SECURITY MANAGEMENT IN A MULTIMEDIA SYSTEM

Emanuil REDNIC
PhD candidate, Economic Informatics Department
University of Economics, Bucharest, Romania

E-mail: emanuil.rednic@gmail.com

Andrei TOMA[1]
PhD candidate, Economic Informatics Department
University of Economics, Bucharest, Romania

E-mail: hypothetical.andrei@gmail.com

Abstract: *In database security, the issue of providing a level of security for multimedia information is getting more and more known. For the moment the security of multimedia information is done through the security of the database itself, in the same way, for all classic and multimedia records. So what is the reason for the creation of a security management system and a set of security rules for this type of information? The reason is the fast progress of multimedia information usage in enterprise activities. More and more distributed activities are based on processing multimedia information in real time, which is why the implementation of such a security system is important.*

Key words: *database security; distributed activities; multimedia information; relational databases; multimedia processing; watermarking; metadata; image resources multimedia filters*

1. Introduction

For more than two decades, a new issue appeared in the database technologies: how to store, manage, manipulate, archive multimedia information. At the beginning the information was not stored in the database, but only a logical reference of the physic location from the hardware, and of course all the others characteristics of the multimedia data was saved in relational tables, like: height, RGB, resolution, format. In this way a pre metadata system for managing this kind of information was created.

Furthermore, due to increased number of operations over these data and the necessity of reducing the access, processing and manipulation and other time costs, brought about the storing of the information in the database. A lot of opposing opinions appeared,

saying that databases were not designed for storing these multimedia types of data, because sustaining these data would unjustifiably load the database, due to non character based information. Why were these objections raised? The answer comes from the limited hardware resources available at the time. Fortunately the progress of database technology was followed by the progress of hardware and now we can argue that the limitation of hardware resources is no more a problematic issue in this matter.

Although the hardware limitation problem was solved, another minus was, is and will be discussed in this field: the limited resource which is time. Most database producers tried to create a system of metadata information for multimedia data in order to obtain increased flexibility, speed and scalability. One of the top producers in the field of multimedia databases is Oracle.

But how did Oracle start with multimedia database management? Oracle designed a new type of data, called long raw; then they went further by creating the BLOB's, which were used to store the multimedia information directly in the database, so that it could be managed using the same tools and could participate in the same DML operations as other types : text, numeric, time. Even with this, BLOB's were not able to manage the metadata information, so a new technology had to be introduced within the Oracle Databases, known as Oracle InterMedia.

As mentioned above, Oracle InterMedia is not a specific standalone Oracle Product, it is included in Oracle Database System, to put it in Oracle's own terms, "Oracle InterMedia Enables Databases to understand the real nature of images".

Oracle InterMedia is built on the database kernel and operates as a privileged component of the database. The advantages of using Oracle InterMedia to store images are, as follows:

- Both the descriptions of an image and the image itself can be stored using industry standard formats;
- InterMedia's objects model and methods make application programming simple in the development phase;
- InterMedia's applications maintenance become much easier as well;
- The metadata information and indexes are now created automatically by the InterMedia system;
- InterMedia eliminated the necessity of parsing the information about the image;

2. Characteristics of Oracle InterMedia

One of the most important types which was introduced by Oracle InterMedia in order to manage the image data is OrdSys OrdImage. Its design can be seen below in *Figure 1. OrdSYS. OrdImage Data Design* .

