A Robust Watermarking Method Supported by an Image Registration Mechanism for Securing Digital Image Libraries

Dimitrios K. Tsolis[1], Spiridon N. Nikolopoulos[1],
Vassilios Fotopoulos[2], George K. Tsolis[1], Emmanouil G. Karatzas[1],
Theodore S. Papatheodorou[1] and Athanasios N. Skodras[2]

[1]Dept. Comp. Eng. & Informatics, University of Patras, Greece.
[2]Hellenic Open University, Patras, Greece

[1]{dkt, gkt, ekaratzas, nikolopo, tsp}@hpclab.ceid.upatras.gr,
[2]vfotop1@physics.upatras.gr, skodras@eap.gr

Abstract

The issue addressed in this work is the design and implementation of a robust watermarking method enhanced with an image registration scheme. The method is integrated into the framework of a Digital Image Library allowing advanced security features like copyright protection, copy control and transaction tracking. For the evaluation of the watermarking method widely accepted benchmarking tools are utilized.

1. Digital Libraries

Libraries have always been one of the main sources of information. Plenty of information for various topics, organized and categorized according to criteria like title, author or scientific region, open to public for exploring and reading is the traditional picture of a library. Nowadays, where everything is going digital, the most promising ancestor of this large buildings filled with hundreds of books is the digital libraries.

The term digital library has been applied to a wide variety of offerings, from collections of electronic journals to software agent that support inquiry-based education, to collections of email, to electronic versions of a public library, to personal information collections, and even to the entire internet.

Information integrity is very important, especially in digital libraries where data accuracy is decisive. Confidentiality is the aspect of security that ensures the privacy of information. Copyright management and protection of the author's intellectual property rights is a necessary but difficult task especially when it comes to digital content, copy control and owner identification are the most popular countermeasures against copyright violations. Provision made for supporting digital signatures in the structure of a digital library can be a powerful instrument in the procedure of checking the validity of the information source. Complementary, fingerprinting the digital content before its distribution among the trustworthy users protects the content from its unauthorized disposal since the trace of a copy will reveal the source of the leak.

2. Digital Watermarking – Theoretical Analysis

The main goal of the watermarking idea is to develop techniques that are used to imperceptibly convey information by embedding it into the cover data. The dominant characteristic of watermarking is the notion of resilience against attempts to remove the hidden data. Thus, watermarking is used whenever the cover-data is available to parties

who know the existence of the hidden data and may have an interest removing it. The robustness against malicious attacks along with the potential of hiding data without degrading the quality of the original content, suggests watermarking as an attractive solution for the security of the digital library content.

Watermarking techniques can be applied to a variety of applications. It is obvious that watermarking requirements are different depending on the scope and the functionality of the application. Although robustness is a desirable property in almost every case, each of the applications has some special characteristics that need attention. Our interest will focus on these watermarking applications that are strongly related to the digital library security.

- **Owner identification.** Nowadays copyright protection is probably the most prominent and demanding application of watermarking. The objective is to embed information about a copyright owner of the data in order to prevent other parties from claiming the copyright on the data. The role of digital watermarks is to resolve rightful ownership, increasing the requirements of this application to a very high level of robustness.
- **Copy control.** The most desired property of a watermarking scheme is to be in position to actually prevent the illegal action. The goal of the copy control application is to prohibit people from making illegal copies of copyrighted content.
- **Digital Signature.** In situations where the information source is of great importance the library administrator must find a way to testify the identity of the information source. Digital watermarking can serve this purpose just by addressing a specified unique key to every possible information source.
- **Transaction Tracking – Fingerprinting.** In other circumstances the security framework of a digital library can increase by conveying information about the legal recipient rather than the source of digital data, mainly in order to identify single distributed copies of the data. This is useful for monitoring or trace back illegally produced copies of the data that may circulate, and is very similar to serial numbers of software products. This type of application is usually called “fingerprinting” and involves the embedding of a different watermark into each distributed copy and keeping a record for the correspondence.

5.3. Watermarking and Image Registration Schemes

5.3.1. 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 Watermarking Application. The strategy adopted is considering the watermarking method, described above, as a “black box”.

The technical requirement in favor 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.

5.3.2. Implementation

The API (Application Protocol Interface) supporting the Watermarking component is consisted of two significant methods. A method called “embed” responsible for the watermark casting and the corresponding method called “detect” capable of detecting the watermark, provided of course that the image is indeed watermarked.

5.3.2.1 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 application 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.

5.3.2.2 Detection

The main weakness of the majority of the watermarking detection mechanisms is there inability to counter the attacks involving the desyncronization 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 for finding the exact image instance during the watermark casting. Finding the right instance and feeding it to the detector supports the mechanism to achieve the 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 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 fed 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 action and in particular the Image Extender of DB2 Universal Database Management System. 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.

5.3.3 Securing the Digital Library Using Watermarking Applications

Securing the digital content has always been a great concern for the Digital Libraries designers. 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 to the digital content. Nevertheless, in circumstances where the adversary succeeds in circumventing the guarding mechanisms, the content is totally unprotected and available for illegal manipulation. On the contrary, the security provided by watermarking techniques relies on the content itself. Thus, the protection continues even after the adversary has managed to obtain the Digital Library's content.

The enforcement of the security measures described in the second paragraph is based on the notion of watermark key. The usage and administration of the watermark key is what differentiate the form of security applied, resulting in different cases. The key is an integer used for the coding of the encrypted information, or perform a more vital role by producing, for example, the pseudorandom noise sequence, like a random generator seed. The basic principle of every watermarking system is that in order for the detection to be successful, the key used by the detector should match the one used by the embeder. On the contrary the selection of any different key must cause the detector to fail. The key requirements for securing every digital image included in the digital 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.

5.5 Evaluation

The primitive advantage of watermarking techniques against other technological solutions of securing digital content is the interrelation of the watermark with the digital content itself. The security provided by the watermark protects the digital objects as long as the detector can verify the watermarks existence. Thus, contrary to the common security attacks where the adversary focalize on trying to overcome the guarding mechanisms and brake the security codes, in the case of watermarking the attacks are implemented through malicious content manipulation. An adversary uses a variety of techniques taken from the sector of image or signal processing with the aim of misleading the detector to respond erroneously. The objective for the adversary is to produce a surrogate of the original image where the watermark's presence can not be verified and the visual modification is trivial. The watermark's ability to resist such kinds of manipulation is described as watermarking robustness. In general, there is a trade-off between watermark robustness and watermark perceptibility. Hence, for fair benchmarking and performance evaluation one has to ensure that the methods under investigation are tested under comparable conditions.

The StirMark version 3.1 [6] was the benchmarking tool used for the evaluation of the present watermarking scheme. All possible attacks were applied to a sample of 5 images taken from the Digital Library of "Ulysses". The attacks were grouped in categories and tested the watermark's robustness, resulting in a score indicating it's resistance to the specified category. Finally all scores were averaged to produce a total score available for comparisons with other watermarking schemes.

Category Attack Name	Score %
Signal Enhancement & Jpeg Compression	100
Jpeg Compression	90
Scaling & Jpeg Compression	100
Cropping & Jpeg Compression	95
Shearing & Jpeg Compression	93
Rotation-Crop & Jpeg Compression	97.5
Rotation-Crop-Scale & Jpeg Compression	79
General Linear Transform & Jpeg Compression	100
Aspect Ration & Jpeg Compression	100
Row-Col Removal & Jpeg Compression	100
General Geometric Distortions	80
Total Score	**94**

Conclusions

Most of effort was dedicated to meet the security requirements, especially focusing on copyright protection and management, copy control and transaction tracking. This was mainly achieved by the development of a robust watermarking technique. The result was a modular watermarking application which serves as an integrated platform for digital image management, metadata management and copyright protection via digital watermarking.

The watermarking method was further elaborated mainly towards a more powerful detection method and transformed to a reusable Dynamic Link Library. The watermarking application was structured upon this method, benefiting by its robustness, and proposed a detection scheme based on supplementary information stored into a image library and related to the digital images. The supplementary information retrieval is supported by an image content similarity query (Query By Image Content). The main advantage of this scheme is the improvement of robustness against geometrical attacks basically due to the assistance of the image registration results.

References

[1] Randall Davis, “The Digital Dilemma”, Communications of the ACM, Volume 44, February 2001, pp. 80.

[2] S. Katzenbeisser, F. A. P. Petitcolas, “Information Hiding – techniques for steganography and digital watermarking”, Artech House, Computer Security Series, 2000, pp. 95-172.

[3] P. Wayner, “Disappearing Cryptography – Information Hiding: Steganography and Watermarking”, Second Edition, Morgan Kaufmann, pp. 291-318.

[4] G. K. Tsolis, D. K. Tsolis and 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”, in *2001 International Conference on Image Processing, Greece.*

[5] 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.

[6] M. Kutter, and F.A.P Petitcolas, “A fair benchmark for image watermarking systems”, Electronic Imaging ’99, Security and Watermarking of Multimedia Contents, Sans Jose, CA, USA, 25-27 January 1999.

[7] Ingemar J. Cox, Matthew L. Miller and Jeffrey A. Bloom, “Digital Watermarking”, Morgan Kaufann Publishers, 2002.