique identifier for a specific part of the content as well as the registration of relevant metadata; (b) Commerce server: this interface will allow the Commerce Server to display/playback content previews and other details of the content itself, allowing the users to browse, preview and obtain more information about the selected content.

- **Authentication server (AUS)**: this server component is responsible for authenticating all the entities, internal and external to the DRM system. It validates the access rights of all the entities and components in the system. The Authentication Server works as a single-sign-on point in the entire system, registering and managing components and users on the system. It uses cryptographic XML credentials to authenticate both components and users in order to authenticate the transactions exchanged between them. This server component will interface with: (a) Commerce server: uses this interface to authenticate the users that wish to acquire multimedia content from the content store; (b) Content Preparation server: uses this interface to authenticate the content providers that want to upload their own content, making it available on the system; (c) Media Application: uses this interface to register new users on the system and to authenticate valid user transactions to other components; (d) License server: uses the interface to authenticate the users that are requesting licenses; (e) IPMP tools server: uses the interface to authenticate IPMP tools providers that provide IPMP tools to the system and that will be used to protect and control the access to the content.

- **License server (LIS)**: the License server is a server component responsible for house keeping the rules associated with a user, the content and his/her corresponding access rights. This component will accept connections from authenticated client Media Applications for downloading of licenses, which will be applied to the protected content through an appropriate IPMP tool. The licenses are XML formatted using Open Digital

Rights Language (ODRL) [5], and, in the future, they will migrate to the Rights Expression Language (REL) [6], currently being developed by MPEG-21. This server component will interface with: (a) Media Application: this interface will allow the user to download the corresponding licenses that are necessary to render a specific content; (b) Commerce server: interfaces with the license server to request the production of licenses for a given content and for a given user according to the commercial relationship established; (c) Content Preparation server: this is used to store the content encryption keys and the generic content licenses; (d) Authentication server: used to authenticate the license download requests.

- **IPMP tools server (ITS)**: the IPMP tools server is the server component responsible for registering new IPMP tools (protection tools) and for receiving authenticated client Media Application requests for the downloading of a specific IPMP tool. It is also responsible for making IPMP tools available to the Content Preparation Server to allow the content protection. This server component will interface with: (a) Media Application: this interface will be used by the Media Application to download the necessary IPMP tools to render the content; (b) Authentication server: this interface will be used to register and authenticate the IPMP tool providers; (c) Content Preparation server: used to make the IPMP tools available to the content production phase.

- **Media Application (MPL)**: this component represents the software that will be used to render the content. This is a generic component with the particularity of being able to display/playback the appropriate content for which the necessary audio/video codec is available (if this codec is not available it may be downloaded from a remote secure server). This application may work with one or several IPMP tools in order to control how the content is accessed by a particular user. This component works on the client side of the general architecture, however it plays an important role in the DRM functions. This client component will need to interface with the: (a) Media Delivery server: this interface is the way the Media Application obtains the content (this can work in a download, streaming or broadcast manner); (b) Authentication server: this interface will allow the user (through the Media Application) to register in the OpenSDRM system and to authenticate; (c) License server: this interface will be used by the Media Application to obtain the necessary licenses to render the content according to the conditions that the user negotiated at the Commerce Server; (d) IPMP tools server: this interface will be used by the Media Application to obtain the appropriate IPMP tools to render the content (codec's, unscrambling tools, watermarking tools, decryption tools, etc.).

- **Payment Gateway (PGW)**: this component will stand between every contact of the Commerce Server (COS) with the Payment Infrastructure (PYI). Its main purpose is to provide the COS with a generic framework of e-commerce payment related functions, whilst hiding inside it all the different details pertaining to the various existing payment methods. This way a number of completely different payment protocols can be used *a priori* and/or added seamlessly in the future, all without compromising the robustness and integrity of the COS component.

OpenSDRM is perfectly capable of supporting the request features of JPSEC, and is also a good candidate for either being used as the support for the RA (which will register protection tools) and at the same time it can act as a protection tool itself.

