HAL
archives-ouvertes.fr

TSAR: Secure Transfer OF High Resolution Art Images

Denis Pitzalis, Geneviève Aitken, Florent Autrusseau, Marie Babel, François Cayre, William Puech

▶ To cite this version:

HAL Id: hal-00320836
https://hal.archives-ouvertes.fr/hal-00320836

Submitted on 11 Sep 2008

TSAR: SECURE TRANSFER OF HIGH RESOLUTION ART IMAGES

D. Pitzalis[1], G. Aitken[1], F. Autrusseau[2], M. Babel[3], F. Cayre[4], W. Puech[5]

1) C2RMF – CNRS UMR171, dept. Documentation and ITC, Paris, France.
   Email: {name.surname@culture.fr}
2) University of Nantes – CNRS UMR6597, IRCCyN Lab, Nantes, France.
   Email: florent.autrusseau@univ-nantes.fr
3) INSA of Rennes – CNRS UMR6164, dept. IETR, Rennes, France.
   Email: mbabel@insa-rennes.fr
4) GIPSA-LAB – CNRS UMR5216, dept. Image and Signal, Saint-Martin d'Heres,
   France. Email: cayre@gipsa-lab.inpg.fr
5) University of Montpellier II – CNRS UMR 5506, dept. LIRMM, Montpellier, France.
   Email: william.puech@lirmm.fr

Abstract – The EROS (European Research Open System) database hosted at the Centre de Recherche et de Restauration des Musées de France (C2RMF) is one of the largest database in the world of Cultural Heritage that is widely recognized for its high resolution images. The French research project TSAR (Transfert Sécurisé d'images d'Art haute Resolution) aims to give the possibility to open this huge amount of art images in a secure and efficient way.

For this purpose, we use a mixture of techniques to assure the security of the data involving cryptography and watermarking techniques as well as multi-resolution compression scheme together with a region-level representation. These algorithms are especially optimized for high resolution art images. In particular, this means that the quality of the transmitted images have to be not reduced, implying the use of lossless coding techniques.

In this paper we present an overall scheme that provides an efficient, consistent solution for secure data browsing, viewing and transmitting, adoptable by any Cultural Heritage institution.

INTRODUCTION

Cultural Heritage (CH) institutions, in particular museums, are supposed to undertake at least two essential missions [1]. Firstly, they have to preserve the items that represent our past and our production and save them from any damage in order to make them available for the future. At the same time, these institutes play an active role in the spread of cultural knowledge. This last educational objective imposes them to widely show and communicate these materials. However, these two missions are somewhat contrary in nature because handling works of art inevitably causes damage. To help solving this major problem, lot of investigations and researches go in the direction of "Digital Libraries" [2,3,4]: digital versions of the original art items are collected in a database on a server accessible via the Internet.

For example, the National Gallery in London, the Tokyo University Digital Museum (through the Digital Museum 2000 project) and the Louvre Museum provide public access to their databases. However, users can only browse, visualize and download low–resolution images. The application has been actually designed to prevent illegal copies of digitized data and the best and easiest way to achieve this consists basically in not transmitting the high resolution content (scientific photography, document scans, etc). High resolution information is therefore stored separately and available for a limited number of people.

This is also the case, in France, of the C2RMF laboratory, based in the Louvre museum. During the last years, it has collected digital information of more than 60,000 works of art concerning more than 1200 French museums. Part of this digital information consists of high

resolution images (up to 20,000 x 20,000 pixels). This information, gathered in the EROS database, is for the moment only accessible to researchers whose work is connected with the C2RMF's activities. In order to open the database to a wider public, when still assuring the protection of the sensible data, two problems have to be resolved. First, as the amount of data is huge, an efficient compression method has to be applied. In particular, for research purposes, this compression scheme has to provide a lossless solution. Secondly, the application must support interactive actions that can make browsing easier for users, together with efficient protection policy.

This article is organized as follows. In the next section the TSAR project and the EROS database are described as the context of our study. After the compression methods are presented. Then we describe the visible and invisible watermarking solution, the encrypting techniques. In the conclusion we show the principles of the corresponding client-server application integration.

THE TSAR PROJECT

The TSAR project (Secure Transmission of high-Resolution Art images) is supported by the French National Research Agency. Five laboratories are involved, namely the C2RMF (Louvre, Paris), IETR (Rennes), IRCCyN (Nantes), LIRMM (Montpellier) and LIS (Grenoble). The C2RMF has developed the EROS (European Research Open System) database storing digital art documentation [4].

The idea is to create a framework to integrate the different security solutions in order to secure the access to the images. The objective is to build hierarchical secure protection based on the rights of various user groups (figure 1).
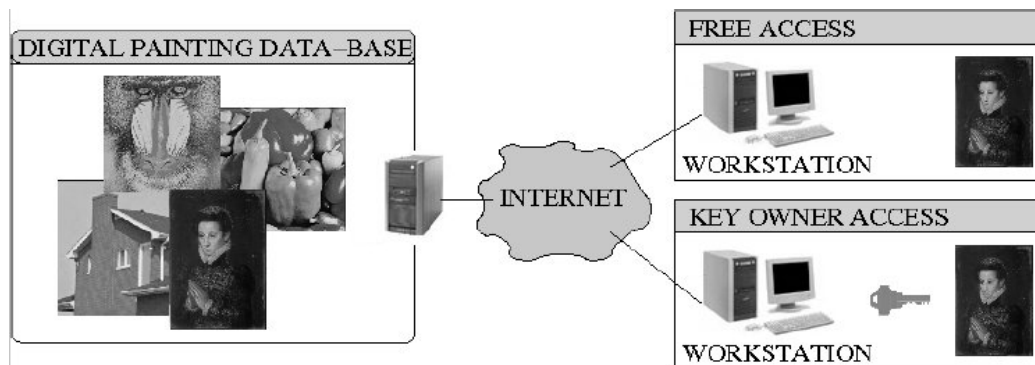
Figure 1. The TSAR/C2RMF adopted solution. A dynamic managed access to image repository.

THE EROS DATABASE

The C2RMF is today one of the most active labs in the field of research in cultural heritage at an international level. The laboratory performs not only restoration, but also documentation and scientific studies, especially chemical and physical analysis, advanced scientific imaging (X-ray, infrared, multispectral, 3D etc). It even has a particle accelerator for ???????? purpose.

The C2RMF has been an active participant in many EU projects since 1989. In this context, many projects have tried to build on and extend the work carried out in previous works, resulting in a coherent and inter-dependent body of work and few tera–bytes of digital content, mainly composed of high resolution images.

These images are accessible by an image server internally developed that is able to provide a quick access to huge images [5]. This system, called IIPImage, is designed for the remote viewing of very high resolution images across the Internet. Its architecture gives it the peculiarity to be usable even over a slow dial up connection. The server can be launched as a plug-in that can work with a variety of web servers such as Apache, Lighttpd, MyServer, Microsoft IIS or any other FCGI-enabled http servers.

Images can be browsed via feature-rich Java or Flex client, a simple Javascript client embedded within a web page or downloaded as a JPEG image dynamically generated at the requested size and resolution by the server. The modular structure of the server gives the possibility to integrate all the security technologies developed within the TSAR consortium to protect the image transmission at different levels.

DATA COMPRESSION METHODS

Advances in digital imaging have resulted in massively increased image resolutions and bit depths as well as in new techniques such as 3D imaging and topographical scanning. These new imaging techniques produce huge quantities of data that need to be adequately managed. Because of the sheer volume of data, new image optimized lossless compression methods must also be investigated.

LAR compression

The LAR method has been initially introduced for lossy image coding [6]. It is based on the assumption that an image can be represented as layers of basic information and local texture. Thus, the overall scheme of this approach consists of two scalable layers: a first one to encode an image at low bit rates, and a second one for visual quality enhancement at medium/high bit rates.

a) Original image
size : 1136×1264, 24 bpp

b) Block-level representation with grid
58703 blocks

c) Highly compressed image (1st layer)
full resolution : 0.16 bpp

d) Region-level representation
Level 1 : 1812 regions

e) Region-level representation
Level 2 : 624 regions

f) Region-level representation
Level 3 : 314 regions

Figure 2. Low resolution LAR image and hierarchical region representation on "CRT" with partition QP[16...2] and N0 < 2

The method relies first on Quadtree partitioning of the image. Homogeneity is provided by a local gradient estimation that fixes small blocks onto contours and large ones onto flat areas. The Quadtree Partition is denoted as $QP^{[Nmax...Nmin]}$ with all square blocks having a size equal to a power of two, and N_{max} and N_{min} representing respectively the maximum and minimum authorized block sizes. The first layer representation consists of rebuilding each block by its mean luminance value, encoded using a DPCM approach. The low bit-rate rebuilt image is visually acceptable thanks to the Quadtree Partition, that accommodates the variable block-size as a function of the original image context.

