RE-ENGINEERING DIGITAL WATERMARKING OF COPYRIGHT PROTECTED IMAGES BY USING XML WEB SERVICES

George K. Tsolis, Spiridon S. Nikolopoulos, Nancy V. Kazantzi, Dimitrios K. Tsolis, Theodore S. Papatheodorou
High Performance Information Systems Laboratory (HPCLab),
Computer Engineering and Informatics Department, University of Patras
Building B, University Campus, Rion - Patras, 26500, Greece
E-mail: gkt@hpclab.ceid.upatras.gr, nikolopo@ceid.upatras.gr, nvk@hpclab.ceid.upatras.gr,
dkt@hpclab.ceid.upatras.gr, tsp@hpclab.ceid.upatras.gr

ABSTRACT
The main issue addressed in this paper is the renovation of the architecture of a Cultural Information System (CIS) by utilizing XML Web Services, focusing on long-term preservation and protection. The robust, multi-bit digital image watermarking facility is encapsulated in a Web Service, which is reused by several components of the CIS for signing and identifying copyright protected images. In addition, the CIS is similarly extended to integrate a conventional digital object identification service (Handle System), adhering to the principles of service-oriented architectures.

KEY WORDS
Digital watermarking, copyright protection, web services, and information systems.

1. Introduction

Cultural institutions throughout the world increasingly fulfill their needs for streamlined internal operation or worldwide presence via the establishment of Cultural Information Systems (CIS). Typically, a CIS is built around at least one digital repository of cultural artifacts, which are considered the most valuable assets of cultural organizations. Consequently, their long-term preservation and protection is always one of the most important aspects of the design and implementation of a CIS.
The technological advancements of the previous few decades offer numerous opportunities towards preserving and protecting this sensitive material. Cultural artifacts may be digitized with formerly unbelievable resolution and clarity, in both the two-dimensional and three-dimensional space. The resultant digital objects can be maintained in relational databases, which provide ample space to store millions of objects, offering in parallel distributed operation, redundancy and security. Object query may be accomplished by using various user-friendly ways, either via characteristics of the objects themselves (e.g. shape/texture/color similarity), or via information that accompanies them (i.e. metadata).
Open standards were established to govern the characterization and classification of digital objects. The introduction of XML (Extensible Markup Language) [1] by W3C [2] has launched numerous resultant languages, protocols and technologies, which are commonly used today by both research projects and commercial applications. XSD (XML Schema Definition) [3] and RDF (Resource Description Framework) [4] have standardized the processes of defining metadata sets and characterizing resources. Generic metadata sets were introduced, the most popular of which is Dublin Core [5]. In order to accommodate the requirements of vertical applications, specialized metadata sets were also introduced, such as DIG35 [6] and MPEG7 [7], to mention only a few.
The utilization of open standards and established metadata sets ensures the long-term preservation and protection of digital objects. However, cultural organizations still appear to face significant hurdles in their efforts to achieve these goals. Practice shows that their use is not adequate to guarantee the sustainability of the CIS. The conventional implementation approach is mainly responsible for this fact.
Traditionally, IS (not only CIS) are architected with a component-based approach. Typically, the distinct components of the IS are closely interrelated, in such a way that modifications in any one of them subsequently cause extensive changes to other parts of the IS. This fact restricts their maintainability and limits their future expansion.
Web Services [8] are a set of open standards and protocols that were introduced to increase the reusability of the components, by making the binding between them more loosely-coupled. This work explores the use of XML Web Services to re-engineer an existing CIS (PRAXITELIS Project), which was implemented on behalf of the Hellenic Ministry of Culture (HMC) by the High Performance Information Systems Laboratory (HPCLab) of the University of Patras. PRAXITELIS Project was selected as a case-study that demonstrates the usefulness and validity of our approach; the principles and methodology can be applied in any CIS, or IS in general.

2. Overview of PRAXITELIS Project

2.1 Architectural Model

We will describe the architectural model of PRAXITELIS [9] in context of a more general business model, developed as part of the IMPRIMATUR Project (ESPRIT 20676) [10]. The validity of this model was further certified via its subsequent adoption by the TRADEX (TRial Action for Digital object EXchange) Project (IST 21031) [11].

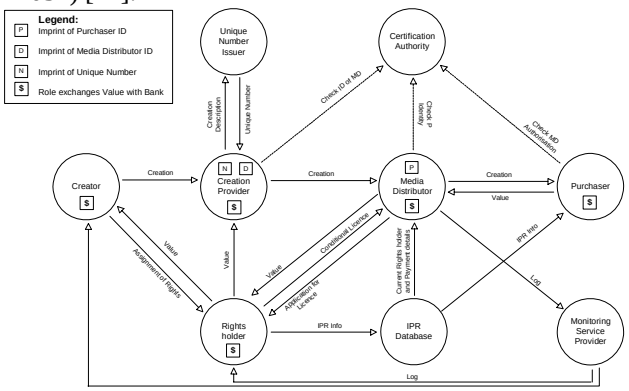

Figure 1: Architectural Model

The players (stakeholders) of the above model are:

- The Creator, who will be the author of the copyrighted work.
- The Rights-holder (or copyright owner). The author does not want, usually, to be involved with the administrative issues related to the management of his intellectual property rights (IPRs); he thus sells to another player the rights to exploit his creations. This player is thus mainly responsible for licensing the use of the creation: he defines the conditions of use, records the IPR information at a registry, and collects the royalties deriving from trading of the works which he is in charge to administer.
- The Creation Provider (or service producer), who will be in charge to prepare creations for being traded in the system, and thus, for example, to embed into creations those mechanisms that will allow the tracking of copyright (watermarks). This player is the repository of the technical knowledge needed to grant that copyright can always be protected.
- The Media Distributor (or service provider), who will have the duty to distribute to Purchasers the creations, and thus will have to satisfy the request of his clients, and to grant that the IPR on the distributed material is protected and the related fees correctly paid. This player will have to offer several simple, preferably electronic, ways to pay for the purchased works, to be able to access the databases where IPR information is stored and to use all technological tools needed to protect the copyright of the creations he trades (watermarking, cryptography, secure protocols). Moreover, he will have to offer to authors, right-holders and other authorized players a set of services to monitor and control the trading of their works, without violating the privacy of Purchasers, and to Purchasers a service as much easy to use as possible.
- The IPR Database or register, which is the repository of all the information related to the IPR of the works to be protected, and that will have to be accessible, at different levels of detail and confidentiality, by all the other players. In particular the information useful for identifying the creation and that detailing the licensing rules, will have to be stored and retrieved effectively; this will allow the correct fees to be paid to the copyright owners.
- The Unique Number Issuer, a naming registration authority who will be responsible for assigning the unique identifier (e.g. the DOI) to each creation, for facilitating its tracking.
- The Monitoring Service Provider or controller, who will be a Trusted Third Party (TTP) responsible for monitoring that all transactions have been carried on legally. The role of the controller is very important, and the establishment of TTPs being in charge of this duty will be one of the key points for the successful diffusion of such systems.
- The Certification Authority, which is also a TTP, which is charged to authenticate all players, by means of electronic certification.

2.2 Existing Implementation

2.2.1 Repository

The repository and IPR Registry of PRAXITELIS project is a Relational Database Management System (RDBMS) [12], which has been implemented in IBM DB2 Universal Database, Version 7.2. The choice of the particular platform satisfies the needs and functional specifications of the project. It is an interoperable tool, supported by most popular operating systems, and provides a lot of functionality. The basic software, in combination with the potential extensions provided, especially the Audio, Image and Video (AIV) Extenders, constitute a useful development tool for digital image repositories. It offers, not only search by image metadata, but also Query By Image Content (QBIC) [13], i.e. search based on the shape, color, texture and other technical parameters of the images.

The database schema is based on the extensive DIG35 metadata set. As a result, the database consists of numerous tables, fields and relations. As part of this work, we will describe only the basic tables used for the electronic shop application, which are essential for understanding the material presented below. The Entity Relation Diagram (ERD) follows in Figure 2.

The principal tables are BASICIMAGE and IPR, where image metadata are stored and a unique identifier is specified for every digital image. The PRICES table currently contains a single price for each image. We chose to implement a separate table, in order to support more rich pricing policies in the future. The BUYER table

keeps the users' personal data and CREDITCARD stores information for users' credit cards, since each user can have more than one credit card. The ORDERS and ORDERSIMAGES tables contain information about orders. For each order, only one record in ORDERS is created, but the number of records created in ORDERSIMAGES depends on the number of images the order consists of.

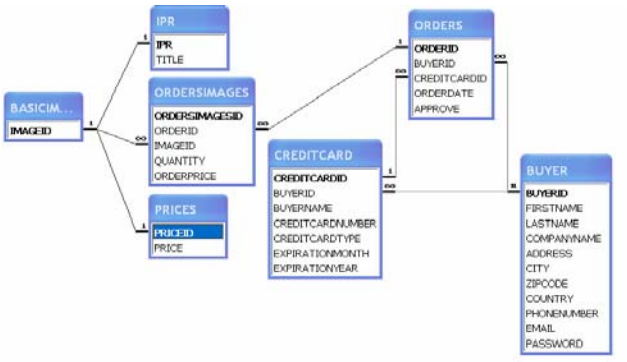

Figure 2: Entity Relation Diagram

2.2.2 Watermarking

During the design and implementation of PRAXITELIS CIS, watermarking was the key functional component used for the protection and management of IPR [14]. PRAXITELIS anticipated for a Web Site serving as a demonstration platform for the rich digital collection of images owned by the HMC. Unfortunately, potential rights violators could easily copy, distribute and commercially exploit the digital images hosted by PRAXITELIS Web Site just by using one of the tools available in the software market. The HMC required for a means to prevent unauthorized users from violating its IPRs. The adopted watermarking system invisibly embeds copyright information inside the image digital content, providing the HMC with a technological means for claiming its rights and proving its ownership over the digital objects. The embedded information represents the HMC's unique and well known copyright notice which is invisibly encrypted into the digital image content. The encryption is based on a private encryption key, used only by the HMC and essential for the decryption procedure. The proof of ownership is impossible without the aforementioned key since the encrypted copyright notice can not be detected.

The method chosen for the adopted watermarking system was mainly based on the elaboration of the MCWG (Multimedia Coding and Watermarking Group) [15] watermarking tool. The core of the MCWG tool is a transform domain technique that is based on the use of the Subband DCT transform [16].

All images were watermarked prior to their exposure through PRAXITELIS Web Site utilizing the HMC private key with the aim of securing the IPRs and preventing acts of copyright violation.

2.2.3 Distribution

One of the fundamental extensions of the project is the electronic sales facility [17], the Media Distributor of PRAXITELIS. The first functionality provided is basket management. Every image the user finds and he is interested in, can be added in his shopping basket and continue his shopping. During this time the user can modify the basket's contents. He may delete an image or change the number of licenses he wants to buy. When he is done, he is directed to the login form (filling in personal and credit card information) in order to buy the selected images. When he finishes with all these, the system sends him an e-mail with the order information, which is equivalent to a receipt. Another functionality provided is user account management. The user can view and change his personal information, but the most useful service is the history of his orders. When an order is approved, there appears a "download" link, in the right hand side of every order, in order to download the corresponding image. The rest, not approved, are marked as "not approved yet".

2.3 Weaknesses of the Implementation

The existing implementation of the CIS presented to this point was accepted and successfully installed at the premises of the Archaeological Receipts Funds (ARF), the primary copyright management authority of HMC. In spite of the success of the original CIS, we have to admit that there is ample room for improvement. More specifically, we have identified certain weaknesses, which are nevertheless justified, since many of the relevant technologies had not yet taken shape during the early stages of development of the CIS. Our work targets to alleviate the following shortcomings:

- The initial implementation of the watermarking function offered limited (single-bit) functionality. This deficiency didn't allow for on-demand watermarking during image distribution. For this reason, and for reasons of simplicity, it was decided that the images would be stored already watermarked in the repository. However, a consequence of this decision was the absence of any per-transaction marking capability. The employment of multi-bit watermarks [18], which are particularly effective for uniquely associating a digital object with its metadata, removed the above shortcomings. The functional model of this experimental improvement is presented in §3.2.
- The image watermarking function was implemented as a software component that was embedded in the image management application. The development platform selected (ActiveX Control, packaged as a dynamically linked library), poses particular requirements on the hardware platform and host applications, in which it can be used. As a result, the reusability of this facility is restricted. The straightforward solution is to introduce a new Web Service that encompasses this component (§3.3.1).
- An additional drawback of the initial implementation was the fact that the front-end electronic sales application was tightly-coupled with the database system. A second

experimental improvement was the redesign of the CIS in order to abstract the communication of the electronic sales facility with the back-end database system. This was accomplished by implementing a prototype Web Service. Moreover, a new sales order approval application, developed in a totally different development environment than the electronic sales application, was added to the internal administration toolset, taking advantage of the functionality of the same Web Service. [19]

- During the design phase of the CIS, the integration of an open object identification system was seriously considered. The HANDLE [20] and DOI [21] systems, although only recently instituted back then, were thoroughly evaluated. However, given the fact that the CIS was supposed to be utilized for internal HMC purposes only, it was decided that the CIS should rather use a simple identification system, based on auto-increment numeric identifiers generated by the RDBMS. On the other hand, the introduction of the electronic sales extension reinstated the requirement for a globally unique object identifier. We propose to tackle this recurring need by developing a new Web Service, which abstracts the interaction of the CIS with the selected object identification system (§3.3.2).

3. Re-engineering the CIS

3.1 Introduction to Handle

The Handle System [20] is a distributed information system designed to provide an efficient, extensible and secured global name service for use on networks such as the Internet. The Handle System is somewhat like DNS, in that it provides a registry to find things online. But it has important differences. While the DNS registers machines (with domain names), the Handle System registers digital objects.

The Handle System includes an open protocol, a namespace and a reference implementation of the protocol. The protocol enables a distributed computer system to store names, or handles, of digital resources and resolve those handles into the information necessary to locate, access, and otherwise make use of the resources. These associated values can be changed as needed to reflect the current state of the identified resource without changing the handle. This allows the name of the item to persist over changes of location and other current state information. Each handle may have its own administrator(s) and administration can be done in a distributed environment. The Handle System supports secured handle resolution. Security services such as data confidentiality, data integrity and non-repudiation are provided upon client request.

Handles can be embedded in URLs and resolved through a proxy server, so that they look just like a "regular" URL. When a handle server resolves an identifier, it returns a handle record which contains owner-specified information for the object, which could be location information, a PKI key, or a variety of different kinds of information or functions about the object such as links to digital rights management or purchase information. In short, the Handle System supports application interactions rather than just queries.

3.2 Watermarking Component Functional Model

The proposed scheme is focused on an integrated service, providing protection and management of IPRs. The core technology supporting functionality requirements is watermarking. Watermark technology integrates encryption methods to ensure unambiguous and categorical proof of ownership, as well as image processing techniques for conveying useful information inside the image digital content. The level of functionality that can be achieved by the proposed scheme depends upon the usage policy of the conveyed information.

According to PRAXITELIS architectural model presented above, the entity that can benefit from adopting the proposed web service within its business model is the Content Provider. Content Provider is responsible for pricing the content, protecting its IP, manage its rights and eventually distribute the content via an electronic shop. New operational modules, that utilize watermarking technology, should be inserted into the operational chain for achieving secure and reliable content delivery.

The Content Provider's primary concern is to secure its ownership over the digital content. Secondarily, it must establish a mechanism capable of describing and identifying financial transactions and agreements over each digital image. Finally, the Content Provider must co-operate with a general naming registration authority in order to obtain unique digital identifiers and assign them to the aforementioned transactions. In our case, this role is fulfilled by the facilities of the Handle System.

A typical scenario includes an organization that owns a great collection of digital images and is willing to sale high quality copies of collection objects for a standard price. Prior to the delivery, the organization embeds a digital watermark inside the image content. The watermark serves three different purposes, a) give proof of ownership, b) identify the transaction that took place and c) correlate the transaction description with the specific image copy. All details necessary for describing a transaction are included within the image metadata information maintained inside the content provider's database infrastructure.

The input argument set, supplied to the watermarking embedding mechanism is consisted of two integer numbers. The first number corresponds to the encryption key while the second to the transaction identification number. The encryption key is used for invoking the core cryptographic module that guarantees for watermark's security. It's a unique private number known used by the copyright holder for the decryption operation and thus the proof of ownership. In the proposed scheme the encryption key is the outcome of a hash function supplied with a seed number. This number constitutes the bases for

the system's cryptographic attributes and should be tightly bound to the copyright holder entity. Thus, there is a need for universal administration of such numbers in order to avoid conflicts and irresolvable disputes. This role is appointed to the aforementioned naming registration authority (handle system), since the produced handles possess the required attributes. In particular, each handle derives as a combination of two distinct numbers, a *prefix* and a *suffix*. The *prefix* is the number assigned by the naming registration authority to an institution after its registration and corresponds to a constant, globally unique number that is officially bound to the specific institution. Among the administration obligations of the registration authority is to ensure the uniqueness of this number under the framework of the handle system. By using the prefix number as the seed number for cryptographically encoding the watermark information within the image digital content, the proposed scheme exploit's the handle system administration facilities for the purpose of successfully resolving every possible dispute, regarding IPRs. The *suffix* is an independent number selected by the institution protocol service and administered locally. According to the conventions adopted by the proposed scheme, the suffix corresponds to the transaction identification number. With respect to the relational database scheme presented above, the transaction identification number is the ORDERSIMAGESID, which is the primary key of the ORDERSIMAGES table. This number is encoded inside the digital image content and can be retrieved by the decryption mechanism. On completion of the aforementioned operations, the content provider is ready to deliver the content.

In case of a dispute over a digital image, the organization must be capable of proving its ownership and retrieving the details regarding the conducted transaction. The organization must fulfill its objectives using just the well-known prefix number and the secret hash function. The hash function, if supplied with the correct seed number, will yield the encryption key used during the encryption operation. The adversary is unable to acquire this key since he is not familiar with the hash function. The detector's response can be separated in two parts. The first part decides upon the existence of the watermark. A negative response means that the organization's watermark is not present and thus can not claim the ownership of the image. A positive response confirms the organization's ownership and resolves the dispute. Apart from the binary outcome, the detector, only when the watermark is present, retrieves the information encoded inside the digital content and returns an integer. This integer is different from the encryption key, corresponds to the transaction identification number and if combined with the prefix will yield the digital identifier that can be resolved and lead to the metadata information describing the transaction details.

Consequently, the e-shop supporting the content provider's distribution infrastructure should deliver only watermark-protected digital copies of collection objects. When the sales personnel approve an order, the Purchaser is notified that he can download the ordered image. The Purchaser should login to the electronic sales system and look at his order history. In the right-hand side of the approved order a "download" link will appear. When this link is selected, an automated administration mechanism should be responsible, initially, for the creation of a digital identifier based on the naming authority prefix number, the invocation of the hash function using some specific identification values acquired from the database, and, secondarily, for the construction of the appropriate watermark, the encryption of the watermark inside the image digital content and finally the correlation of the digital identifier with a URL demonstrating the transaction details. When this is done, the download of the watermarked image will start and the Purchaser will have it saved in his computer. The rights management and control is accomplished via the utilization of the watermarking detection mechanism.

3.3 Web Services Description

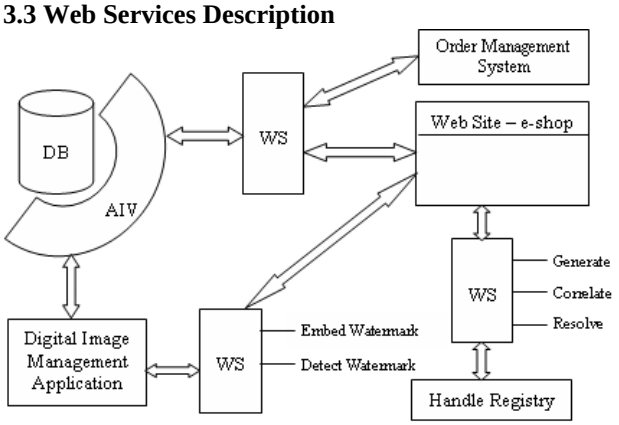

Figure 3: Service-oriented view

3.3.1 Watermarking

The Watermarking Web Service incorporates multiple functionalities inside the content provider's operational chain. Rights protection and management comes as an integrated service provided by the Web Service, with the aim of relieving the end user from the complexity of interfering with the underlying system. Instead, his only interaction is with the supported Application Protocol Interface (API). The API implements two basic interfaces for embedding and detecting digital watermarks.

The interface responsible for the embedding operation (**Embed**) requires five different arguments from the service user:

Encryption Key: An integer value that, when used in conjunction with the hash function, produces a secret number appropriate for the invocation of the cryptographic module.

Transaction Identification Number: An integer value that will be encoded as an imperceptible watermark inside the image digital content.

Input Image File: The binary data of the original unwatermarked digital image.

Output Image File: The binary data of the resulting watermarked digital image.

Strength Modifier: An integer between 1 and 4 indicating the embedding strength of the watermark procedure. A value of 4 produces more robust watermarks, but introduces more distortion to image quality.

The interface response returns a zero value on success of the watermarking process and a negative value in case of failure.

Respectively, the interface responsible for detecting digital watermarks (**Detect**) requires the following input arguments.

Decryption Key: The integer used during the embedding procedure. With regards to the specific watermarking system, the encryption and decryption keys must be identical in order for the detection to be successful.

Input Image File: The binary data of the image under detection.

The detector's response, as already mentioned, is consisted of two parts.

Detection Intensity: Indicating the existence possibility of the watermark inside the image content. If this value is well above a predefined threshold the watermark is considered detected.

Decrypted Information: An integer value representing the number encoded during the embedding procedure. Normally, this number corresponds to the transaction identification number.

The initial, all-in-one, implementation of the Digital Image Management Application was done in MS Visual Basic 6 and the watermarking function was embedded as an ActiveX Control. For the implementation of the Web Service, the development platform of choice was MS Visual Basic .Net 2003. The most significant issue of the implementation was to handle large binary (image) data transactions using SOAP.

The earliest solution was to reference such data objects (large images) on the Web, using URLs. This works well when the data location is stable over time and accessible to the message receiver. However, in situations where information is transient, or when the receiver of the data doesn't have access to the Web, this is not considered a good solution. To address these problems permanently, the data in question has to travel with the message.

The easiest way to put binary data into an XML-based message is to encode it as base64, which converts it into a stream of characters that is safe for XML. The downside of encoding is that it is inefficient; the binary form of data is almost always more compact than the base64 form, because the latter uses a limited range of characters to represent a much richer stream of data. Typically, base64 encoding involves a 33% bloat in the size of a given stream of data, making XML messages even bigger. Additionally, encoding and decoding binary data involves considerable processing overhead, which in turn affects the scalability and performance of applications that use it.

These shortcomings led to the development of SOAP Messages with Attachments (SwA) [22], a Web Services specific technology that uses MIME Multipart/Related packages to send binary data and other attachments alongside XML messages, thus avoiding the overhead of encoding. This avoids the overhead and bloat of encoding. But practice uncovered considerable interoperability problems with SwA. In effect, SwA introduced a new data model for messages, which was not compatible with XML-based messaging principles.

After identifying the issues with SwA, work began on a concrete solution. This started as the Proposed Addendum to SOAP Messages with Attachments (PASWA) [23] and has since been adopted by the W3C XML Protocol Group [24] as the cohesive pair of Message Transmission Optimization Mechanism (MTOM) [25] and XML-binary Optimized Packaging (XOP) [26] specifications.

The idea behind all of this is simple. XOP is an alternative serialization of XML, allowing you to express any XML document as a XOP package. In a XOP package, anything nominated as a base64 string is encoded as an attachment, in much the same way as SwA does. However, the linking between the data and the attachment is different; rather than relying on the application to handle this, the format does so itself.

3.3.2 Digital Object Identification

The Unique Identification Web Service is a typical case of encapsulating and extending a subset of functions of a legacy system (Handle) in a middleware application. The operations of Handle that it leverages are registration and resolution of digital object identifiers. The new capability added is automatic generation of unique numbers. More specifically, the methods implemented are:

Generate: This method generates a new digital object identifier. As already mentioned, handles constitute of a prefix, which is exclusive for each interested party or application, and a suffix. The uniqueness of the prefix is guaranteed by a naming registration authority, which, in our case, is the Global Handle Registry. The suffix is generated by the Web Service as a globally unique UUID [27]. This method does not require any input arguments, since the prefix is static and hardcoded. The only return value is the concatenated identifier.

As we have described in §3.2, PRAXITELIS uses an internal, transaction-specific suffix, the uniqueness of which is assured by the RDBMS. For that reason, if we disregard the added-value benefit, the applicability of Generate in our system is restricted.

Correlate: This method registers a new identifier in the handle server and it correlates it with a transaction marker. The first argument is, of course, the resource identifier, which can be either generated by the method described above, or provided by the application. The second argument is the transaction identifier, which, in our case, coincides with the handle suffix. The only return value is the indication of success, or failure (e.g. in case the handle provided is already in use). The important by-product of this method is that the handle value is also

associated to a specially crafted URL, which references the metadata set of the identified resource.

Resolve: This method is complementary to Correlate. It returns the transaction identifier that corresponds to the handle value provided as an argument.

The primary benefit of this service is based on the fact that handles are globally unique and resolvable. This can be leveraged by applications, both internal and external to the CIS. More specifically, by using a handle resolver, internal users have the ability to directly access the transaction details of a watermarked image, in an attempt, for example, to identify improper use. More importantly, purchasers have the ability to view the publicly available information (metadata) of any image they have acquired.

In another manifestation of the platform independence property, this Web Service is implemented in Java.

4. Conclusion

One of the principal aims of PRAXITELIS is long-term preservation of digital images. This goal is achieved by the future-proof implementation of the digital repository, the standards-based metadata that supplement the stored content, the flexibility of the content management applications and the robustness of the multi-bit digital image watermarking technology.

However, our findings indicate that this seems to only partially achieve the long-term preservation goal in practice, because these attributes do not ensure the longevity of the CIS itself. This occurs mainly because the implementation of each of the subsystems of the CIS, as well as the interaction between them, is closely tied to the intricacies of the software platforms selected, thus discouraging the replacement of any of these subsystems. In addition, it obstructs the maintenance and hinders the improvement of the CIS.

Web Services provide a mechanism for overcoming these deficiencies. This work shifts the existing view of information systems as a set of interoperating components (component-oriented) to a set of distinguished services offered by those components (service-oriented).

References:

[1] W3C, Extensible Markup Language (XML) 1.0, Recommendation, 4 Feb 2004, http://www.w3.org/TR/REC-xml

[2] World Wide Web Consortium (W3C), http://www.w3.org/

[3] W3C, XML Schema, Recommendation, 28 October 2004, http://www.w3.org/TR/xmlschema-0/

[4] W3C, RDF/XML Syntax Specification, Recommendation, 10 February 2004, http://www.w3.org/TR/rdf-syntax-grammar/

[5] The Dublin Core Metadata Initiative (DCMI), http://dublincore.org/

[6] International Imaging Industry Association (I3A), DIG35 Metadata Specification, http://www.i3a.org/i_dig35.html

[7] Moving Picture Experts Group, MPEG-7 Overview (Version 9), http://www.chiariglione.org/mpeg/standards/mpeg-7/mpeg-7.htm

[8] W3C, Web Services Activity, http://www.w3.org/2002/ws/

[9] G. E. Kalamaras, G. K. Tsolis, D. K. Tsolis, P. A. Zafiris & T. S. Papatheodorou, Integrated Environment for the Management, Protection and Exploitation of Digitized Material of the Hellenic Cultural Heritage. *WWW9 - Culture Track*, Amsterdam, Holland, 2000.

[10] Intellectual Multimedia Property RIghts Model and Terminology for Universal Reference (IMPRIMATUR), http://www.imprimatur.alcs.co.uk/index.htm

[11] TRial Action for Digital object EXchange (TRADEX), http://www.iccd.beniculturali.it/download/tradex.pdf

[12] G. K. Tsolis, D. K. Tsolis & T. S. Papatheodorou, An Advanced Digital Image Repository and an XML-based application for Intellectual Property Protection and Management of Digital Objects. *Proc. WebNet 2001*. Orlando, Florida, USA, 2001, 1243-1248.

[13] IBM DB2 Image Extenders, Query by Image Content (QBIC), http://wwwqbic.almaden.ibm.com/

[14] G. K. Tsolis, D. K. Tsolis & T. S. Papatheodorou, A watermarking environment and a metadata digital image repository for the protection and management of digital images of the hellenic cultural heritage. *Proc. IEEE International Conference on Image Processing 2001*, Thessaloniki, Greece, 2001, 566-569.

[15] V. Fotopoulos, A. N. Skodras, “A Subband DCT Approach to Image Watermarking”, Proc. X European Signal Processing Conference (EUSIPCO-2000), Tampere, Finland, 5-8 Sept. 2000.

[16] The Multimedia Coding and Watermarking Group, http://www.mcwg.gr

[17] D. K. Tsolis, G. K. Tsolis, E. G. Karatzas, D. A. Koutsomitropoulos & T. S. Papatheodorou, An Electronic Sales Infrastructure for the Exploitation of Digital Cultural Heritage and Copyright Protection of Digital Images. *SSGRR 2002 International Conference titled “Advances in Infrastructure for e-Business, e-Education, e-Science, and e-Medicine on the Internet”* in L'Aquila, Italy, ISBN: 88-85280-62-5.

[18] D. K. Tsolis, S. N. Nikolopoulos, V. Fotopoulos, G. K. Tsolis, E. G. Karatzas, A. N. Skodras & T. S. Papatheodorou, A Robust Watermarking Method Supported by an Image Registration Mechanism for Securing Digital Image Libraries. *EVA 2004, Electronic Imaging & the Visual Arts*, Florence, Italy, 2004.

[19] G. K. Tsolis, N. V. Kazantzi & T. S. Papatheodorou, Increasing Long-Term Preservation of Cultural Information Systems by Using XML Web Services. *10th Panhellenic Conference on Informatics (PCI'2005)*, Volos, Greece, 11-13 November 2005, submitted.

[20] The Handle System, http://www.handle.net/

[21] The Digital Object Identifier System, http://www.doi.org/

[22] SOAP Messages with Attachments, W3C Note 11 Dec. 2000, http://www.w3.org/TR/SOAP-attachments

[23] Proposed Infoset Addendum to SOAP Messages with Attachments, Version 0.61 Draft, 1 April 2003, http://www.gotdotnet.com/team/jeffsch/paswa/paswa61.html

[24] W3C, XML Protocol Working Group, http://www.w3.org/2000/xp/Group/

[25] SOAP Message Transmission Optimization Mechanism, W3C Recommendation 25 January 2005, http://www.w3.org/TR/2005/REC-soap12-mtom-20050125/

[26] XML-binary Optimized Packaging, W3C Recommendation 25 January 2005, http://www.w3.org/TR/2005/REC-xop10-20050125/

[27] IETF, Network Working Group, A UUID URN Namespace, Internet-Draft, Dec. 2004, http://www.ietf.org/internet-drafts/draft-mealling-uuid-urn-5.txt