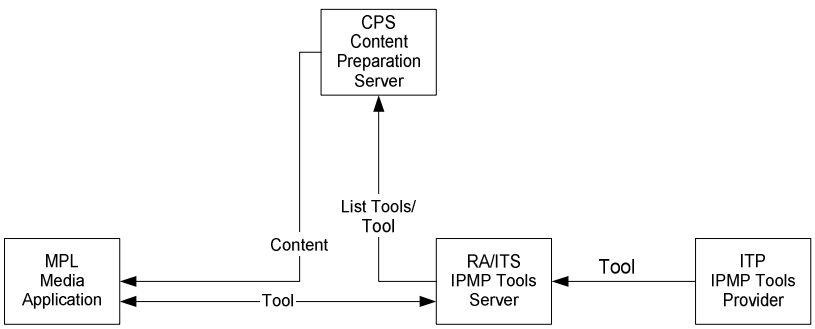

Figure 7 Integration of OpenSDRM within the JPSEC RA

The integration of JPSEC RA within the OpenSDRM platform is a trivial process. OpenSDRM already has a component which is responsible for registering the protection tools associated to content – the IPMP Tools Server. As it was described previously this tool receives requests from tools providers and registers the associated tools assigning unique registration numbers. Additionally, it also provides the means for the content providers to choose the appropriate protection tools and the protection tools download functionality from the Media Application (Figure 7).

5 USAGE EXAMPLE

There are many cases in which these protection mechanisms and DRM infrastructures may be used to protect digital imaging content. For the sake of this paper one specific scenario/example will be considered - Earth Observation (EO) products e-commerce.

Images acquired by remote sensing satellites offer a unique perspective of the Earth, its resources, and the human impact upon them. In little more than a decade, satellite remote sensing has proven itself, as a commercial industry, to be a cost-effective source of valuable information for numerous applications including urban planning, environmental monitoring, agricultural management, oil exploration, market development, real estate sitting and many others [19]. The value of satellite images and the information derived from them are obvious. They provide the user with an overhead look at objects and features on the Earth's surface and help him/her to understanding relationships among those features that might not be as apparent when viewed from ground level. Of course, the 'remote' aspect of satellite imaging also enhances this value by enabling the user to see things halfway around the globe without ever leaving his office [19].

The practical value and applicability of satellite imagery continues to grow as advanced new satellites are launched and join those already in orbit. With more satellites on the way, imagery is available in an increasing - and often confusing - selection of scene sizes, spectral resolutions, revisit frequencies, and spatial details [19]. While these new space-based sensors make imagery more useful than ever, they also present users with greater challenges in choosing the right imagery.

Remote sensing applications require efficient implementation of the compression algorithms for very large images, interactive tools for data selection and personalization of the content. Content security is also a relevant aspect to be considered, which images have intrinsic value that must be protected both in terms of piracy protection and conditional access, for B2B as B2C e-commerce business processes [17].

Images acquired on board space crafts (earth observation satellites, scientific probes, etc) represent in most cases very large volumes of data. It is then necessary to store this data on board (during non visibility period) and to transmit them to ground. Due to the stringent limitations (in terms of mass and power supply) which apply to on-board equipment and to the cost of this equipment, it is essential to reduce to a minimum the on-board storage capacity and the on-board transmission rate needed to fulfill the mission. Therefore the images are on-board compressed using a proprietary compression technique and stored until they are sent to the Earth ground receiving station [19]. The following example will present three scenarios: (1) the registration and protection of images, (2) the secure e-commerce of EO products, and (3) the conditional access to image data.

5.1 REGISTERING AND PROTECTING IMAGES

The Content Preparation Server issues a request to the Registration Server, to register this image. The image is registered in, and a unique ID is assigned to it (this unique ID follows the MPEG-4 DIID format). Metadata for this image is also registered and stored on the Registration Server (this metadata will be obtained directly from the proprietary file format).

The unique image identifier is signed by the Registration Server and embedded into the image code-stream in order to create a persistent association between both. At this stage the image code-stream will be encrypted resorting to cryptographic keys, or other protection mechanism. This encryption results in one original encrypted file with one or more different keys. The encrypted file can be read normally in a JPEG2000 compliant viewer. However, the image will never be displayed appropriately without the correct decryption/unscrambling keys.

The encryption process deals with the JPEG2000 code stream in such a way that only the packets, which contain image data information are encrypted. All the other code stream data will be in clear mode.

The keys used for such encryption process are then sent and stored in the License Server creating an association between the keys and the image unique identifier. The encryption process used is dependent of the IPMP encryption tool (protection tool) to be used, which is chosen by the Content Provider and supplied by the IPMP tools Server.

