# Space and Planetary Imaging using JPEG2000[1]

Carlos Serrão[(1)], José Miguel Salles Dias[(1)]
*[(1)]ADETTI/ISCTE – Associação para o Desenvolvimento das Telecomunicações e Técnicas de Informática*
*Ed. ISCTE*
*Av. Das Forças Armadas, 1600-082 Lisboa, Portugal, www.adetti.scte.pt*
*Email:{carlos.serrao, miguel.dias}@adetti.iscte.pt*

**ABSTRACT**
The raising demand for Digital content Rights Management (DRM), protection and security, enabling effective on-line access, exchange and trading of all types of digital media items (ranging from a simple text file to a large space or planetary image) and, at the same time, supporting global interoperability of customer devices and traded items, can only be met by a good mix of open architectures and proprietary technologies. In this paper, we present a novel integrated architecture that supports the secure handling of large remote sensing ISO JPEG2000 coded images, obtained from satellite. This effort is within the scope of further developments and new extensions for this standard, namely:
- Trans-coding of proprietary digital image formats used in satellite imagery, to the new JPEG2000 format;
- Inexpensive network clusters for parallel computing to improve the algorithmic process of coding very large digital images obtained from satellites.
- Coding of multi-component and multi-spectral images as well as volumetric images (JP3D);
- Exploration of interactive on-line image satellite catalogues (JPIP);
- Secure transmission, and protection of the image content based in OpenSDRM (JPSEC).

## 1. INTRODUCTION

Images acquired by remote sensing satellites offer a unique perspective of the Earth, its resources, and the human impact upon it. 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 [1].

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 her in 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 her office [1].

The practical value and applicability of satellite imagery continue 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 [1]. 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 personalisation of the content. Content security is also a relevant aspect to be considered [2, 3], whose images have intrinsic value that must be protected both in terms of privacy protection, conditional access and B2B and B2C e-commerce business processes [4, 5].

The image compression standard JPEG2000 [4] 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). The compression performance using JPEG2000 overcomes JPEG, with the drawback of a much higher complexity. For software and hardware platforms, the complexity of JPEG2000 is believed to be around ten times higher than JPEG [4, 5]. This is a crucial problem for its adoption for real-time systems such as earth observation satellites [2].

[1] This work is being funded by the European R&D initiatives IST 28646 PRIAM, "Protected Real Time Access to Mega Images" and IST 34096 2KAN, "JPEG2000 Advanced Networking"

JPEG2000 introduces flexibility in the transmission of images with a progressive improvement in image quality. The standard supports the capability of transmitting arbitrary regions of interest inside the image, with greater fidelity than others. It is also capable of providing lower resolution and/or low quality representations of an image for quick viewing, by only decoding a selected portion of the total transmitted image. JPEG2000 is able to code a wide range of images, from black and white, to greyscale, full-colour (24 bit/pixel) images, to hyper-spectral space and planetary images that typically contain several dozen colour bands [4, 5]. Another important feature is the ability to provide error-resilience during transmission, that is to say, an error during progressive transmission will only affect a small portion of the final image rather than the whole image. As it stands currently, an image than has been compressed to the same final size with JPEG2000 and JPEG, will show much less visible artefacts with the first, due to the increased ability of wavelets to represent an image at low resolution than with the later, where the individual 8x8 blocks become noticeable for large compression ratios. The two formats behave similarly for high quality reproductions but JPEG2000 increasingly outperforms JPEG as more and more compression is introduced, while maintaining the same visual fidelity [4, 5].

The issue of secure access to satellite imagery, is sensitive, since they contain value that image producers and providers, think that requires protection. An effective way for protecting, not only digital images, but also other types of digital content, is to use a Digital Rights Management solution, which deploys protection and security, and controlled access to content and which is particularly relevant in the digital content e-commerce.