To encode texture, the second layer performs a variable blocksize DCT transform to fit the $QP^{[Nmax...Nmin]}$ partition. Scalability can then be content-dependent: the enhancement of contours presupposes that only the smallest blocks are processed. Subjective quality tests have been carried out between JPEG, JPEG2000 and LAR codecs: LAR outperforms other techniques for nearly all the test sequences. For color images, an original hierarchical region-based representation technique adapted to the LAR coding method has been designed, allowing advanced functionalities such as Region of Interest coding or region-level encoding of chromatic images (Figure 2). The LAR compression method can also be used, by its nature, as crypting algorithm [7].

Mojette compression

The baseline of this compression method consists in encoding the difference between several similar finite Radon projections. Two differential encoding techniques are required to efficiently encode the Radon transformed data. An intra-projection encoding technique is first performed. This differential encoding process takes benefit of the redundancy present in such projections. The second step consists of encoding the similarities between Radon projections, this is the inter- projection encoding procedure.

The used Finite Radon transform (called Mojette transform [8]), allows to ensure both compression and data redundancy. The main novelty of this work is the use of a secure distributed storage or transmission tool in a lossless compression context (figure 3).
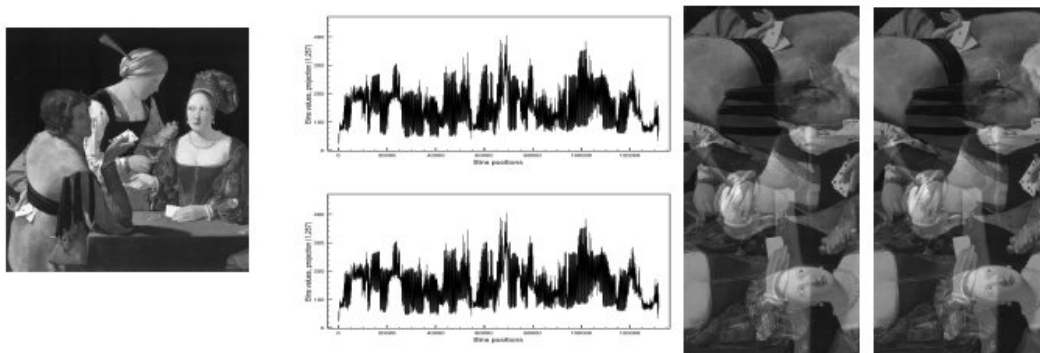
Figure 3. In the center two 1D projections with projection vectors $(1, q_i)$ where q_i is i-171 and ii-172. On the right the same projection data displayed as images with columns heights of q_i and a width of 514

WATERMARKING

Selective encryption

The proposed approach is a selective encryption in the Huffman coding of the Discrete Cosine Transform (DCT) coefficients using the Advanced Encryption Standard (AES) [9].

Selective encryption (SE) is a method that encodes only the most important portion of the data in order to provide a proportional privacy and to reduce computational requirements. The objective of our work is to leave free the low-resolution image and give full-resolution access only for authorized person. This approach is based on AES stream ciphering using VLC (Variable Length Coding) of the Huffman's vector. The proposed scheme allows decryption of a specific region of the image and results in a significant reduction in encrypting and decrypting processing time. It also provides a constant bit rate and keeps the JPEG bit-stream compliance (figure 4).

Figure 4. a) Work-of-art original image 512×640, b) Ciphered image for C = 128, c) Ciphered image for **C = 8 ????.**

Secure watermarking against Watermarking Only Attack (WOA)

More investigation is done in the watermarking field with two other methods that must be truly secure in the WOA framework [10]. The first one is called Natural Watermarking and can be made either stego-secure or subspace-secure. The second is called Circular watermarking and is key-secure.

QUALITY EVALUATION

In watermarking and data hiding context, it may be very useful to have methods checking the invisibility of the inserted data or, at least, checking the objective quality after the mark embedding or after an attack on the watermarked media [11]. Many works exist in the literature dealing with quality assessment mainly focused on compression application. Nevertheless, visual quality assessment should include special requirements that depend on the application context.

Komparator is an objective quality metric for color images based on Human Visual System (HVS) properties which doesn't need any priori knowledge about the type of degradation introduced in the distorted image. As first step, a visual representation of the original and the distorted images is computed: in this stage a model based on results obtained by psychophysics experiments on color perception and on masking effects is used. The model adopted for early vision stages is inspired by the S. Daly's Visual Difference Predictor (VDP) extended to color. The visual representation stage is then followed by an error pooling process merging all the obtained distortion maps into a single value. This stage is made up by a frequency, a component, and a spatial pooling taking into account the density and the structure of the error.

CONCLUSION AND FUTURE WORKS

Electronic Imaging & the Visual Arts
EVA 2008 Florence

The opening of art picture databases represents a promising method for the spread of cultural knowledge but it demands a number of requirements in terms of reproduction rights and access control, along with a fast, secure and user-friendly navigation.

This paper has presented an overview of a first conjoint effort, in the TSAR project, based on multiple parallel research projects in terms of efficient and original solutions for secure transmission of high definition images.

The LAR, the Mojette transform, the selective encryption, the persistent watermarking methods are developed all together within a Cultural Heritage institution with a real set of case studies and a real problematic.

The design of a client-server application is currently underway and will be the result of the parallel works ongoing in the TSAR project.

ACKNOWLEDGMENTS

References

[1] C. Xiaowu, O. Haifen, L. Xixi, C. Mingji, Z. Yi, H. Ke and M. Shunag, "The Progress of University Digital Museum Grid", in proceedings *IEEE International Conference on Grid and Cooperative Computing Workshops*, GCCW '06, 2006.

[2] EDL http://www.blueconsultants.com/edlnet/

[3] MINERVA http://www.minervaeurope.org/

[4] G. Aitken, C. Lahanier, R. Pillay,D. Pitzalis, "Database Management and Innovative Applications for Imaging within Museum Laboratories" *7th European Commission Conference "SAUVEUR"*, June 2006, Prague, Czech Republic

[5] D. Pitzalis, R. Pillay, and C. Lahanier, "A new Concept in high Resolution Internet Image Browsing," in *10th International Conference on Electronic Publishing (ELPUB)*, June 2006.

[6] O. Déforges, M. Babel, L. Bédat, and J. Ronsin, "Color lar codec: a color image representation and compression scheme based on local resolution adjustment and self-extraction region representation," *IEEE Transactions on Circuits and Systems for Video Technology*, in revision, 2007.

[7] M. Babel, O. Déforges, L. Bédat, J. Motsch, "Context-Based Scalable Coding and Representation of High Resolution Art Pictures for Remote Data Access", in proceedings *IEEE International Conference on Multimedia and Expo*, Beijing, China, 2006.

[8] F. Autrusseau, B. Parrein, M. Servieres, "Lossless Compression Based on a Discrete and Exact Radon Transform: A Preliminary Study", *IEEE International Conference on Acoustics, Speech and Signal Processing, ICASSP'06*, Toulouse, France, 2006.

[9] J.M. Rodrigues, W. Puech, A.G. Bors,"A selective encryption for heterogenous color JPEG images based on VLC and AES stream cipher," *IS&T European Conf. on Color in Graphics, Imaging and Vision,* Leeds, UK, June 19-22 2006.

[10] F. Cayre and P. Bas, "Kerckhoffs-based embedding security classes for woa data hiding," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 1, March 2008.

[11]P. Le Callet, F. Autrusseau, P. Campisi, "Visibility control and Quality assessment of watermarking and data hiding algorithms", in *Multimedia Forensics and Security*, Idea Group Publishing, Editor: Chang-Tsun Li, 2007.