5.2 SECURE E-COMMERCE OF SATELLITE IMAGES

Satellite images are made available for users through the Commerce Server, which interfaces with the other components in the OpenSDRM architecture. The Commerce Server will be able to request thumbnails from the Content Preparation Server and basic metadata from the Registration Server. It will also be able to control the user's management through the Authentication server.

A User using a normal web browser can access the Commerce Server, via the Internet, and browse through the catalogue looking for available satellite images of his interest and corresponding to his search criteria. To use this catalogue the User must be registered, through the Commerce Server and managed by the Authentication Server. This connection will be secure using SSL protocol.

The Authentication Server registers the User and returns to the Commerce Server a User identifier (secured by SSL). Whenever the User logs in to the Commerce Server, its identity is always confirmed by the Authentication Server.

After being registered and authenticated to the catalogue, the user can place EO product image orders. The User can negotiate with the system the desired type of image access (for instance it will be possible to set the resolution level to which the User wants to be able to access). Price is set upon the User choices. The Commerce Server registers the orders on a database and requests payment information of the User (cryptographic authorization of the Authentication Server on the Users behalf), to the Authentication Server (secured by SSL).

Once the Commerce Server receives payment details from the User, submits that information to the Payment Gateway who handles payments with financial entities (secured also by SSL). The Commerce Server orders to the License Server the creation of a license that will allow the User access to the content in the specified way (this connection must be secured). The license contains the usage conditions and the cryptographic keys needed to access the content. This license is also encrypted in order to guarantee that only the rightful User is allowed to decrypt it.

The Commerce Server also sends information to the Media Delivery Server informing that a specific User has bought the rights to access one particular image. The Media Delivery Server requests from the License Server the user entitlements to access the image. On the server-side this will help to control the user's access limiting it just to the parts he has acquired access to.

5.3 CONDITIONAL DISPLAY OF SATELLITE IMAGING

Either manually issued by the User, or automatically by the web browser, a special purpose OpenSDRM-enabled JPEG2000 application is started. This application starts by communicating with the Media Delivery Server (through SSL). When running for the first time, this application requires the user to authenticate itself.

The application presents to the User a list of images he has acquired and that are available on the Media Delivery Server. Upon the User selection of these images, the application communicates with the Media Delivery server (through SSL), asking for that particular image. The Media Delivery Server gets the image (or part of it) from the file system and sends it to the viewer (using the JPIP protocol over SSL). This Media Delivery Server parses the User license in order to enforce the User's appropriate access to the image data.

The application checks the image data being received and analyses it. If the image is protected then the application retrieves information about the IPMP tool, which was used to protect it, checks if this tool is already installed at the client side and then initializes it. If the tool is not available, the application downloads it from the IPMP tools server (through SSL) and runs it.

The application, using the appropriate IPMP tool, verifies how the image is protected and checks if the User has already downloaded the appropriate license. If a license is found, the IPMP tool also verifies if it is still currently valid. If the license is not on the system, the IPMP tool downloads it from the License Server (using SSL).

If there is already a license in the User system, but it has expired, then the User must acquire a new license at the Commerce Server.

The User can also request the associated metadata with the image, communicating first with the Media Delivery Server and subsequently, getting the metadata from the Registration Server database (using SSL).

The User operates the application to navigate on the image, select parts of it, and perform zoom, pan and other operations. Connection between the application and the Server are secured using SSL and the operations over the image will be limited according to the IPMP tool and the license conditions.

Finally, the User can then save the image to his system according to the conditions established on the license and enforced by the IPMP tool.

6 CONCLUSIONS

Free valuable content is an asset that trends to disappear from open networks such as Internet. This is applicable both for audio visual content, such as digital images. Recently the new JPEG2000 digital image standard has emerged, offering new possibilities to the digital imaging world. One of these new functionalities is security.

Security in this domain poses many challenges, not only in the way of applying the correct protection method to the digital imaging, but also it raising questions on how to control the granular access to the content and on how to manage the content IPR. The Part 8 extension, JPSEC, of the JPEG2000 standard, is normalising the most appropriate solutions to allow JPEG2000 code-streams and file formats to be protected with a set of protection methods, which may range from a simple image scrambling to a complex DRM infrastructure. The protection mechanisms and technologies are, however, independent from the JPEG2000Part 8 JPSEC.