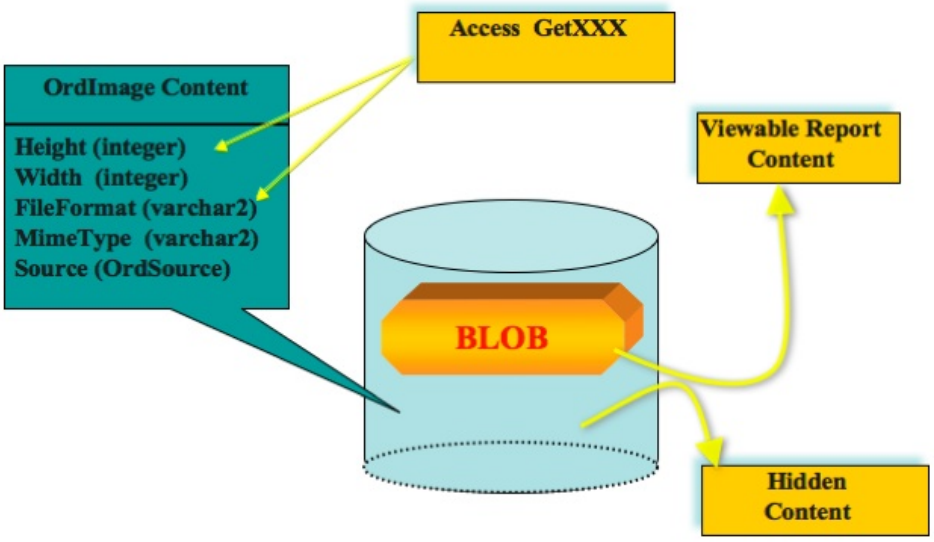

Figure 1. OrdSYS.OrdImage Data Design

As it is a Java based object, besides the Get Methods, OrdImage has as well a set of Set Methods and in all multimedia processing these GET/SET methods appear in pairs, as shown in the below sample PL/SQL procedure:

contrast.prc

```
create or replace procedure contrast(p_cod test_inter.cod%type) is
Image ORDSYS.ORDImage;
begin
SELECT photo INTO Image FROM test_inter t where t.cod=p_cod FOR UPDATE;
Image.process('contrast = 50');
Image.setProperties;
UPDATE test_inter SET photo = Image WHERE cod=p_cod;
COMMIT;
end contrast;
/
```

Figure 2. The content of "Contrast" procedure

Most of the important characteristics of Oracle InterMedia are:

- Searching and indexing/archiving of images records will be most useful if their metadata can be searched. Searching the large images can be efficient only if indexes are available to support the search. In a common way, index searching have been accomplished by complex algorithms that parses image metadata and load it into a series of indexed tables. Oracle InterMedia extract metadata from an image into an XML document, which can be stored in a single XMLType column, in the same table that contains the image column. Indexing this text column offers the robust search capabilities which lead to a faster DML;
- Flexibility: Just after the images are stored in the database, these can be manipulated like any other relational data. Set of images can be updated, deleted, copied to another table(s), by using simple SQL queries or as well PL-SQL code;
- Image manipulation: Once an image is stored in the Oracle Database as an

InterMedia object, it can be manipulated easily: the image format can be changed, RGB (red green blue collor pallete), image scaling, image cropping, image resizing, or image rotation/inversion;

- Space management: Even if the hardware limitation is not anymore problem, still how much space these data is using. Reducing the storage is a requirement for performance feature of data access as well for backup and recovery solutions. Within Oracle Database, this management includes: compressing images; changing the format, will decrease the size of the image, like changing a bitmap image to a jpeg one; remove and check the unused space; resizing and shrinking data files.

It has to be mentioned that all the features of the database itself can be applied to the InterMedia as well, like encryption, auditing access, backup and recovery, data replication, archiving. One of the most important operations in managing high amounts of multimedia data is the creation of data warehouses: features like materialized views and summary management offer a very high speed in information analysis and retrieval. Data warehouses users and applications can search for patterns in order to create/associate and retrieve summary information, which depends on the filter applied to images data, which is used in the search operations.

Oracle InterMedia provides as well, for application development, the freedom to create specific types of operations as the entire metadata system is based on the XML system, a known standard in the n-tier based applications.

3. Multimedia processing

Multimedia processing has always been based on the pixel mapping matrix. This can be achieved by sequential access, which means that each pixel is saved with its characteristics: RGB, lightness and color intensity. The image is first divided in groups of pixels, then the splitting process goes deeper to the pixel level.

Another method used more frequently because of the way graphic information is stored and as well as for the shorter processing time. This is the method used by OCR - Optical Character Recognition Software. A section of the image resource is much easier to process than the entire resource itself. Types of sections that are used by OCR software are presented in *Figure 3. Graphic Sections Used by OCR* .