In this paper, we present a proposal for a new integrated architecture that supports the secure handling of large remote sensing ISO JPEG2000 coded images, obtained from satellite. This architecture, referred to as openSDRM – Open Secure Digital Rights Management, presents a new open DRM [1] solution being developed by Adetti [6]. This efforth is based on and adapts the technology of several standardization initiatives (OPIMA[2], JPEG2000 and MPEG). Digital items such as large multi-spectral images obtained from remote sensing scenarios (as in Space and Planetary mission scenarios), are clearly an example of content that requires availability and protection, and this is also in the scope of the new ISO JPEG2000 standard. In fact, this standard opens new perspectives for the management of digital imaging content, if we compare it with the current JPEG.

## 2. THE OPENSDRM SOLUTION

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].

The Internet's global reach enables the transmission of content on an unprecedented scale. At the same time, cheap, abundant digital technology makes it possible to create and efficiently distribute all forms of content and information in digital format, including text, images, email, audio, video, software, and games. Widespread Internet penetration, combined with digital technologies, permits anyone with these tools at their disposal to easily make a potentially unlimited number of copies of a piece of content without any degradation in quality and to distribute a single copy to an unlimited number of users. As a result, unprotected digital content is extremely vulnerable to theft, unauthorized access, and propagation [2, 3].

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 farther, 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, and royalty, 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

[2] OPIMA (Open Platform Initiative for Multimedia Access), is an initiative in the Industry Technical Agreement (ITA) program of the International Electrotechnical Commission (IEC), that has been established for the purpose of specifying a platform capable of enabling a framework where content and service providers have the ability to extend the reach of their prospective customers. Likewise, consumers have the ability to access a wide variety of content and service providers, in a context of multiple content protection systems.

protection of content through encryption, 2) expression and association of usage rules with content, and 3) enforcement of the usage rules [1].

The OpenSDRM architecture (Figure. 1) is adaptative [8], which means that it can be configure 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 space and planetary imagery. Additionaly, the security architecture proposed is inline with the recent international specifications OPIMA, MPEG-4 and MPEG-21 as well with some of the proposals for JPEG2000 standard Part 8 – JPSEC – JPEG2000 security [8].

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 and preparation** (Content Preparation Server, Registration Server), **content protection** (Registration Server, License Server, Intellectual Property Management and Protection - IPMP tools server and Authentication Server), **content interactive distribution** (Media Delivery Server), **content negotiation and acquisition** (Commerce Server, Payment Gateway), **strong actors and users authentication** (Authentication Server) and **conditional visualization** (Media Player, IPMP tools Server, License Server) [8].

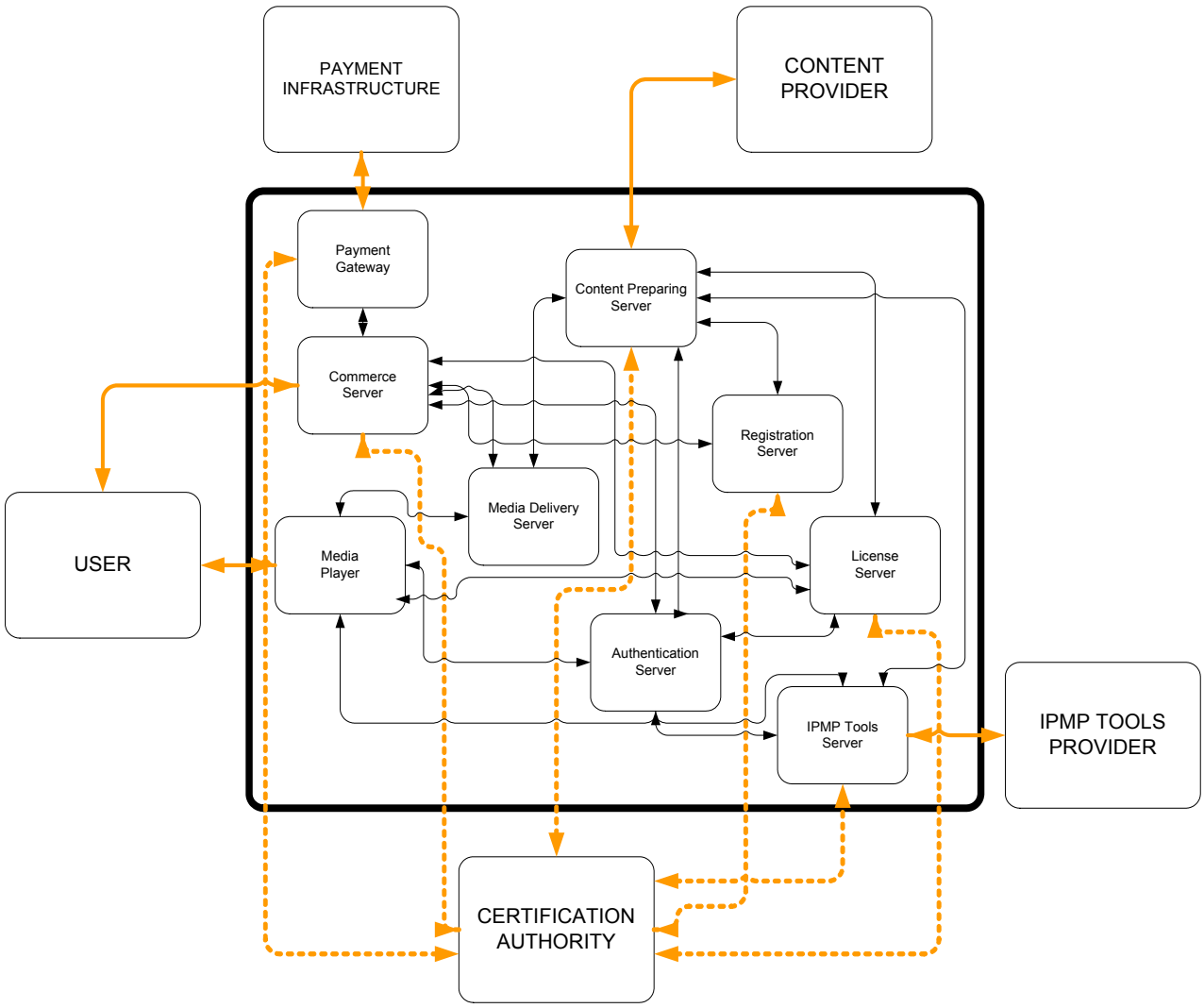


**Figure 1. OpenSDRM detailed architecture**

This architecture provides an integrated DRM solution, interfacing with several external actors which have their own specific role and requirements: **User** (requires access to content), **Content Provider** (wants to make content available for trading, be assured that this content is protected and that it receives a financial return for the traded content**), IPMP tools Provider** (wishes to commercialise their own content security tools), **Payment Infrastructure** (represents the

financial environment) and the **Certification Authority** (the entity responsible for injecting recognised trust on the system).

As mentioned OpenSDRM, currently being developed at Adetti, is being applied to several R&D projects and has been submitted as a reference architecture for the JPEG 2000 security extension, JPSEC.

## 3. OPENSDRM AND SATELLITE IMAGERY E-COMMERCE

The OpenSDRM DRM solution is currently being used on a R&D EC project called PRIAM[3] (IST 28646), in collaboration with SpotImage[4], the commercial operator of the Spot system. SpotImage offers products and services derived from various optical and radar sensors with resolutions ranging from 1 km to 1 m. This architecture will secure the image delivery from the SpotImage image catalogue database to the final consumer [9].

### Requirements for Satellite Imagery E-Commerce

Satellite images present some very specific requirements due to its inherent characteristics. This section focuses the security-based requirements which are applicable to the electronic commerce of these type of images [9].

- User registration: when ordering an image from the catalogue, the user must provide some registration data in order to access the ordering process;
- User authentication: if the user wishes to order an image from the catalogue, he must be authenticated. The authentication process is handled by a normal login and password agreed between the user and the system;
- Image data transmissions between server and client are secure and authenticated: the transmission of image data between the image server and the client will need to be secure and authenticated;
- User online image orders are secure: whenever the user wishes to acquire one image, the ordering process might be handled online in a secure way.
- A payment method must be provided: user payment information must be supplied and verified in a secure way.
- Metadata access protection: The access to the image metadata will be protected;
- User is informed of transitions between secure and unsecured modes: every time the server switches between secure and unsecured mode, a message is sent to the user for information;
- At any time the user can abort the process: when the user aborts the process, the session is switched back to unsecured mode;
- Content (image) protection: this means that the image will be encrypted according to an encryption scheme and will be delivered to the client encrypted;
- Conditional access to different resolution or progression levels: it should be possible to control the user's access to different image resolution or progression levels by partially encrypting the image file with different keys.
- Conditional access to different parts of the images: it should be possible to define and control the user's access to different parts of the image. This will most probably need some kind of trans-coding facilities on the server side for protecting the image on the fly.
- Conditional access combining different parts of the images and different resolution and progression levels: this requirement is the combination of the last two.
- Image quality should not be affected by the protection mechanism: this is a major requirement since the image can never become affected by the usage of some kind of encryption technique.
- Code-stream size should not be affected by the protection mechanism: also, the image code-stream should not increase too much by the usage of an encryption technique.
- Users will have different clearance rights to the image: users when buying the image will negotiate several conditions with the server that will provide an image that will fit the user needs. Payment will reflect the user choices (this could include resolution level, access to metadata information, among others). On the client side, the client platform will enforce the client access through the usage of a specific image viewer and an IPMP tool.
- Metadata access will be protected: the access to the image metadata will be controlled according to the user's clearance level access. Metadata accessible to be user will be recalculated to describe the part of the image and the level of resolution the user has paid for.

[3] Protected Real Time Access to Mega images
[4] http://www.spotimage.com

- Encryption time: time for encryption of image content must be negligible compared to the time for compression and transmission of the image
- Decryption time: Time for decryption of image content must not degrade the time to display the image on the client side.

**OpenSDRM Architecture for Satellite Imagery E-Commerce**

Based on the requirements identified, it was defined an architecture (using OpenSDRM) to adapt to the current SpotImage business model for satellite imagery e-commerce. This architecture is scattered over the network using the new distributed computation paradigm – Web Services.

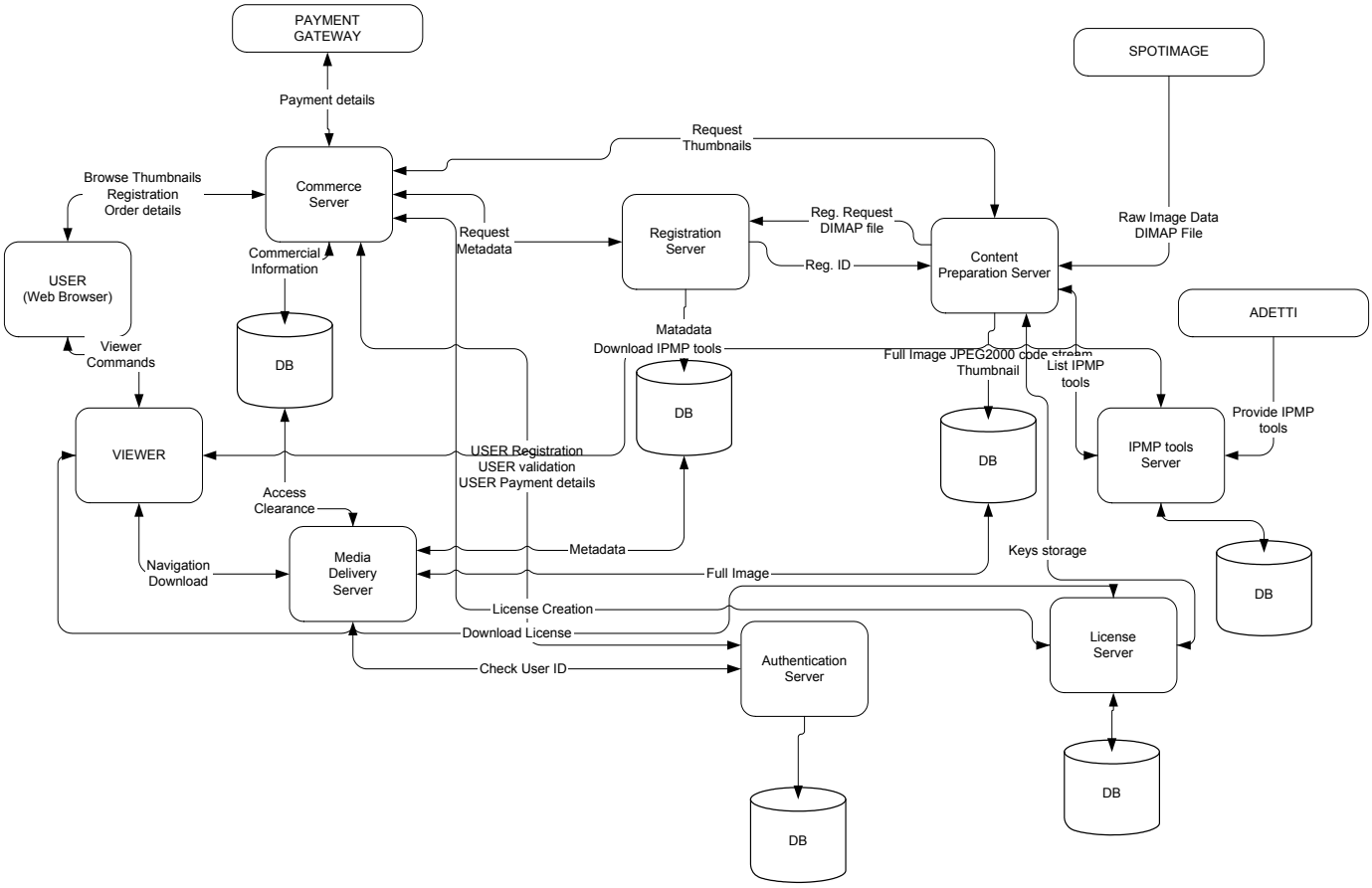


**Figure 2. OpenSDRM architecture adapted for satellite imaging**

All the messages exchanged between the different architecture components use SOAP over SSL/TLS protocol. This assures the security of all the communication messages exchanged on the system. The next section on this paper will present the several different phases of this OpenSDRM-based satellite digital imaging E-Commerce [8].

**Image Acquisition and Preparation**

Images acquired on board space crafts (earth observation satellites, scientific probes ...) represent in most cases very large volumes of data (each image captured by the SPOT5 satellite can go up to 1.73GB in size for the multi-spectral case[5]). It is then necessary to store these 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 fulfil 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 [10].

[5] For image resolutions of 2,5m and 60 Kms size.

JPEG2000 plays an important role in this phase since two original image compression possibilities exist: (a) the first refers to the usage on board of the satellite of a JPEG2000 compression hardware. This solution encodes in real time the raw image data according to dynamic established parameters. The second possibility (b) refers to the usage of a Beowulf Cluster architecture running a parallel version of a JPEG2000 encoder. In this solution the raw data is received from the ground station and it is encoded in JPEG2000 code-stream format. This was the adopted solution, since it was not possible to include a JPEG2000 compression hardware on board of the SPOT5 satellite.

SpotImage, after receiving the data from the SPOT5 satellite, uploads it to Content Preparation Server where it is compressed on the JPEG2000 encoder running on the Beowulf cluster. This is an internal transfer and therefore it is secure. The Content Preparation Server encodes the raw image data into a JPEG2000 code stream and produces also a small image thumbnail in normal JPEG format. This thumbnail will only used for faster browsing of the user in the image catalogue. If a JPEG2000 viewer plug-in is available for the web browser then this thumbnail may not be needed. These resulting images are stored on the Content Preparation Server.

**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 follow the DIMAP specifications).

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 according to cryptographic keys. 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 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 to be used, which is chosen by the Content Provider and supplied by the IPMP tools Server.

**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 its interest and corresponding to her 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 satellite image orders. The User can negotiate with the system the type of image access he desires (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 of the User information (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 to access to the content in the way it was specified by him (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 as bought the rights to access one particular image. The Media Delivery Server requests from the License Server the user entitlements to access the image. This will help on the server-side to control the user access just to the parts he has acquired access to.

**Conditional Display of Satellite Imaging**

Either manually issued by the User, or automatically by the web browser, a special purpose OpenSDRM-enabled JPEG2000 viewer is started (Fig. 3). This viewer starts by communicating with the Media Delivery Server (through SSL). When running for the first time, this viewer requires the user to authenticate itself.

The viewer 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 one of this images, the viewer 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[6] protocol over SSL). This Media Delivery Server parses the User license in order to enforce the User appropriate access to the image data.

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

The viewer, using the appropriate IPMP tool, verifies how is this image 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).

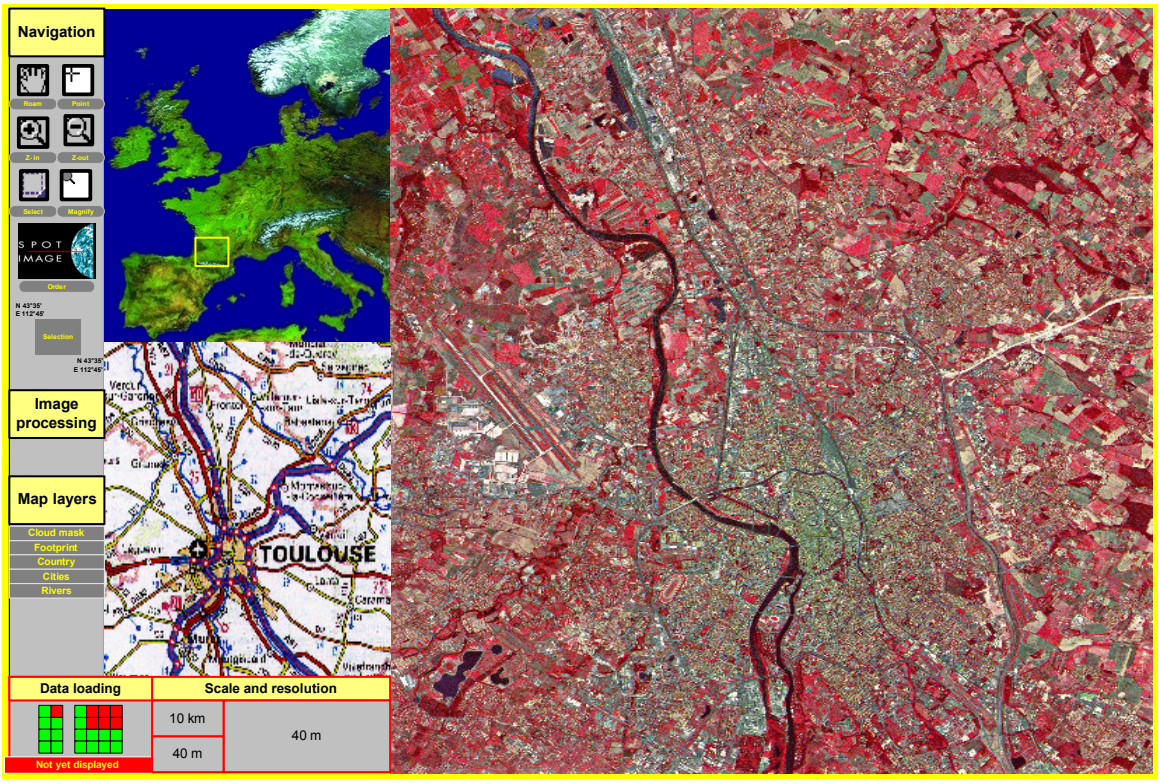


**Figure 3. Interactive Viewer for Satellite Images (source: SpotImage)**

[6] JPEG2000 Interactive Protocol, is being defined in Part 9 of the JPEG2000 standard.

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 viewer to navigate on the image, select parts of it, perform zoom, pan and other operations. Connection between the viewer 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 its system according to the conditions established on the license and enforced by the IPMP tool.

## 4. CONCLUSIONS

Satellite imaging is one of the areas that can take advantage of the new image coding standard JPEG2000. Not only in terms of image compression, a quite relevant aspect, but also from the perspective of the new standard parts being currently specified and developed, such as security, interactive protocols, wireless transmission of images and multi-component and multi-spectral representation capabilities.

The efficient compression scheme of JPEG2000, can handle images with higher quality and dimensions and provide satellites with increased storage capability. The standard can also provide more flexibility due to the compression options it offers [2, 4]. This could help satellite providers to reduce time-to-market in solutions for satellite imaging E-commerce, which can be turned into an important competitive advantage [5].

The new interactive capabilities of JPEG2000 (through its new JPIP extension part) [12], can improve the usability of the satellite images, allowing providers to store on just one image file, all the different resolutions they currently need to make available in multiple redundant files or in pyramidal schemes. On the user point of view, satellite imagery browsing can be greatly improved, with the availability of such interactive features between the image viewer and the server.

In this paper, we have presented OpenSDRM, a generic architecture which can be used to provide security to JPEG2000 images, as well as DRM platform for handling content protection through the value chain of satellite imagery, from producer to consumer [8]. We believe that this type or architecture is a crucial requirement for E-commerce of satellite images. This architecture is being applied in the IST PRIAM R&D project and used together with an image satellite provider to improve the current E-Commerce business model. Information gathered from user trials, will be used as input on the further development of the JPEG2000 standard security extension [2, 3, 8].

## ACKNOWLEDGEMENTS

The authors would like to thank Igor Lapim of Spot Image for the close collaboration within the PRIAM project, and also to our collegues from the IST 2KAN project, Manuel Gamito and Paulo Trezentos from ADETTI, Vania Conan from Thales, Jean Barda from NetImage, Touraj Ebrahimi from EPFL, Claude Rollin from SACD an many others, for the valuable comments an suggestions regarding the issues of the new extensions of JPEGC2000.

## REFERENCES

[1] Lampim, I., “D22 - User’s requirements for remote sensing applications”, IST Project 28646, PRIAM, 2001
[2] Ebrahimi, T., "JPSEC Scope and Requirements 1.0", ISO/IEC JTC 1/SC 29/WG1 N2388, 2001
[3] Conan, V., Rollin, C., "JPSEC Scope and Requirements 2.0", ISO/IEC JTC 1/SC 29/WG1 N2548, 2002
[4] Taubman, D., Marcellin, M., "JPEG2000: Image Compression: Fundamentals, Standards and Practice", Kluwer Academic Publishers, 2001
[5] Adams, M., “The JPEG-2000 Still Image Compression Standard”, ISO/IEC JTC 1/SC 29/WG1 N2412, 2000
[6] www.adetti.iscte.pt
[7] Duhl, J., Kevorkian, S., "Understanding DRM systems - a IDC whitepaper", IDC/Intertrust, 2001
[8] Serrão, C., Conan, V., Sadourny, Y., “JPSEC – Protecting the JPEG2000 code-stream”, ISO/IEC JTC 1/SC 29/WG1 N2650, 2002
[9] Serrão, C., Lampin, I., Meessen, J., “Security Framework Development”, IST Project 28646, PRIAM, 2001
[10] Lampim, I., “D22 - User’s requirements for remote sensing applications”, IST Project 28646, PRIAM, 2001
[12] Taubman, D., “The JPIK Protocol (JPeg2000 Interactive, Kakadu)”, ISO/IEC JTC 1/SC 29/WG1 N2392, 2001