The Registration Authority, RA based tool for JPSEC to register different protection tools, from different vendors, provides JPEG2000 with the possibility of not being tied to any particular protection tool, allowing a more flexible and open protection tools software market. The only visible modification that JPSEC introduces in the JPEG2000 code-stream is the creation of a new specific SEC marker, which will be able to store information about the tool, used to protect the content as well as some specific parameters relevant in the context of that specific protection tool.

As it was already mentioned, this kind of protection mechanism introduce new possibilities in the scene of content trading. An example application in which this aspect is crucial is the electronic commerce of digital images.

Another important aspect that this paper introduces and defends, is that protecting and controlling access to digital images is just part of the equation, when dealing with the overall access to protected imaging content. In fact, if more sophisticated features are required, such as the IPR management, then we stress the fact that DRM technology needs to be employed. In this sense, DRM and, in particular, open source DRM such as OpenSDRM, is a good example of a JPEG2000 protection tool.

7 ACKNOWLEDGEMENTS

The authors would like to thank to all the partners working in close collaboration within the IST PRIAM and IST 2KAN project and also all the contributions made to JPSEC, for the valuable comments and suggestions regarding the issues of the new extensions of JPEG2000.

REFERENCES

1. Jan Bormans, Keith Hill , "MPEG-21 Overview v.4", ISO/IEC JTC1/SC29/WG11/N4801, 2002
2. Jack Lacy, Niels Rump, Panos Kudumakis, "MPEG-4 Intellectual Property Management & Protection (IPMP) - Overview & Applications Document", ISO/IEC JTC1/SC29/WG11/N2614, 1998
3. Craig A. Schultz, "Study of FPDAM ISO/IEC 14496-1:2001 / AMD3", ISO/IEC JTC 1/SC 29/WG11 N4849, 2002
4. Niels Rump, Young-Won Song, Hideki Sakamoto, "MPEG-21 Digital Item Identification and Description (DII&D)", ISO/IEC JTC1/SC29/WG11/N4532, 2001
5. Multimedia Description Schemes (MDS) Group, "MPEG-21 Rights Expression Language Working Draft", ISO/IEC JTC1/SC29/WG11/N4533, 2001
6. Multimedia Description Schemes (MDS) Group, "MPEG-21 Rights Expression Language WD V3", ISO/IEC JTC1/SC29/WG11/N4816, 2002
7. Joshua Duhl, Susan Kevorkian, "Understanding DRM systems - a IDC whitepaper", IDC/Intertrust, 2001
8. David S. Taubman, Michael W. Marcellin, "JPEG2000: Image Compression: Fundamentals, Standards and Practice", Kluwer Academic Publishers, 2001
9. Touradj Ebrahimi, "JPSEC Scope and Requirements 1.0", ISO/IEC JTC 1/SC 29/WG1 N2388, 2001
10. Raphael Grosbois, Pierre Gerbelot, Touradj Ebrahimi, "Authentication and Access Control in the JPEG2000 compressed domain", SPIE 46th Annual Meeting Proceedings, 2001
11. Vania Conan, Claude Rollin, "JPSEC Scope and Requirements 2.0", ISO/IEC JTC 1/SC 29/WG1 N2548, 2002
12. J. Scott Houchin, "JP2 file format specification", ISO/IEC JTC1/SG29/WG1 N1801, 2001
13. Morris Dworkin, "Recommendation for Block Cipher Modes of Operation, Methods and Techniques", NIST Special Publication 800-38A (2001 Edition)
14. Vania Conan, Yulen Sadourny, Stève Thomann, “Symmetric block cipher based protection: contribution to JPSEC”, ISO/IEC JTC1/SG29WG1-N 2771, 2002
15. Carlos Serrao, “JPSEC – Introduction to OpenSDRM architecture and its applicability on JPSEC core experiments”, ISO/IEC JTC 1/SC 29/WG 1 N2723, 2003
16. Vania Conan, Claude Rollin, “JPSEC report and definition of three Core Experiments”, ISO/IEC JTC 1/SC 29/ WG1-N 2694, 2002
17. Carlos Serrao, Vania Conan, Yulen Sadourny, “JPSEC – Protecting the JPEG2000 code-stream”, ISO/IEC JTC 1/SC 29/WG 1 N2650, 2002
18. JURA – JPEG Utilities Registration Authority, http://jura.jpeg.org.
19. Carlos Serrao, Miguel Dias, “Space and Planetary Imaging using JPEG2000”, 7th International Workshop on Simulation for European Space Programmes, ESA/ESTEC, Noordwijk, The Netherlands, 2002