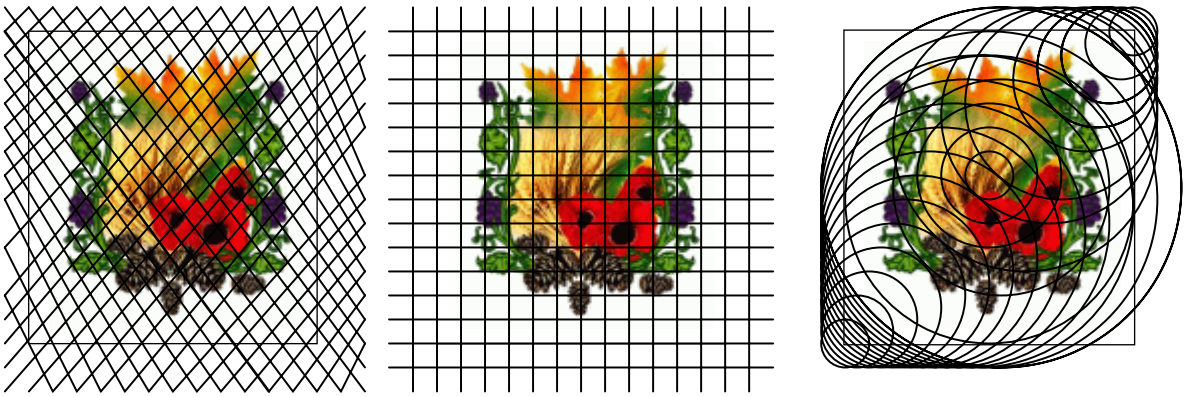

Figure 3. Graphic Sections Used by OCR

Other graphics processing operations are related to altering the color palette of the image resource, the orientation, translation, resizing:

- Transforming the image to grayscale is presented in *Figure 4. Image GrayScale Process*:

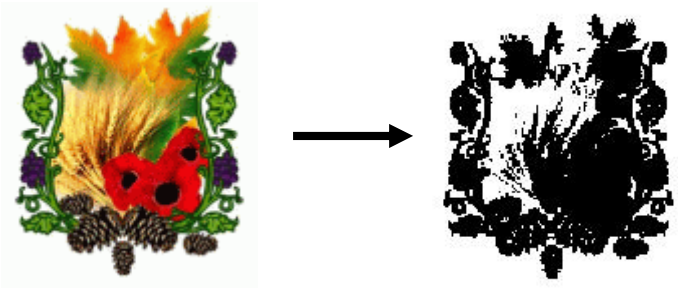

Figure 4. Image Grayscale Process

As a main characteristic OCR handles the recognition of an image by using either predefined patterns or custom ones, which are always based on fragments cropped from the image resource itself.

- Multimedia Mirroring is presented in *Figure 5. Mirroring Process*

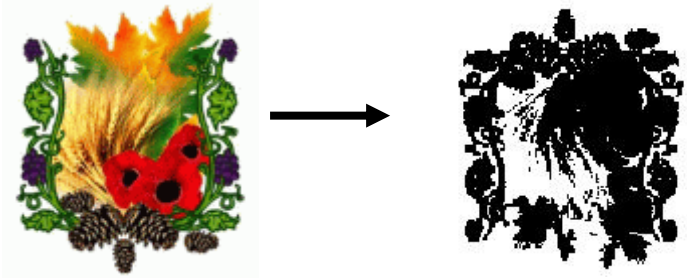

Figure 5. Mirroring Process

- Negative image: is creating by resetting all the pixels, so as each value is calculated by the complementary to the value of black color, like is shown in *Figure 6. Image Negative Process*

Figure 6. Image Negative Process

4. Multimedia Security System

The issue of multimedia security resources is a subject that has to be taken into account by multimedia application developers administrators as well by the users. This can be achieved both on the database level and on the GUI level.

On the database level, security can be achieved by the following:

- On the user level:
  - With the database mechanism of managing users: by granting/restricting access, creating roles, privileges at DDL operations, or/and at DML operations;
  - With LDAP mechanisms by integrating LDAP users into the database. In order to achieve this, Oracle Database comes with the facility of an integrating technology called Enterprise User Security.

- On the data level:
  - Using watermarking as a means to generate modified images;
  - Embedding links on metadata level.

Watermarking is the process of embedding information in content. When watermarking is done by digital means we refer to digital watermarking.
Watermarking classification is achieved by the level of visibility, so as:

- Visible watermarking, where the watermark is visible to the user when the image is read (it can be read through the same means as the image);
- Invisible watermarking, where the watermark is invisible to the user (it cannot be read through regular image reading).

Invisible watermarking can have one of two purposes:

- To transmit the information to the user by indirect means, which assumes that the image reading software is used in conjunction with other software which has the purpose to read the additional information;
- To function as a preconstituted means of proving ownership of the multimedia content in the event that some user might decide to infringe on the rights of the owner (this is usable in a court of law by the means of a technical expertise).

A good example of visible watermarking is superimposing the actual signature of the author or the name of the rights owner. It is advantageous to do this at the moment of content delivery without altering the original content.

Invisible watermarking can be used because of the intention of the rights owner (as a means of controlling infringement or as a means of transmitting additional information) or it can have a technical justification.

For example, the developer can opt to store the information in such a way that, while it is not viewable when the image itself is viewed, it can be read by other tools. This

can be justified by performance constraints or by standardization (to avoid difficulties created by inhomogeneous formats)

Another aspect to be taken into account is that when the information is not intended to be read by the user in any way, we are in fact talking about a steganographic signature.

A steganographic signature is inserted into an object in order to be able to prove ownership in case of infringement as it has no impact on the legal use of the content.

Watermarking implementation can be achieved by either public or private means. In the case of public watermarking, when each image is stored in the database, a copy of it is automatically created in another table. On the backup table, each image will have applied to it a distinguishing watermark. How a watermark should look like: either the name of the database user posted on a specific corner, transversal or any other combination of the text position, or a predefined word like : demo or specimen. It's recommended to create a parallel relation between the word used for watermark and role that the user has in the database. This allows for the use of a set of predefined words can be used: superuser, dba, sysadmin, orcladmin, like is is detailed in *Figure 7. Database watermark*

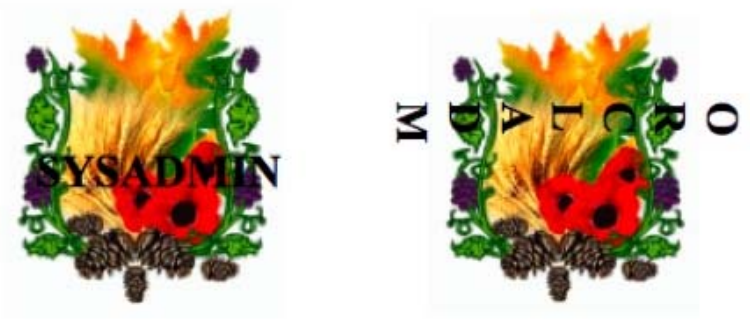

Figure 7. Database watermark

Watermarking can be either public, made automatically by adding the predefined watermark word or the custom one as it is shown in *Figure 7. Database Watermark*, or private. Private watermark can be either visible by the common user or not, this depends of the DML privileges he has on that specific image data. A sample of these custom DML privileges are shown below:

In the same way watermark can be either private or public, through the information that is added to the picture, the watermark can be either visible by the graphic views or human eyes or none. This leads to the conclusion that private watermarks are obtained by altering graphic information at pixel level and involve a small number of pixels so as the change cannot be detected by common graphic tools.

Embedded links on metadata level are a different method of including CMI in digital content is to include a link to the information instead of the information itself. Including a link to the information might lead to proprietary systems where the link only has significance to specific software used so the solution is to include some sort of standardized link such as an object identifier.

A significant argument for the use of embedded links is that the size of the information an owner wants to include in the content can be very large (for example, the owner can have an interest to tie to any type of content the terms of use associated to it) so it might not be practical to include it in the content itself.

Another possible use stems from the fact that while the overhead might not be significant for content of significant size, a standardized system might be preferable.

Implementation of embedded links on metadata level can be done through metadata stored in the database. Just as the graphic information is already provisioned in the watermarking implementation, the metadata information is required to be provisioned in order to provide the source information for embedded links. Why is necessary to create provisioning tables for the metadata information? As a standard for security of database information XML, metadata information created by Oracle InterMedia should not be altered directly, so that the information generated by the system will remain the same as it was at the time the image was stored in the database, so called T0. After the metadata information was provisioned it can be used to create a specific repository for all images that are managed in the database. Also, since the information is XML organized, it can be easily displayed in a web page based form, which can be used afterwards for the embedded links.

Embedded links can be either created dynamically or statically; the method used depends on the security standards and requirements that are mandatory in the implementation of the multimedia database application. The types of the embedded links are either web link based, which are the classically URL used for accessing a web page using the HTTP protocol, or either a document identifier, which can be either the classical path for accessing the document on the disc, or custom ones, by adding in the name of the document a specific coding: for the name of the document, the person who altered it, the version/date of the image resource, or either a random code (an alphanumerical representation for example).

5. Graphics related metrics in multimedia security systems

In order to create metrics systems for a multimedia security system, it is mandatory to first establish the entities involved in it. The main entity involved is human, followed by the graphics resources. Also, a main factor involved for creating the graphics metrics are the letters of the Latin alphabet, as described in *Formula 1*, for the case of the watermarking process:

$$GPW = (TU * FL(U,L) + TUX) * NC \qquad (1)$$

GPW – graphical process index for watermarking
L – total letters of Latin alphabet
TU – total number of users involved in the system
TUX – total number of users integrated from other directory systems
NC – number of colors used by watermark resource

FL – is a function defined on the users set, and the total letters of the alphabet, and it shows how many letters are necessary to write a user identifier

Example

For *U* - user is Scottyy , *FL(Scotty,L) = 4*, the letter *T* repeats twice in the user identifier.

We can consider *L* a constant number of letters. In this case, the *FL* function is not influenced by *L*, but for example, when applying *FL* for a non English/American user set from a Directory Service, letters like "Y", "Q", will not appear in users' identifiers. For example, in the case of a Romanian common/traditional base of names, we will not have those to letters included. Considering the above, it is mandatory to define FL as depending on L.

In Directory Services management, TU, presented in *Formula 2*, depends as well on TO (total operations made in the LDAP system), as it is described in the article "*Identity Management in University System*".

$$TU(TO) = TO + \Phi * TO \qquad (2)$$

- Total operations *TO*
- Total connections *TCN*
- Total authentication failures TF
- Total binds *TB*
- Total unbinds *TU*
- Total searches *TS*
- Total compares *TCC*
- Total modifications *TM*
- Total modifications of user distinguishing name *TMD*
- Total additions *TA*
- Total deletions *TD*

Φ is an indicator that can measure the instability of the LDAP system, due to high amounts of managed users, and takes values in the interval [0, 1]

where:

$$TO = TCN + TCN + TF + TB + TU + TS + TCC + TM + TMD + TA + TD \qquad (3)$$
$$TBV = TB + TU \qquad (4)$$
$$TR = TCN + TF \qquad (5)$$
$$TMO = TS + TCC + TM + TMD + TA + TD \qquad (6)$$
$$TO = TBV + TR + TMO \qquad (7)$$

For the embedded links, the graphics metrics is presented in *Formula 8*.

This depends, by the following:

$$GPEL = GPELD + GPELS + \alpha \qquad (8)$$

GPEL - graphical process index for embedded links
GPELD - graphical process index for dynamically embedded links
GPELS - graphical process index for statically embedded links

α influences *GPEL* an index that represents the number of embedded links not used anymore in system, used very rarely, less than 3 times in a month, or which are invalidated and not removed yet from the system.

The correlation between *GPELD* and *GPELS*, is presented in *Formula 9*, made by Ω – correlation index, so as

$$\Omega = GPELD/GPELS \qquad (9)$$

Ω can be either lesser or greater than 1 depending on the implementation of the multimedia security system.

In conclusion, the proposed multimedia/graphics metrics system can be extended, depending, of course on the level of complexity of the implemented system. In the present article, the definition of the graphics metrics system started from the multimedia security features involved in a real system: watermarking and embedded links. However, the metrics can be extended with RGB metrics, InterMedia transactional metrics. The last ones will be discussed/presented in a future article.

6. Conclusions

In an enterprise organization the necessity of archiving the documents in the databases, not only the textual information, but as a scanned copy as well appears more and more frequently. The necessity of using multimedia databases in document management has thus increased as well. Solutions for the archiving of business documents are taken into consideration as well multimedia databases as a way to implement them.

Why use multimedia databases? First of all because of the scalability advantages stemming from storing large amounts of multimedia data, secondly because of the flexibility of accessing the information, short time for either DDL and DML operations, easily achieved import/export of the information, either by using the facility of the relational databases or using databases files.

Multimedia databases can be used as well in various fields such as medical, cadastral, shipping, mailing, geographical, geodesic, transportation activities and the list goes on; as a common point for these activities are that these involve processing, in a significant percentage, multimedia information and to a lesser extent alphanumerical ones like in the case of financial/banking activities.

Besides the advantages, the multimedia databases also have some limitations, such as those relating to searching the information using a multimedia filter (a filter is an amount of pixels, even random, even consequently, from an image or a specific division or

subdivision of the image). For the moment the only way to search for specific multimedia information is by interrogating the metadata information of the multimedia information. This feature of interrogating the databases records by a multimedia filter would increase the security of multimedia information, for example through the possibility of a user to create a password based on specific pixels from an image; should the picture be altered, the password would be altered as well; in order to change the password the RGB information of a pixel would be changed. This topic is however outside the bounds of the present article and will be discussed in a future paper.

Bibliography

1. Dhananjavan, L. **Oracle Identity And Management – all in one**, ORACLE, USA, 2007
2. