Journal of Universal Computer Science, vol. 13, no. 4 (2007), 543-571
submitted: 2/1/06, accepted: 27/4/07, appeared: 28/4/07 © *J.UCS*

A Cultural Information System Providing e-commerce Web Services, Digital Rights Management and Copyright Protection

Dimitrios K. Tsolis
(Computer Engineering and Informatics Department, University of Patras, Greece
dkt@hpclab.ceid.upatras.gr)

Spyros Sioutas
(Spyros Sioutas, Department of Informatics, Ionian University, Greece
sioutas@ionio.gr)

Lambros Drossos
(Technological Institute of Messolongi, Department of Applied Informatics in Administration and Economics, Greece
ldrossos@teimes.gr)

Theodore S. Papatheodorou
(Computer Engineering and Informatics Department, University of Patras, Greece
tsp@hpclab.ceid.upatras.gr)

Abstract: The issue addressed in this paper focuses on the design and implementation of an advanced information system for Cultural Organizations, which serves as a platform for the exploitation through e-Commerce web services and, in parallel, the protection of copyright and digital rights management of the cultural content. The main components of the information system are: (a) Digital Image Library, which offers specialized services, (b) copyright protection and digital rights management of digitized material and (c) the E-Commerce web services, supported by advanced technologies, for the proper exploitation of the digital cultural content. The work described in this contribution focuses on digitized material of Cultural Heritage and is deployed at several cultural organizations.

Keywords: integrated information system, copyright protection, digital rights management, watermarking, e-commerce applications, usable user interfaces, web services, metadata, licensing
Categories: H.4.0, H.5.0, H.5.1

1 Introduction

The great value of cultural content is by now well recognized as it relates directly not only to culture in general but to important and vast markets, mainly Education, Tourism, Entertainment and Research. The cultural organizations are currently trying to adopt to new technologies mainly towards the direction of creating and providing wide access to digital cultural content aiming at having a key role to the digital content industry and to increase the actual visitors . Nevertheless, wide access and delivery of valuable content through information systems raise several critical issues,

pertaining to management, protection and exploitation of digitized cultural content [House, 98]. These include at first the critical problem of IPR (Intellectual Property Rights), protection and the unauthorized use and exploitation of digital data ("electronic theft") and secondly the creation and use of appropriate e-commerce web services which take into account the special characteristics of cultural content. Besides economical and other implications, such problems create considerable scepticism to cultural organizations and individual content owners. As a result content of great educational and economical value is often held secret and private.

2 From the Objective to Requirements – Cultural Organizations

Requirements are used in judging a system's overall design, methods and implementation. They provide a clear and analytical picture of the objectives and if met they prove of one system's effectiveness. Moreover one could draw value from the requirement formulation process especially if similar systems are going to be deployed to new case studies. The current section is presenting the general objective of the system, the requirements and their formulation method.

2.1 Objective Analysis

The general objective is:

"Cultural organizations, museums, libraries and archives are currently trying to adopt to the Information and Communication Technologies mainly towards four directions, a) the improvement of their internal work-flows through digitization and advanced content management, b) digital rights management and copyright protection for the produced cultural content c) provision of wide access to the digital cultural content via the Internet aiming at the increase of the actual visitors and d) the direct commercial exploitation of the digital cultural content using e-commerce technologies and services. The objective is to design and implement a system which supports these organizations to achieve the aforementioned goals".

The need of designing and implementing such an information system is becoming important for cultural organizations worldwide, mostly due to the following reasons:

1. Advances in technology have improved the ability to reproduce, distribute, manage and publish information [Randall, 01]. Reproduction costs are much lower for both right holders (content owners) and infringers, and digital copies are perfect replicas. The average computer owner today can easily do the kind and the extent of copying that would have required a significant investment a few years ago.
2. The computer networks have changed the economics of distribution. Networks enable sending multimedia content worldwide, cheaply and at a high speed. As a consequence, it is easier and less expensive both for a rights holder to distribute a work and for an individual to make and distribute unauthorized copies. Finally, the World Wide Web has altered at a fundamental way the publication of information, allowing everyone to be a publisher with worldwide reach. The variety of documents and multimedia content of all sorts on the Web demonstrate that many people worldwide are making use of that capability. This is affecting the Cultural Sector too.

3. The information structure has been integrated into everyday life, affecting directly the intellectual property legislation [CSTB, 99]. Today, actions that can be taken casually by the average citizen – downloading files, forwarding information found on the Web – can at times be violations of intellectual property laws. Others as such as making copies of information for private use may require difficult interpretation of the law simply to determine their legality. Consequently, individuals in their daily lives have the capability and the opportunity to access and copy vast amounts of digital information, yet lack a clear picture of what is acceptable or legal. On the other hand, the necessary amendments of the copyright legislation in several cases do not cope with the entirety of the problem, resulting in certain legislative weaknesses.
4. The available e-commerce applications and information systems, mainly based on the need of interoperability and platform independence, do not take into account the special characteristics of the cultural content and the high level requirements of the cultural organizations for appropriate manipulation and use of this content. These requirements do not only affect to web and multimedia presentation but also to appropriate and scientific documentation, special licensing modes, special access and search services etc. A cultural organization demands the cultural content to be considered as a priceless scientific resource which needs protection and special care.

The majority of information systems in the Cultural Heritage sector are mainly concentrated to the commercial exploitation of digital images. At the same time, some prevailing examples of copyright infringement especially for digital images of Cultural Heritage could be viewed in many corporate web sites, where the unauthorized commercial exploitation of digital images is conducted in an everyday basis. This improper exploitation of digital images, through these information systems, is proving the lack of awareness of copyright laws for both content holders and content users.

2.2 Formulation of Requirements Method and Process

The design and implementation of the integrated information system was based on a formulation of requirements process which used the "spiral" model of development. The "spiral" model allows successful software engineering while in parallel verifies constantly if the needs of the organizations are being met. Based on the model the following steps were repeating constantly till the final system deployment:

1. Problem analysis. The key entities involved were defined, as well as their needs and relations between them. For every entity the user requirements and technical specifications were analyzed and a diagnosis of the necessary systems, applications and services was completed. The result of this important step is the entity – relations diagram which depicts the system's architecture, parameters and data flow.
    - Simplification. Due to the large complexity of the issue methods for the problem simplification were introduced.
2. Design of the system based on the problem analysis step and on the defined requirements.
3. Implementation of subsystems and integration.

4. Evaluation of the produced applications, services, user interfaces etc.

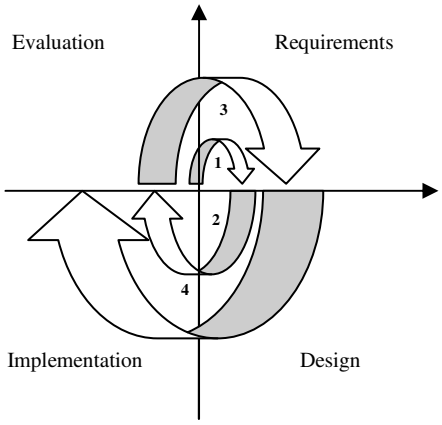

Figure 1: The "Spiral" Model

2.3 Entities & Requirements

The problem analysis step has produced a set of entities which play an important role to the overall system's implementation as well as their requirements. These entities and the correspondent requirements are summarized in the following table1.

