

Technical Description

Embedding and Retrieval-in-Order of Multiple Watermarks in PACS Images

Published: January 2011

www.astoninventions.com/WM

This technical description accompanies a white paper entitled *Embedding and Retrieval-in-Order of Multiple Watermarks in PACS Images*.

Technical Description

Embedding and Retrieval-in-Order of Multiple Watermarks in PACS Images

Contents

1	Architecture.....	1
2	Content Database.....	2
3	Watermark Database	3
4	Content Provision System	5
5	Watermark Analysis System.....	8
6	Further Reading.....	11

1 Architecture

The proposed Content Management System comprises four core components (Figure 1):

- Content Database
- Watermark Database
- Content Provision System
- Watermark Analysis System

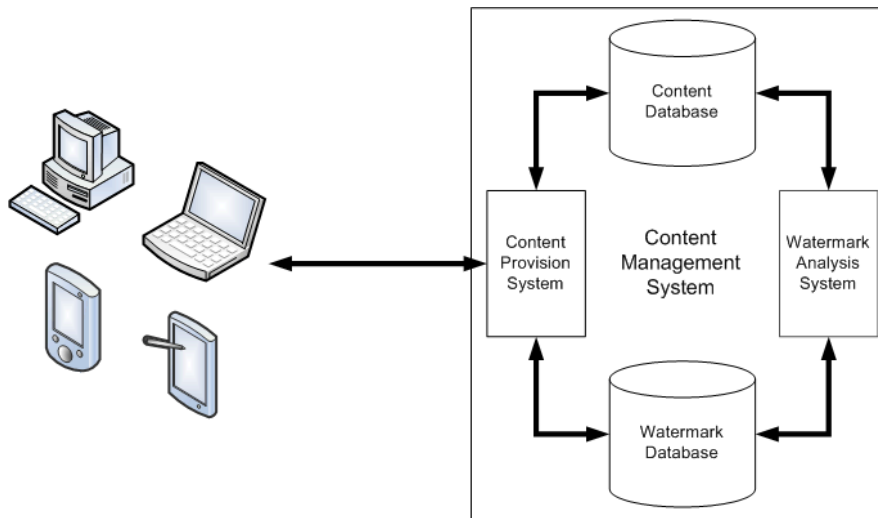


Figure 1: Content Management System Architecture

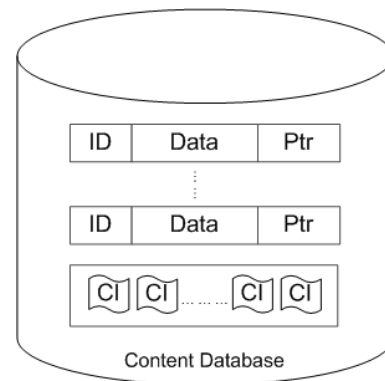
End-users will be able to connect with the Content Management System using a diverse array of computing devices.

2 Content Database

The Content Database stores the cover images. It also contains a table of records, with each record representing a particular stored cover image.

Each record comprises a unique ID number, various data or metadata, and a pointer that links the record to its corresponding cover image (Table 1).

The Content Database usually pre-exists the installation of the Content Management System, and no changes to the database structure will be necessary.

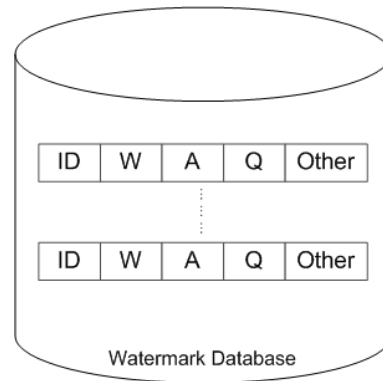


<i>ID</i>	The identification code of each cover image stored in the Content Database.
<i>Data</i>	Various data or metadata, such as the cover image creator, the date and place of creation, the identity of a rights owner, a description of the semantic content of the cover image, the name of the patient, a patient number, names of doctors, etc.
<i>Ptr</i>	A pointer that links a record with a particular cover image.
<i>CI</i>	Cover images stored in the Content Database.

Table 1: Elements of the Content Database

3 Watermark Database

The Watermark Database stores records that correspond with each cover image in the Content Database. Each record comprises data about the process used for adding a watermark to its corresponding cover image (Table 2).



<i>ID</i>	The identification code of each cover image stored in the Content Database.
<i>W</i>	A Separating Matrix. This is a matrix which decomposes an image into its base Source Vectors.
<i>A</i>	A Mixing Matrix. This is the inverse of the separating matrix, used to recombine the watermarked sources to recreate the watermarked image.
<i>Q</i>	A Quantization Value. The larger the value of Q, the more robust will be the embedded watermark, but the embedded watermark will then be more noticeable.
<i>Other</i>	Other data, such as an indicator of which source vectors have been used previously, which have an embedded watermark, and any encryption keys necessary to decrypt the watermark.

Table 2: Elements of the Watermark Database

3.1 Source Vectors

In this scheme, watermarks are embedded in the Source Vectors of each individual cover image. Source vectors are the fundamental components of each image (Figure 2). For example, a source vector component might represent the influence of sunlight or shade on pixel colouration. Each of these components can be decomposed into separate source vectors.

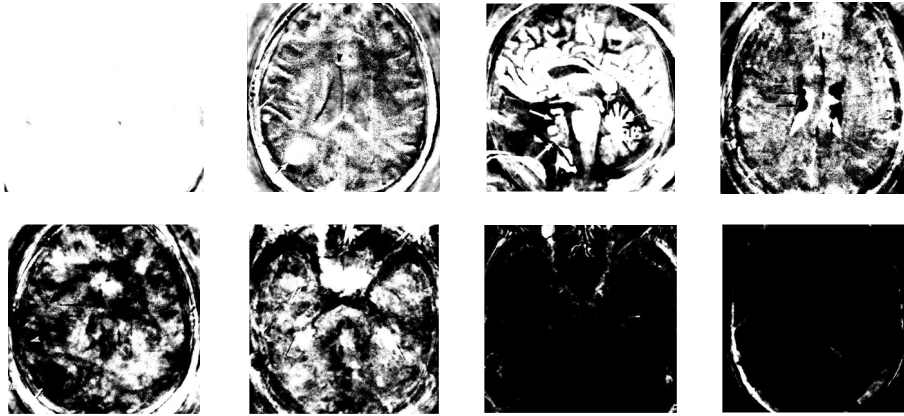


Figure 2: Sample Source Vectors

The Separating Matrix contains data representing the decomposition of each image. This is pre-computed by statistical analysis of a large number of cover images with similar content to those stored in the Content Database.

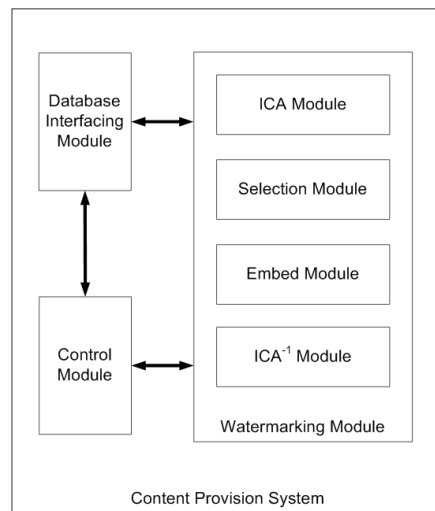
Statistical analysis is performed by Independent Component Analysis (ICA), a computational method of separating a multivariate signal (such as an audio or video recording, or still images) into source vectors.

4 Content Provision System

The Content Provision System comprises three components:

- Control Module that controls the overall operation of the Content Provision System
- Database Interfacing Module for interfacing with the Content Database and the Watermark Database
- Watermarking Module for embedding a watermark in a cover image

The Watermarking Module in turn comprises four sub-modules (Table 3).



<i>ICA Module</i>	Performs an ICA operation on an image retrieved from the Content Database. The ICA Module therefore separates a cover image into its source vectors.
<i>Selection Module</i>	Selects a source vector produced by the ICA Module.
<i>Embedding Module</i>	Embeds a watermark into the chosen source vector.
<i>ICA⁻¹ Module</i>	Performs an inverse ICA operation, that is, it reforms an image from its source vectors.

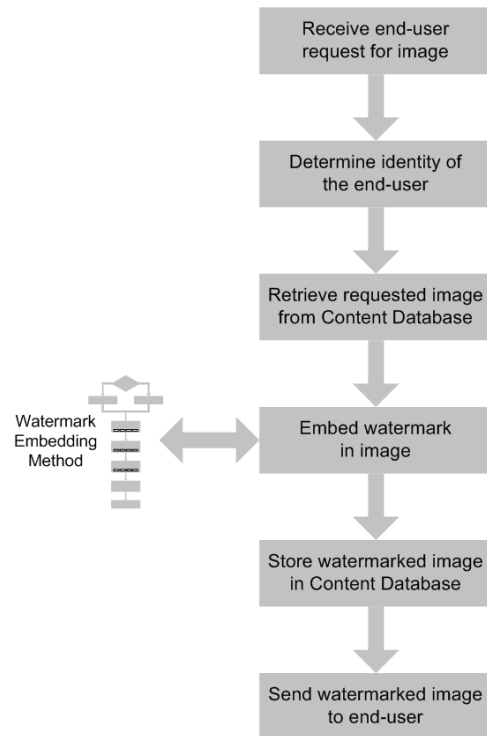
Table 3: Components of the Watermarking Module

4.1 Fulfilling End-user Requests

The Content Provision System receives and fulfils all end-user requests for images. The Control Module initially identifies the specific end-user making the request, by requesting the end-user to log-in to the system.

The Control Module then retrieves the requested image from the Content Database, and the Watermarking Module embeds a unique watermark into the image, using the Watermark Embedding Method.

The watermarked image is then stored in the Content Database, where it replaces the original image. Only then is the watermarked image provided to the end-user who made the original request.



4.2 Watermark Embedding Method

Before the Watermarking Module embeds the watermark into a cover image, it first checks for any previously embedded watermarks created by this system.

If the image has been previously watermarked, the Watermarking Module retrieves the separating and mixing matrices from the corresponding record in the Watermark Database.

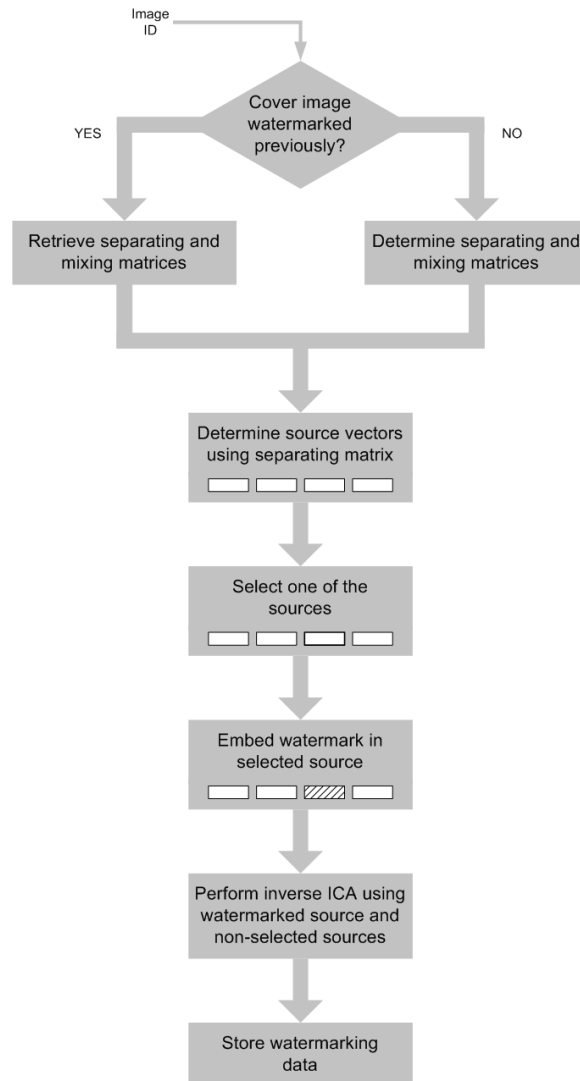
If the image has not been previously watermarked, the Watermarking Module uses the ICA Module to perform an ICA operation on the image.

In either case, the ICA Module then uses the separating matrix to determine the source vectors for the image.

The Selection Module identifies one of the source vectors to be used, and the watermark is embedded in the selected source vector by the Embedding Module (using the Quantization Value).

The ICA⁻¹ Module then performs an inverse ICA operation, to convert all source vectors back into the image—to reconstruct the complete image, which now includes a watermarked source vector.

Finally, data used in the watermarking process is stored in the Watermark Database.



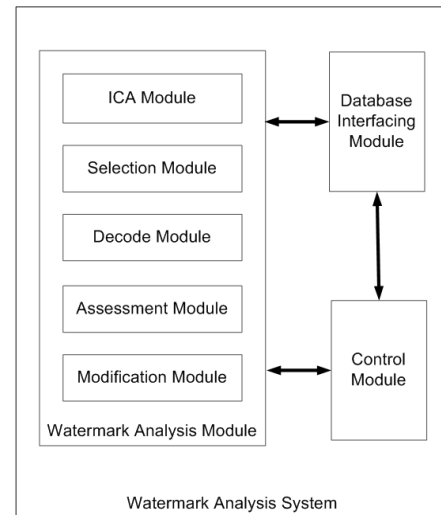
5 Watermark Analysis System

The Watermark Analysis System receives all suspect images that need to be analysed, such as a confidential image found circulating on the Internet. For instance, a suspect image may need to be analysed to ascertain its origins—that is, to determine the identity of the last end-user to access the image. This is achieved by decoding and analysing all watermarks embedded within the suspect image.

In essence, the Watermark Analysis System determines the order in which the watermarks were embedded within the suspect image, or merely the most recently embedded watermark.

The Watermark Analysis System comprises three components:

- Control Module that controls the operation of the Watermark Analysis System
- Database Interfacing Module for interfacing with the Content Database and the Watermark Database
- Watermark Analysis Module for analysing a suspect image



The Watermark Analysis Module in turn comprises five sub-modules (Table 4).

<i>ICA Module</i>	Performs an ICA operation on an image retrieved from the Content Database.
<i>Selection Module</i>	Selects a source vector produced by the ICA Module.
<i>Decoding Module</i>	Decodes a watermark out from the chosen source vector.
<i>Assessment Module</i>	Assesses the results of watermark decoding operations.
<i>Modification Module</i>	Modifies the suspect image, if necessary.

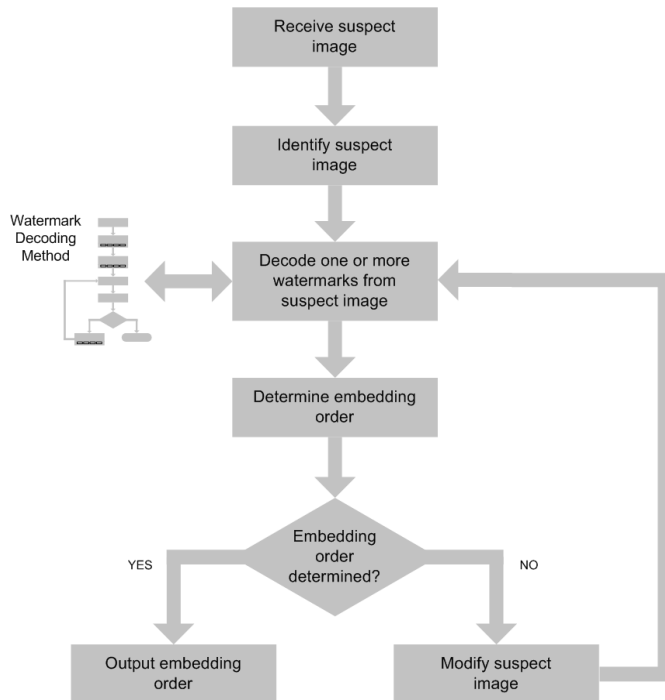
Table 4: Components of the Watermark Analysis Module

5.1 Examining Suspect Images

When a suspect image is received, the Control Module matches the suspect image to an image stored in the Content Database. This is achieved automatically using image matching algorithms, or manually by a human operator.

The Control Module then uses a Watermark Decoding Method to decode all watermarks embedded within the suspect image and determines the order in which the decoded watermarks were embedded.

If the embedding order can be adequately determined, the order is provided to the operator. If the embedding cannot be adequately distinguished, the Watermark Analysis System modifies the suspect image, in an attempt to disrupt the embedded watermarks, by affecting their data integrity indications. The Control Module then attempts once more to determine the embedding order.



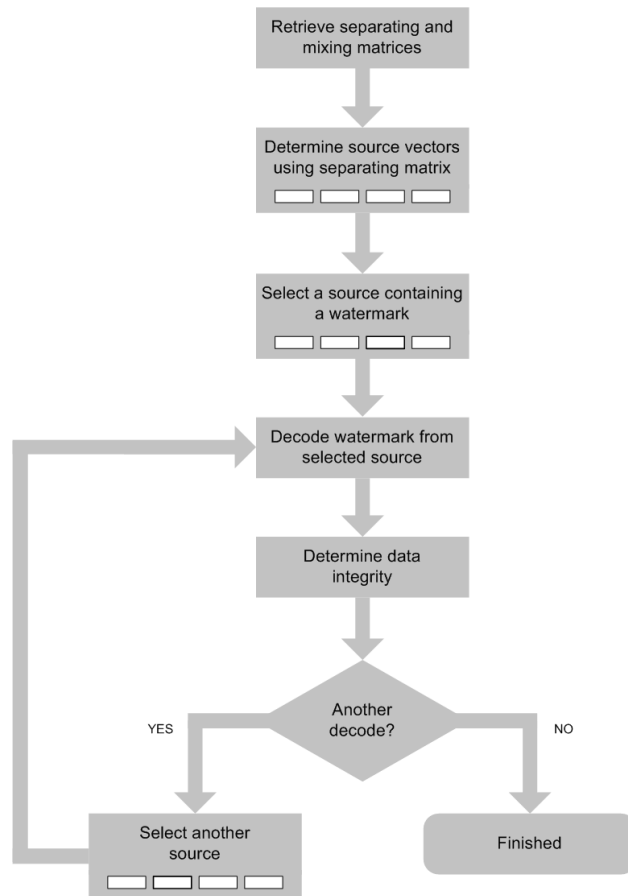
5.2 Watermark Decoding Method

The Watermark Decoding Method begins by retrieving the separating and mixing matrices from the Watermark Database.

It then uses the ICA Module to determine source vectors corresponding to the suspect image, by using the separating matrix.

The Selection Module identifies a source vector that has been used previously for embedding a watermark, and the Decoding Module decodes the watermark from the selected source vector. The Decoding Module then calculates the data integrity of the decoded watermark.

If another watermark has been embedded within the suspect image, the Decoding Module repeats this process until all watermarks have been decoded.



6 Further Reading

Stéphane Bounkong, David Saad & David Lowe (2002), “Independent Component Analysis for domain independent watermarking”, Artificial Neural Networks—ICANN 2002, Lecture Notes in Computer Science, Volume 2415/2002, 81.

Available from: <http://www.springerlink.com/content/vl7h077thv8qbevj/>

Borémi Toch, David Lowe & David Saad (2003), “Watermarking of audio signals using Independent Component Analysis”, Proceedings of the Third International Conference on Web Delivering of Music.

Available from: <http://bit.ly/ergmWU>

Stéphane Bounkong, Borémi Toch, David Saad & David Lowe (2004), “ICA for watermarking digital images”, Journal of Machine Learning Research, Volume 4, pp. 1471-1498

Available from: <http://jmlr.csail.mit.edu/papers/volume4/bounkong03a/bounkong03a.pdf>

Inna Stainvas & David Lowe (2004), “A generative model for separating illumination and reflectance from images”, Journal of Machine Learning Research, Volume 4, pp. 1499-1519

Available from: <http://jmlr.csail.mit.edu/papers/volume4/stainvas03a/stainvas03a.pdf>

BR Matam & David Lowe (2009), “Exploiting sensitivity of nonorthogonal joint diagonalisation as a security mechanism in steganography”, DSP ‘09 Proceedings of the 16th international conference on Digital Signal Processing.

Available from: <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=05201074>

BR Matam & David Lowe (2010a), “Watermark-only security attack on DM-QIM watermarking: Vulnerability to guided key guessing”, International Journal of Digital Crime and Forensics, Volume 2, Number 2, pp. 64-87, April-June

Available from: <http://www.igi-global.com/Bookstore/Article.aspx?TitleId=43555>

BR Matam & David Lowe (2010b), “Watermarking Audio Signals for Copyright Protection Using ICA”, in Ali Mohammad Al-Haj (Editor), Advanced Techniques in Multimedia Watermarking: Image, Video and Audio Applications, pp. 144-157, Hershey, PA: IGI Global

Available from: <http://www.igi-global.com/Bookstore/Chapter.aspx?TitleId=43471>

About Aston University

Aston University is a long established British university known for its ground breaking research and strong links to industry. Research at Aston makes a real difference to individuals, organisations and society—we're advancing scientific and theoretical knowledge, and working to share and implement the outcomes of our activities.

Aston has a policy of actively creating, protecting, and commercializing its intellectual property. We currently manage some 50 patent families, and we're seeking licensees who can help bring these technologies to market. We also have a number of spin-out opportunities of interest to entrepreneurs and investors.

The technology described in this technical description is the subject of an international patent application (PCT/GB2010/000308).

Further information about this technology—including the white paper, a copy of the patent application and a podcast—is available from www.astoninventions.com/WM.

References used during the creation of this document are available upon request.

Aston University
Business Partnership Unit
Aston Triangle
Birmingham B4 7ET, United Kingdom
+44 (0)121 204 4242
www.astoninventions.com

Copyright © 2011 Aston University. All rights reserved. Aston Inventions, Aston University and the Aston University logo are trademarks or registered trademarks of Aston University. Other names may be trademarks of their respective owners.