Entity	Role	Requirements
Cultural Organization	Content and copyright owner, wishes to digitize, promote and exploit the digital cultural content	Means of providing content to the Content Provider entity. Demands: - Digitization services based on international technical standards. - Content management tools (metadata editing etc). - Copyright protection for the digital content. - Digital Rights Management (e.g. setting restrictions of use). - Fee and profit collection.
Content Provider	Creates the circumstances for the further exploitation of the content. Digitization process is included.	- Digitizes content based on technical standards. - Implements and owns the Digital Image Library. - Preserves the digital content in the long term. - Identifies the content uniquely and its content owner in cooperation with the Unique ID Provider. - Protects and manages the copyright of the digital content (e.g. uses watermarking techniques, encryption etc.). - Provides the Cultural Organization with user interfaces for content and digital rights management. - Provides the Content Distributor with digital

		content especially adjusted for distribution via the Web and e-Ecommerce applications. - Provides with pricing policies.
Digital Image Library	Repository of Digital Content. Manages digital content and its metadata, (descriptive, technical and metadata about the Intellectual Property Rights)	- Serves as a platform for content management, protection and long-term preservation. - Supports distributed content management. - Facilitates security against attacks. - Implements watermarking algorithms for the copyright protection of the digital content. - Implements Query by Image Content algorithms for advanced image search based on color, patterns etc. - Supports the Content Provider entity with usable tools and user interfaces.
Unique ID Provider	Provides unique ids for the persistent identification of content.	- Assigns a unique identification number to every digital object. - Assigns a unique identification number to every content and copyright owner (the Cultural Organizations). - Implements international schemata of identification (e.g. Digital Object Identifiers, ISBN, etc.). - Sends unique ids to the Content Provider when requested.
Content Distributor	Distributes the digital content through Web and e-Commerce applications	- Acquires watermarked digital content from the Content Provider. - Provides the Buyer with e-Commerce web services for the digital content. - Authenticates the Buyer. - Implements e-payment and e-banking applications. - Preserves log files for the transactions which include the unique ids of organizations, digital content and buyers. - Controls and traces the digital content usage from the buyers.
Buyer	Acquires digital content	- Demands usable services of a high performance and quality from the Content Distributor. - Acquires the digital content through e-Commerce web services for private or other use. - Demands secure transactions. - Is aware of the copyright status of the digital content acquired. - Fulfills financial transactions. - Uses advanced search services for digital content, electronic catalogs, baskets, personalization services etc.
Bank	Fulfills financial transactions through e-banking applications.	- Provides the Content Distributor entity with e-payment and e-banking applications.

Table 1: Entities, Roles and Requirements

2.4 The Entity – Relations Diagram & Technical Specifications

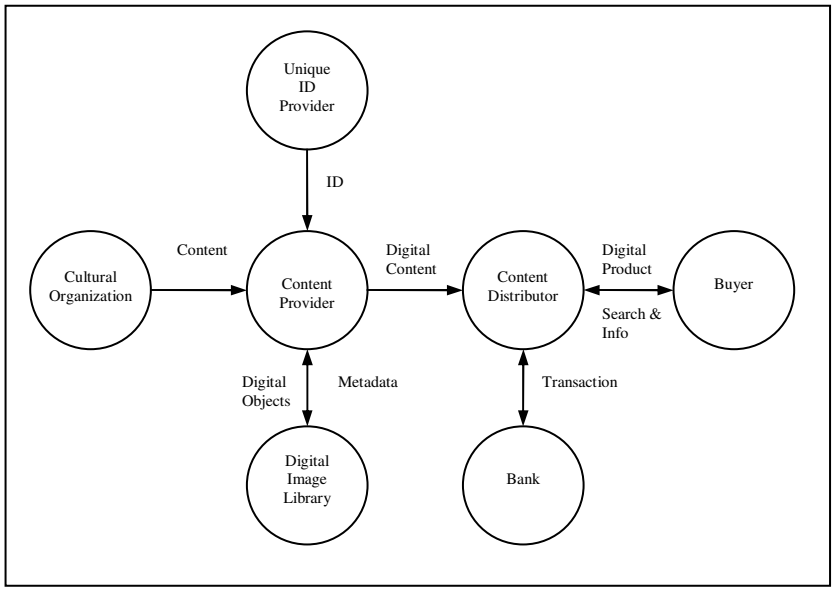

Figure 2: ER Diagram

The above ER diagram points out that the issue is complex and several key entities have to produce, interact, protect, manage, distribute and transact so as valuable cultural content to be exploited while at the same time its copyright is being protected.

Based on the requirements and the communication needs we can define the technical specifications for every entity. A summary of the most important technical specifications is presented in the next table 2.

2.5 Simplification

The above analysis has produced significant results regarding the functional requirements and technical specifications which the information system should be based upon. In the framework of an implementation for case study and especially if many entities do not exist in a real-world case then a simplification of the problem is required. Simplification is achieved through the union of several entities in one entity in the above ER diagram. The new entity introduced is the Trusted Third Party (see table 3) which is concentrating all requirements and specifications of the entities which it has substituted. Simplification does not apply to the technological solutions, standards and methods used for the implementation of the information system. On the contrary, the tools, systems, databases are implemented in accordance with the needs and specifications as stated above.

Entity	Technical Specifications
Cultural Organization	- User interfaces and tools provided by other entities for the management of the digital content and its metadata.
Content Provider	- Implementation of the Digital Image Library. - User interfaces and standards for digitization. - Tools for metadata management, including the intellectual property rights management information. - Watermarking algorithms for copyright protection. - Interoperability of tools and UIs.
Digital Image Library	- Search tools and engines. - Query by Image content capabilities. - Security and interoperability. - High Performance and data mining.
Unique ID Provider	- Unique identification schema and algorithm. - User interfaces for the production and distribution of unique ids to interested parties.
Content Distributor	- E-Commerce applications (electronic catalogs, basket application, e-payments etc.). - Electronic licensing. - Transactions Database. - Web services for content search and acquisition.
Buyer	- User interfaces and tools provided by other entities especially focusing on access to the content and e-commerce.
Bank	- E-payment and e-banking applications.

Table 2: Technical Specifications

Old Entity	New Entity
Cultural Organization	Cultural Organization
Content Provider	Trusted Third Party
Digital Image Library	Trusted Third Party
Unique ID Provider	Trusted Third Party
Content Distributor	Trusted Third Party
Buyer	Buyer
Bank	Bank

Table 3: Simplification

After the simplification the next ER diagram is produced.

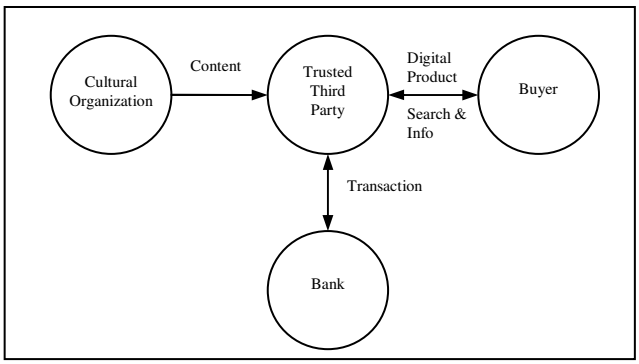

Figure 3: The Simplified ER Diagram

2.6 Conclusion

In accordance with the problem analysis step we have defined all the key entities, their requirements and technical specifications which play an important role for the design and implementation of the integrated information system. The Trusted Third Party is the entity which embodies all the subsystems, applications and tools which the information system implements. The rest of the entities use the tools and user interfaces which the Trusted Third Party provides. The next section presents the design and implementation of the integrated cultural information system based on the defined requirements.

3 Information System's Development

In this section the information system's design and development is being presented in detail. During the information system's implementation, specific technological solutions were applied and exhaustively tested (e.g. watermarking) so as the technical and functional requirements to be fulfilled.

3.1 The Information System – a Design Overview

The cultural information system (see figure 4) is designed based on the requirements and technical specifications which were defined in the previous section. The system:

1. Provides an appropriate infrastructure for the production, protection and distribution of digital cultural content, especially focusing on digital images and its special characteristics.
2. Implements a Digital Image Library and the accompanying search, access and management services.
    a. Provides cultural organizations with user interfaces and tools for digitization, management and long term preservation of the cultural digital content and its metadata.

3. Protects the copyright of the digital images though robust watermarking techniques. Multi-bit watermarks are embedded to the digital images which are commercially exploited and delivered to the buyers.
4. Supports the digital rights management process for the cultural content and for the transactions taking place.
5. Provides an effective mechanism for tracking down improper use of digital images which are owned by the cultural organization.
6. E-commerce services and applications implemented range from typical e-commerce applications (electronic catalogs and shopping kart) to advanced services such as searching for images based on the image content and detection of unauthorized content use.

The general system's architecture and its main components are the following:

- The Digital Image Library.
- The copyright protection subsystem, which protects digital content with watermarking techniques and provides for digital rights management.
- The E-Commerce applications.

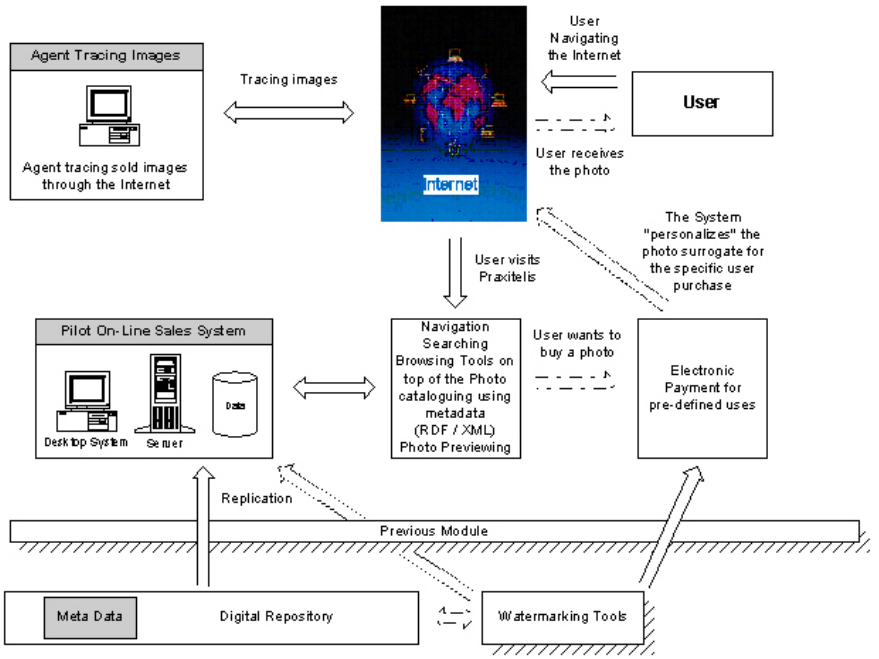

Figure 4: Information System's Architecture

3.2 Digital Image Library

The design and implementation of the Digital Image Library is required for further development of the information system. The Digital Image Library is consisting of the Image Repository and the Metadata sets which are described in detail.

3.2.1 Image Repository

The efficient management of digital images is based on an advanced database system. The design and development of the Digital Image Library for this platform is an important and quite complicated task.

The Digital Image Library is designed and developed in accordance with metadata sets described in the following paragraph. The metadata sets are incorporated through tables, fields, triggers and views in the Database. The specific tables and fields, which are used for the image library, were selected on the basis of the next requirements:

- Custom metadata of the cultural organization.
- International metadata for the dissemination of culture.
- The international standards for describing, characterizing and identifying digital images.
- The international standards for managing and storing in the long-term data produced by the e-commerce transactions.
- The international standards for managing and protecting the Intellectual Property Rights.

The software instruments selected for the development of the Digital Image Library are the IBM DB2 Universal Database, with the assistance of the IBM DB2 XML and AIV Extenders. The specific system provides advanced services for searching and retrieving digital images according to their actual content. For example it supports digital image retrieval using similarity criteria like colour, histogram, shape etc. In this case the user can use a colour specification or even the image itself as a query to the image library.

3.2.2 Metadata

The need for adopting international metadata standards is profound, especially for applications aiming at cultural content exchange. The DIG 35 Specification "Metadata for Digital Images", Version 1.1 [DIG35, 00] holds a very important role in the selection of fields and tables, regarding the digital images metadata. This metadata standard is already being widely used in simple end-user devices and even to worldwide networks. The database structure has also a special focus on metadata for the Intellectual Property Rights management. In particular, these sets were divided in six major sectors:

- Technical metadata. Technical metadata are related to the image parameters, such as the image format, image size, compression method, and colour information.
- Image creation metadata. The image creation metadata include general information concerning the creation of the digital image. This information

involves the time and date of creation, the name of the creator, and information about the capturing device.

- History metadata. The history metadata are necessary so as to identify and record the processing steps that might have been applied to a digital surrogate. This may help to avoid any further processing steps, and to identify independent objects in a composition of digital pictures. This set of metadata contains information on whether or not a digital image is cropped, rotated, retouched, or suffered a colour adjustment.
- Content description metadata. The content description metadata contain descriptive information about the location, the capture time and date, etc.
- E-commerce related metadata related to the transactions taken place by the Internet user with the information system. These data include all the necessary information which describes a transaction such as, transaction ids, user profiling data, dates, amounts, special terms and conditions etc.
- IPR related metadata. This important metadata set is related with the intellectual property rights and involves information about the copyright, the image creator and rights holder, the restriction of use and contact points.

Amongst the various metadata standardization initiatives, Dublin Core (DC) [Dublin Core, 00] has gained significant visibility and respect. Dublin Core is a metadata standard fully applied to cultural heritage and supports the diversity, convergence and interoperability of digital cultural objects. The basic Dublin Core data model is a simple content description model, defined by its 15 elements. The need for incorporating the DC elements in the digital image library is significant mainly because many cultural organizations are already using the DC model and this will support the wider interoperability of the system.

The most common practice of efficiently combining two or more metadata standards is mapping. Mapping between metadata formats requires the creation of a mapping table. The advantage is that this mapping makes it possible for both simple DC-based as well as more detailed DIG 35 (Digital Imaging Group) content-based search to be done. The main difficulty of mapping DIG 35 to DC is the difference of granularity. The DC element set has only 15 elements and on the other hand DIG 35 is a highly structured and detailed metadata set. The mapping table of the two standards was developed. In addition a mapping table was developed between the custom made metadata set of the cultural organization and the Dig 35 correspondent set. The final result was an extended metadata set with a specialized structure capable of producing the metadata information according to the desired level of detail.

3.2.3 User Interfaces and Tools for Digital Content Management

The Digital Image Library provides also user interfaces and tools which assist cultural organization to digitize, store and manage digital content and the aforementioned accompanying metadata. The tools are implemented using web services technologies and taking into account international usability standards and guidelines.

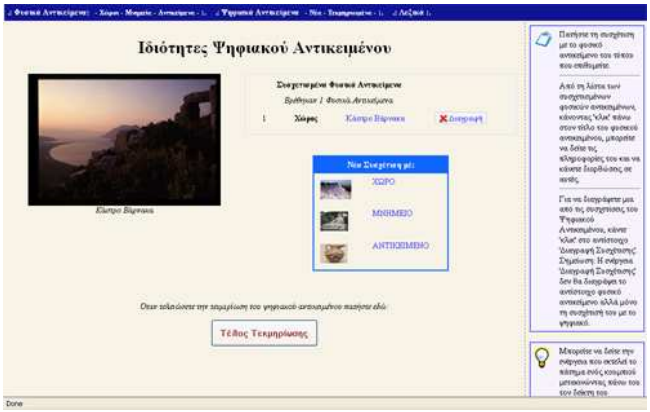

Figure 5: Tool for Digitization and Metadata Management

3.3 Copyright Protection Subsystem

The copyright protection subsystem is an intermediate layer between the e-commerce applications and the digital image library. Its main function is to protect the copyright of the digital images stored and exploited by the information system. Using a simplified view of the subsystem, it is considered as a black box which takes the original digital images as an input and produces the watermarked images. The whole process is automated and whenever a new original image is stored to the digital library the watermarked surrogates are being created which carry the copyright owner id and other information used for copy control, digital signature, unauthorized use tracking and transaction management.

3.3.1 Watermarking Algorithm

Watermarking principles are mainly used whenever copyright protection of digital content is required and the cover-data is available to parties who are aware of the existence of the hidden data and may have an interest removing it [Cox, 02]. In this framework the most popular and demanding application of watermarking is to give proof of ownership of digital data by embedding copyright statements. For this kind of application the embedded information should be robust against manipulations that may attempt to remove it. Many watermarking schemes show weaknesses in a number of attacks and specifically those causing desynchronization which is a very efficient tool against most marking techniques [Katzenbeisser, 00]. This leads to the suggestion that detection, rather than embedding, is the core problem of digital watermarking [Wayner, 02].

According to the above the first most important step towards the implementation of the watermarking algorithm is the selection and evaluation of the watermarking method. The method chosen is mainly based on the further elaboration of the MCWG (The Multimedia Coding and Watermarking Group, http://www.mcwg.gr) watermarking tool, focusing on constructing a more efficient detection mechanism,

resulting to a more robust watermarking technique. The core of the MCWG tool is a transform domain technique that is based on the use of the Subband DCT transform [Fotopoulos, 00]. The marking formula is the same well known multiplicative rule used in the large majority of the existing literature. The tool has performed positively in the past in a large variety of attacks, including those that an application like Ulysses would require. It did not though provide support for geometrical attacks. Thus some improvements were considered necessary.

There were two main directions for improvement. The first one was to maximize the detector's performance. As known from the literature, in the case of such systems, the detector's output is a function of two parameters that have to do with the selection of the marked coefficients vector: size and length. An adaptive algorithm has been designed and included into the system that fine-tunes the selection of these parameters [Fotopoulos, 02]. The results of this improvement are clearly beneficial to the system. The other improvement direction has to do with the geometric attacks problem. A supplement to the system was created based on the notion of the centre of mass. This familiar term from the classical physics theory has been introduced in the image domain by carefully selecting two different logical representations of the image array [Skodras, 02]. Extensive tests performed on images that were rotated, scaled and changed by means of aspect ratio, have proved that those changes can be satisfactory restored, thus providing a positive response from the re-synchronized system. This extension was also included into the original watermarking method.

The proposed watermarking method was tested particularly with digital images provided by cultural organizations all over Greece and fine-tuned in accordance with the produced results. In addition, certain actions were taken for the further development of the method so as to incorporate multi-file support, monochrome and colour images and multidimensional digital images.

3.3.2 Integration Strategy

By integration strategy we mean the methodology followed and the decisions made during the incorporation of the watermark embedding and detection procedure to the information system. The strategy adopted considers the watermarking method that was previously described, as a "black box".

The technical requirement in favour of this implementation is the re-usable format (Software Development Kit and Dynamic Link Libraries) provided for the watermarking method, appropriate for a wide variety of software developments. The watermarking is considered as a generic class, with specific attributes, functions, arguments, parameters and return values. The advantage of this strategy is that the watermarking method is independent from the development of the basic infrastructure (e.g. the Digital Image Library) and the user interfaces.

3.3.3 Implementation

The API (Application Protocol Interface) supporting the Watermarking component is consisting of two significant methods. A method called "embed" is responsible for the watermark casting and the corresponding method called "detect" is capable of detecting the watermark, provided of course that the image is indeed watermarked. The specified API proved to be very handy during the development of the information

system, mainly because its structure as an independent DLL (Dynamic Link Library) component, universally applicable by just referencing the corresponding class.

Embedding

One of the most important aspects of the system is its ability to preprocess the digital image and preserve some valuable supplementary information in the database. The association between the digital image and the supplementary information is accomplished through an integer value called imageid, acting as a foreign key for the supplementary information database table. The watermarking algorithm has the responsibility of connecting to the database and storing the supplementary information, acquired from the image preprocessing, always associated with the actual image through the imageid. The best way to demonstrate how the embedding method works is to present the next figure (Fig. 6):

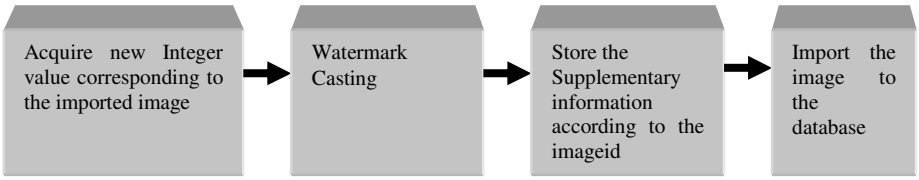

Figure 6: Watermark Embedding Process

The special reference on this particular system function is justified by the significance of the supplementary information to the process of image registration and consequently, robustness against geometrical attacks during the detection process.

Detection

The main weakness of the majority of the watermarking detection mechanisms is there inability to counter the attacks involving the desynchronization of the detector. Geometrical attacks are a small but important subset of this kind of attacks. The best countermeasure against the desychronization attacks is definitely the notion of "image registration".

Image registration is the procedure of finding the exact image instance during the watermark casting. Finding the right instance and providing it to the detector helps the mechanism to achieve synchronization and detect the watermark. However, finding the appropriate instance, without further information available, is not a straightforward task. In the trivial case, the necessary additional information is the original image. This is mainly the reason why the non blind detectors (the original image is in the detector's disposal) perform better than blind detectors (only the watermarked image is available).

The presence of a digital library and specifically of a DBMS (Database Management System) with advanced search capabilities provided the basis for a more efficient detection mechanism through the cooperation of the image database with the watermarking technique. The detector is initially provided with a digital image in order to decide whether it is watermarked or not. If the first attempt to find the watermark is unsuccessful the detector must try to register the image hoping to find

its synchronization and detect the watermark. At this point the original image is essential for the detector. Although, our system has access to a large number of digital images stored in the database, it is impossible to decide which image corresponds to the original copy of the image in the detector. This is where the advanced search capabilities take over and in particular the Image Extender of DB2 Universal Database Management System.

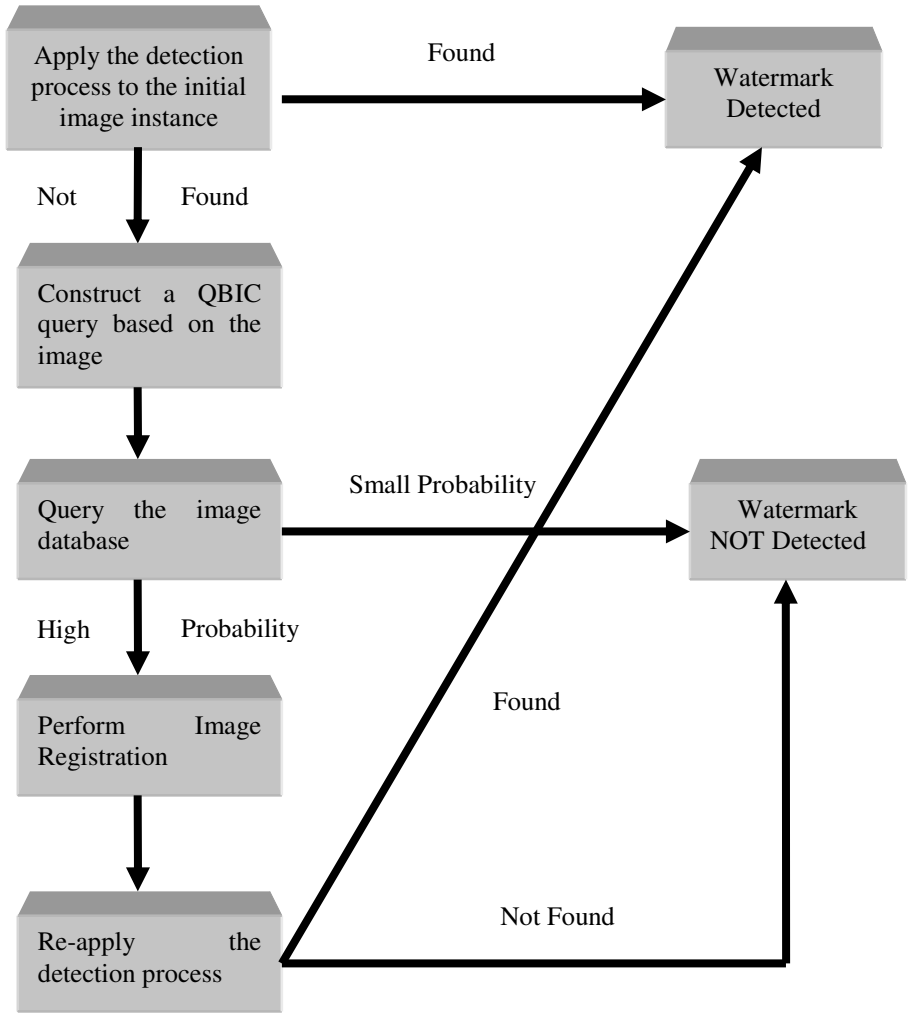

Figure 7: Watermark Detection Process

DB2 Image extender is a tool that allows the storage of and query of image data with the same convenience as with traditional ones. The prominent feature of Image extenders is the functionality of querying images, based on related business data or by image attributes. The entire image database search can be based on data that the user

maintains, such as name, number and description, or by data that the DB2 Image Extender maintains, such as the format of the image, its distribution of colours, the illustrated shapes etc. The QBIC (Query By Image Content) queries is the solution to the problem of selecting the correct original image.

Just before the initialisation of the detection process a QBIC query is constructed based on the image under examination. The query response is a similarity measure reporting the probability that the original copy of the image under examination is the one indicated by the image extender. If the probability is high enough, the detector continues the detection procedure having access not only to the original image but also to the supplementary information derived from the image pre-processing. The association between the original image and the supplementary information is conducted through an integer value returned by the QBIC query, which corresponds to the foreign key of the corresponding database table. Figure 7 demonstrates the possible scenarios.

3.3.4 Evaluation and Robustness

In this section we present the experimental results concerning the evaluation and robustness of the watermarking algorithm. Robustness is the most highly desired feature of a watermarking algorithm especially if the application demands copyright protection, and persistent owner identification. In addition the image distortion and false positive parameters are being evaluated.

In our experiments the metric selected for evaluating the image distortion introduced by the multi-bit watermark casting is PSNR (Pick Signal to Noise Ration). Although PSNR is definitely insufficient for modeling the complexity of the human visual system is by all means an effective metric for measuring image similarity. The following table 4 demonstrates the results.

Image Database				
Original Images				
Chariot	Horse	Mask	Plate	Scene
Watermarked Images				
water_chariot	water_horse	water_mask	water_plate	water_scene
PSNR	**PSNR**	**PSNR**	**PSNR**	**PSNR**
66.65	69.52	64.90	68.36	65.99

Table 4: Image Database – PSNR

Regarding the fact that in most cases a PSNR value above 40 decibel is satisfactory the derived results can be consider to meet the image quality requirements.

Keys					**Chariot**				
50	**100**	**200**	**350**	**700**	1	1	1	1	1
22715	12662	25325	27935	23102	0	0	0	0	0
22430	23392	25316	28203	2170	0	0	0	0	0
16275	22561	2367	21228	32468	0	0	0	0	0
21417	20718	19320	17222	12328	0	0	0	0	0
4906	6314	9131	13355	23212	0	0	0	0	0
9000	1073	17987	26975	4255	0	0	0	0	0
3863	24449	86	29076	9340	0	0	0	0	0
26227	32712	12916	32372	12235	0	0	0	0	0
20017	27912	10934	1851	24347	0	0	0	0	0
21604	2031	28420	2467	29292	0	0	0	0	0
28180	11332	10403	25394	5760	0	0	0	0	0
940	7595	20906	8104	21924	0	0	0	0	0
13042	20424	2421	24568	10709	0	0	0	0	0
26566	10606	11456	29111	15696	0	0	0	0	0
20934	20780	20474	20015	18943	0	0	0	0	0

Horse					**Mask**					**Plate**				
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Table 5: Experimental Results

Casting multiple zero-bit watermarks onto the same coefficient area raises the probability of causing abnormal fluctuation of the detector's false positive probability. In order to confirm that no such case is true, we used 5 different watermarks applied to a sample of 5 images for approximating the false positive probability. The watermarks were generated from 5 different integer numbers, also responsible for the generation of the vector containing the rest integer values required by the embedding mechanism. Every image was watermarked using each of this numbers as a watermark key while afterwards the detector was tested for possible false positive response with every number contained in the produced vector. That is, an image watermarked with the number *K1* as a watermark key was examined by the detector 15 more times using as primary keys the numbers of the vector produced by the random generator with *K1* as a seed. The reason for examining only this small subset of numbers instead of a large random set is that this numbers hold highest probability of causing a false positive, due to the statistical dependence introduced to the correlation function. Table 5 demonstrates the experimental results:

The table above indicates only one false positive response under the "Plate" image. Thus, the derived conclusions justify our hypothesis about the false positive probability of the detector which remains in relatively low values, thanks to the statistical independence introduced by the embedding start point shifting.

The watermark's robustness depends on the efficiency of Image Extenders which were analysed in the section above. The watermarks robustness has been extensively tested. The average score of the watermarking robustness against various types of attacks is 94% which is a very efficient result for the type of application under consideration. The results are briefly analyzed below (table 6).

Type of Attack	**Average Score**
Convolution and Median Filters	100%
Jpeg Compression	90%
Scaling	100%
Cropping	95%
Shearing	93%
Rotation – Crop	97,5%
Rotation – Crop – Scale	79%
Linear Transformations	100%
Aspect Ratio	100%
Row and Column Removal	100%
Geometric Distortion	80%

Table 6: Watermarking Robustness – Various Attacks

Closing the performance evaluation it is worth mentioning the results derived from the print-scan or digital to analog attack. A small number of images after they have been compressed with a jpeg algorithm, they were printed to plain paper. Using a flatbed scanner the images were scanned back to their digital form and delivered to the watermark detector. The detector output is presented in the following table 7.

Image Format	Image Compression	Print Quality	Result
Tiff	None	Best	Detected
Tiff	None	Normal	Detected
Jpeg	Medium Compression High Quality	Best	Detected
Jpeg	Medium Compression High Quality	Normal	Detected
Jpeg	Medium Compression Medium Quality	Best	Detected
Jpeg	Medium Compression Medium Quality	Normal	Missed

Table 7: Print – Scan or Digital Analog Attack

The watermarking robustness, taking into account its application to the copyright protection subsystem of the integrated cultural information system, is more than adequate. The JPEG compression, crop and rotation attacks which are the more common types of attack for applications which distribute digital cultural content through the web is being dealt effectively.

3.3.5 Copyright Protection with the Watermarking Algorithm

Securing the digital content is of a great concern for the proposed information system.

The reasonable approach would be to adopt a strategy of securing the content by guarding it. By guarding we mean the establishment of complicated mechanisms difficult to overcome without proper authorization. Encryption and user authentication are some of the techniques used to forbid access of the digital content. Nevertheless, in circumstances where the adversary succeeds in circumventing the guarding mechanisms, the content is totally unprotected and vulnerable to illegal manipulation. On the contrary, the security provided by watermarking techniques relies on the content itself. Thus, protection continues even after the adversary has managed to obtain the Digital Image Library's content. In the proposed information system the watermarking algorithm, which was described, is used to facilitate important security tasks over the content. The main tasks are copyright protection by copy control and owner identification, digital signature and transaction tracking.

The enforcement of the aforementioned security measures is based on the notion of the watermark key. The usage and administration of the watermark key is what differentiate the form of security applied, resulting in different cases. The basic principle of every watermarking scheme is that in order for the detection to be successful, the key used by the detector should match the one used by the embedding mechanism. The selection of any different key must cause the detector to fail. An important detail concerning the detector's output is the value returned. In the trivial case the returned value is a simple indication deciding for the watermark's existence (Yes / No Boolean response). Under different circumstances it is useful for the detector to return an integer value. This value will serve as a pointer to a useful piece of information regarding the digital object. The watermark key administration, which

is implemented into the information system, will be described in the following scenarios.

The copyright protection scenario is the most important one. This is based on two cases, the owner identification and copy control.

In the owner identification case the image owner casts a watermark to the image using a private key. The scenario begins with a dispute between the image owner and an adversary. They both claim ownership of the digital image and they are both asked to give proof of their assertion. The copyright owner with the correct key value in his disposal can prove his assertion by feeding the key to the detector and confirming the watermark's presence. On the contrary, the fake claimer is unable to prove his ownership since his not aware of the correct key value.

Copy control is performed in a quite similar way. The Digital Image Library administrator watermarks every digital image of the library with a constant well known key, before the content distribution takes place. This key is the declaration of the "never copy" instruction. Additionally, compliant devices are equipped with the detector of the watermarking mechanism along with the well know key. Upon the arrival of the watermarked digital image to the compliant device, the detector performs a watermarking detection. In case of positive response the compliant device understands the "never copy" instruction and forbids the replication of the image. This example illustrates the necessity of the device requirement to carry an incorporated detection mechanism, which is a quite ambitious expectation since the watermark detector essentially degrades the device functionality. Only law enforcement will make the above scenario appear as a realistic situation.

Consequently, the requirements of the copyright protection application of the digital library's security, are restricted to the casting of two watermarks, the first using the copyright owner's private key declaring his ownership, and the second using the well know constant key declaring the "never copy" instruction.

The next scenario concerns the digital signature security application and describes how the database administrator can discover an intruder trying to populate the database with malicious data. In digital image libraries of maximum importance and security the group of people authorized to contribute information is limited and well defined. The library administrator responsible for the validity of the content should maintain a record correlating a watermark key with the contributor's identification information. These keys are secretly distributed to the trusted party so as each authorized contributor should obtain a unique private key. When someone wishes to store information in the digital library, he sends the information along with his identification to the library administrator, only after he had watermarked the image using his private key. The image library administrator looks through his record and obtains the key related to the identity information provided by the unknown contributor. In case of positive response the administrator proceeds on storing the information to the library, in any other case the data are thrown away. In this way only the authorized group of people is permitted to contribute information to the digital library. The requirements of the digital signature security application are only one watermark per digital image and a Boolean response by the detector.

Finally the last scenario illustrates the transaction tracking security application, where the head of digital image library's security has the duty of tracking and capturing the information leak. As in the previous case this security application is

applied in situations where the digital library content is very important and confidential. Once again the security administrator needs to maintain a record with numbers and names. The difference from the previous application is that now, no identity information is provided with the digital image, thus the security administrator has no way of knowing the correct key for the detection. The solution to this problem is the combination of a constant well-known key for the watermark casting, with a numerical detector's response allowing the correlation of the digital image with its original source. Just before the security administrator distributes the information to the authorized recipients, for example when a buyer is purchasing digital images from the information system, a watermark is embedded using the constant key. If a confidential image or document is found in the wrong hands, the security administrator can initialize the watermark detection process using always the constant key. The detector will result in a number indicating the original source of the image, likely responsible for the leak.

Summarizing the key requirements for the security purposes, every digital image included in the Digital Image Library should contain a key for the owner identification application, a key for the copy control and a key representing the digital signature, all combined with a Boolean detector response. The last key requires a numerical output by the detector and refers to the transaction tracking application of the information system.

The proposed information system raises two basic issues concerning the watermarking technique. The first one is related with the data payload embedded into the image and the second with the detector ability to detect multiple watermarks. Data payload refers to the number of bits a watermark encodes within a unit of time or within a digital object. For a photograph, the data payload would refer to the number of bits encoded within the image.

The drawback in encoding a substantial number of bits into the image is the distortion introduced comparing to the original image. In our case the proposed watermark key administration requires three zero-bit watermarks (the detector's output is either one or zero) and one 14-bit watermark encoding 16384 different fingerprints. Mainly due to the inherent resilience of the DCT-domain technique [Barni, 98] the distortion introduced by the encoding of 17 bits is imperceptible as indicated by the calculated PSNR (Peak signal to noise ratio) value presented in the evaluation paragraph. By multiple watermarks we refer to the detector's potential of detecting a small amount of different watermarks into the same image without confusion. As in the previous case, in the proposed information system the watermark algorithm's inherent capability solves the problem by maximizing the detector's output sufficiently above the selected threshold when the key is valid and minimizing it below the threshold in case of an irrelevant key value. The following graph (Fig. 8) demonstrates this feature.

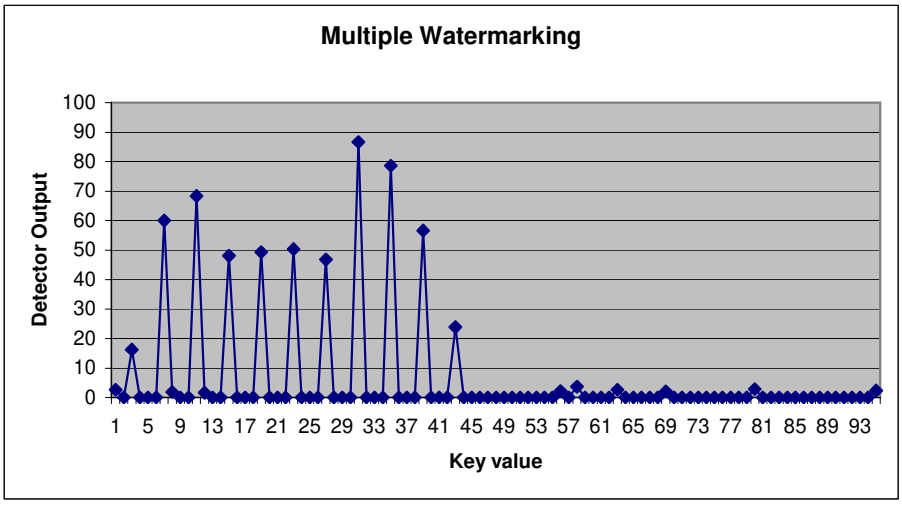

Figure 8: Multiple Watermarking Feature

The detector used in the proposed information system reveals the existence of 11 watermarks. Three of them correspond to the three zero-bit schemes while the rest 8 positive responses are used for the encoding of the fingerprint. The detector has succeeded in detecting all eleven watermarks without any confusion or misleading, resulting in a capability of facilitating proof of ownership, copy control, digital signature and transaction tracking at the same time.

3.3.6 Conclusions

As a conclusion we have proved that the robust watermarking algorithm and its implementation to the cultural information system as a black box is offering an effective platform for proof of ownership, copy control, digital signature and transaction tracking at the same time. As a result the requirements of the cultural organizations regarding the copyright protection of the digital content distributed through the information system and the Internet have been sufficiently met. Finally, the copyright protection subsystem offers innovative and state of the art services for IPR protection.

3.4 E-Commerce Applications

The last layer of the information system's architecture is the one that provides all the e-commerce applications and web services. These applications aim at establishing new standards in the field of e-commerce mainly in the digital cultural content sector. The most important components are:

- Definition of a standardized pricing policy specifically for the digital images of the cultural organizations.
- Flexible on-line license agreement which defines restrictions of use and rights for personal use.

- Design and implementation of an e-Commerce system based on the Digital Image Library with an advanced on-line catalog.
- Methods of secure commercial transactions using watermarking technologies.

The e-commerce applications implemented have the following characteristics:

- The applications are interconnected with the Digital Image Library.
- The user is using a advanced search and categorization services as an on-line catalog. These services utilize fully the capabilities of the Digital Image Library.
- The digital images purchased through the Internet are watermarked.
- Strict security is applied during the transaction, the transfer of personal data (Visa numbers, ids, etc.) and the electronic payment.

In the next paragraphs an analysis of the pricing policy and the e-commerce web services is following.

3.5 Pricing Policy

The definition of the pricing policy for digital images of cultural heritage is depending mainly on the quality, size and content. Price is not affecting the protection mechanism applied by the information system to the digital images. Even free digital images are being watermarked robustly so as the proof of ownership, copy control, digital signature and transaction tracking feature to be available for the digital content. In addition price is not affected by the rights of use (e.g. reproduction, distribution etc.), because a standard set of restrictions and use rights are being applied to all digital images through a standard license agreement.

The standardized pricing policy for digital images purchased through the web is promoting a flexible user license agreement ("signed" on-line). The users that adhere to the terms of the license have the right to reproduce a digital image, to use the digital image in web sites, CD-ROMs, to edit the image and create original works, but do not have the exclusive rights to resell the digital image or indirectly gain profit based on the digital image. The pricing policy is depending on the digital image quality, size and content and could be summarized in the next table 8.

QUALITY	FILE SIZE	PIXELS	MAXIMUM SIZE	PRICE
Low	2 MB	1024 X 1280	14,2" X 17,8" 72 ppi	€30
High	14 MB	1700 X 2550	5.7" X 8.5" 300 ppi	€120
Very high	32 MB	2800 X 4200	9.3" X 14" 300 ppi	€200

Table 8: Price as a function of quality, size and content

Finally, the digital images are provided to the user through the Internet and the estimated time to download is shown in the table 9 below:

FILE SIZE	COMPRESSED FILE	28,8	56K	ISDN	ADSL
2 MB	100 – 700 KB	5 – 7 min	1 – 2 min	< 1 min	<1 min
14 MB	1 – 3 MB	10 – 25 min	5 – 15 min	< 5 min	< 1 min
32 MB	2 – 5 MB	20 – 40 min	10 – 20 min	< 10 min	< 2 min

Table 9: Estimated time for downloading

3.6 Electronic Product Catalog

The electronic product catalog of the system is structured upon the Digital Image Library and is used as the on-line searchable catalog for the information system. This electronic catalog is not only the gateway of the information system to the world, but also provides numerous basic and advanced services. The basic features include:

- News and announcements dynamically exported by the announcements database of the cultural organization.
- Information and helpful documents.
- Online help that depends on the web page the user is exploring. The online help ranges from simple text to animated examples of how the system works.

Except for the basic features the electronic product catalog implements advanced services for the user. These services include:

- Registration forms collecting user data that are stored directly to the Digital Image Library. This data is the basis for statistics and reports and the future extensions of the system.
- Advanced methods for searching the digital multimedia content. The search methods consist of:
    - Search for metadata and free text. The user is expected to fill the required fields. The fields are referencing specific database columns and produce dynamic web pages. The user is able to search the database using relational constraints (AND, OR) and free text queries.
    - Query by Image Content (QBIC). This advanced feature allows the user to send a query to the database in terms of color and/or layout. The layout search provides for queries that are created by the user and represent basic shapes (circles, rectangular,…) filled with the preferred color. For example a user could search for an image shaped like a yellow disc and the query will result to several images representing the sun.
    - Zoom-in collections are those that give the flexibility to the Internet user to zoom in certain images. These collections are firstly presented by zoom-able thumbnails and some basic information.
    - Copyright notices and protection. The digital images are protected by digital watermarks that identify the cultural organization as the copyright holder of the digital content.

- A thematic based catalogue that organizes the digital content in categories. The user is able to refine his search using the content categories.
- Collections and Selected Cultural Presentations. Selected digital collections are created and enriched with accompanying information. They refer to specific cultural topics of common national and international interest.

3.6.1 Implementation Principles

The most advanced web technologies were exhaustively tested and evaluated. The largest part of the information system is built on pure web technologies, avoiding impressive but high bandwidth technologies like Flash or Quick Time VR. The principles of human computer interaction and usability were taken under high consideration.

Dynamic web pages, for the search results, are created with PHP (PHP: Hypertext Pre-processor is a server-side, cross-platform, HTML-embedded scripting language used to create dynamic web pages. PHP is Open Source software). The descriptive pages of the artifacts (containing a large image and detailed information) are created using Java technologies implemented as user defined functions in the database. The news pages are generated, managed and updated using Java technologies, powered by an Application Server. Zoom in collections are presented through Java applets.

Advanced services for searching and retrieving digital images, such as QBIC (Query By Image Content) searches, are created by Java applets with the support with the Digital Image Library.

All the above implementation decisions were taken after a thorough evaluation of the technologies that could be used for each case. A very important factor in the technologies evaluation was the interoperability, scalability and security of the end product (at least at the server side).

3.6.2 Implementation Paradigm

The Query by Image Content search engine is an advanced feature that allows the user to explore new ways of accessing the e-catalog content. Three main services are implemented:

- Query by Image predominant color and histogram.
- Query by Image layout.
- Query the database using a user specified digital image.

These advanced search tools are developed through the combination of web technologies such as PHP and Java Applets, embedded SQL, C++ and Dynamic Link Libraries (DLLs – Libraries which are linked to application programs when they are loaded or run rather than as the final phase of compilation), all presented with simple HTML and XML forms.

For example the Query by Image Layout is considered (see figure 9). The user is able to draw his query in terms of colored rectangular and circles. Considering that the information system is installed in a different platform than the Digital Image Library, in order to improve performance and interoperability, a Query by Image Layout involves the following steps:

- The user draws his query with the support of a Java Applet that provides for basic shapes and colors.

- A temporary file is created in the e-commerce server with PHP graphic libraries and commands, which is representing the user-driven query.
- A COM object is instantiated by PHP. The COM object is an ActiveX Control, which is a system registered Dynamic Link Library (DLL). The COM object is created with C++. The main functions of the COM object is the connection with the Digital Image Library, the necessary file format conversions of the temporary image (so as the transparency colors to be preserved), the import of the image in the Digital Image Library and the disconnection from the database. The image is stored in the Digital Image Library externally and as a result a temporary file is created in the Database Server. The COM object is also compiled as .so (shared object) file for UNIX platforms.
- An SQL statement is used for fetching a result set using success indicators and percentage of similarity, deleting the temporary fields and tuples.
- PHP is used to format and present the result-set in HTML tables and to delete all the Web Server's temporary images.
- The QBIC Layout search is a multi-user search tool.

```
<HTML>

        <? PHP

          $SQL = "SELECT imageid, mmdbsys.qbscorefromstr

          ('texture file=<SERVER, \"$tmp$Serverfile\">', IMAGE)

          from orax.basicimage order by 2 asc");

          $TemporaryFile;
          $TemporaryFileNames;
          $DeletionRoutines;


          $instance = com(QueryImage.Query);
          DLL instantiation
          Connect with Database
          File Format Conversion
          Import Image to Database
          Disconnect from Database
        ?>



        <!APPLET>
                LayoutSearch.class
                ColorSelection.class
                ColorSlider.class
                ColorSquare.class
                ColorPercentageGuage
                BrightnessSlider.class
                ImageButton.class
                ImageCanvas.class
        </APPLET>



</HTML>
```

Figure 9: Query by Image Layout – Structure

3.7 Electronic Payment subsystem

Purchasing digital images from the proposed information system, over the web, is a process that involves various functions and mechanisms. The most important are shown bellow:

- The standard basket mechanism for the collection of the images to be purchased. The basket collects all the digital images to be purchased. The digital images are presented as thumbnails while adding new or deleting images is an easy and usable process. The basket provides, also, the total cost of all the digital images to be purchased, the cost per image, basic information about the images (title, quality, file size, etc.), hyperlinks from the basic information to detailed descriptions, changing the amount of every digital image to be purchased, saving an order before checking out, etc.
- Checkout mechanism. The main features are:
    - It is supported by a secure (SSL) server.
    - Connection to credit card authorization on-line is provided.
    - User profile for addresses and sensitive data (visa number) are stored in the Digital Image Library.

When a transaction is completed a transaction identification number (id) is produced which is a pointer to detailed information about the name and addresses of the purchaser, the digital images purchased, the conditions and restrictions of use for each purchase, the relevant dates and total amounts. The transaction id, except for its storage to the Digital Image Library, it is also imperceptibly embedded into each digital image itself, using the watermarking techniques algorithm. The watermarked images with the transaction ID support the traceable usage of the images over the web. Detailed information about this mechanism is presented to the next paragraph.

4 Lessons Learned

Throughout the presented work some important lessons were learned which affected the overall system's design and implementation.

At first an effective method for requirements definition and analysis is necessary for the further design and implementation of this system or similar ones. The requirement analysis proved the complexity of the issue, defined the key entities which till today have been ignored and introduced the notion and significance of the Trusted Third Party as an organization which should support cultural organizations towards content digitization, management, copyright protection and exploitation. The information system was implemented on the basis of the requirements and technical specification of this Trusted Third Party.

The cultural information system was based on a Digital Image Library as a backbone for content and metadata management (including metadata for digital rights management) and focused on how to provide robust copyright protection for the digital content stored. An effective copyright protection mechanism includes algorithms and methods for facilitating proof of ownership, copy control, digital signature and transaction tracking at the same time.

Before implementing e-commerce applications and services for digital images the definition of a specific pricing policy and of an effective e-licensing strategy is

necessary. Prices should be depending only on quality, size and content of the digital images and not on the usage rights. The rights of use should be common for all the digital content distributed through the e-Commerce web services. The robust copyright protection mechanism should protect all the digital images, even those freely distributed. Finally, the e-Commerce web services provided support wide and effective access to the digital content through advanced search engines which facilitate even query by image content algorithms for the digital images.

5 Conclusions and Future Enhancements

Designing and implementing an integrated information system for digital rights management and protection, providing at the same time e-commerce services, for a cultural organization is a demanding and complicated task.

Through out our case study, most of effort was dedicated to meet the functional and technical requirements and to deal with the lack of basic infrastructure as far as the copyright protection and management is concerned. The result was a powerful information system that plays the role of an integrated platform for the storage and management of the digital images, their metadata and most of all for the copyright protection via digital watermarking. The watermarking method was further elaborated mainly towards a more powerful detection method and reconstructed as a portable and reusable Dynamic Link Library. The main contributions of this scheme is the ability of proving that a random watermarked image, probably downloaded through the Internet, corresponds to a specific image stored in the information system. Consequently, a) it is proved that the cultural organization is the copyright owner of the specific image and b) the corresponding key for retrieving all the copyright related information (copyright plate, important dates, contact points, etc.) is now available.

As far as the e-commerce applications are concerned “traditional” and advanced services have been developed, allowing the cultural organization to exploit the digital content produced in a proper way.

Based on the above, in order to optimize the function, interoperability and openness of the information system some services should be re-engineered, with the use of web technologies. The research will focus mainly on re-engineering the digital watermarking process, for the copyright protected images, by using XML Web Services. Specifically, the robust, multi-bit digital image watermarking facility will be encapsulated in a Web Service, allowing its reuse by several components of the information system primarily for signing and identifying copyright protected images.

References

[Barni, 98] M. Barni, F. Bartolini, V. Cappellini, A. Piva, “A DCT-domain system for robust image watermarking”, Signal Processing, “Special Issue on Watermarking”, (66) 3 (1998), pp. 357-372.

[Cox, 02] Ingemar J. Cox, Matthew L. Miller and Jeffrey A. Bloom, Digital Watermarking. (2002). Morgan Kaufann Publishers.

[CSTB, 99] Computer Science and Telecommunications Board, National Research Council. (1999). The Digital Dilemma: Intellectual Property in the Information Age (pp. 2-3). Washington: National Academy Press.

[DIG35, 00] DIG35 Specification - Metadata for Digital Images. Version 1.0. (2000). Digital Imaging Group.

[Dublin Core, 00] Dublin Core Metadata Standard. (2000). Dublin Core.

[Fotopoulos, 00] V. Fotopoulos, A. N. Skodras, A Subband DCT Approach to Image Watermarking. (5-8 September 2000). Tampere, Finland: X European Signal Processing Conference (EUSIPCO-2000).

[Fotopoulos 02] V. Fotopoulos, A. N. Skodras, Adaptive Coefficients Selection for Transform Domain Watermarking. (October 2002). Technical Report TR2002/10/02. Patras, Greece: Computer Technology Institute.

[House, 98] House of Representatives. (1998, Οκτώβριος). Digital Millennium Copyright Act.

[Katzenbeisser, 00] S. Katzenbeisser, F. A. P. Petitcolas, Information Hiding - techniques for steganography and digital watermarking (pp. 95-172). (2000). Artech House, Computer Series.

[Randall 01] Randall Davis, "The Digital Dilemma", Communications of the ACM, Volume 44, February 2001, pp. 80.

[Skodras, 02] V. Fotopoulos, A. N. Skodras, Geometric Deformations and Watermarking. (September 2002). Technical Report TR2002/09/02. Patras, Greece: Computer Technology Institute.

[Wayner, 02] P. Wayner, Disappearing Cryptography - Information Hiding: Steganography and Watermarking (Second, pp. 291-318). (2002). Morgan Kaufmann.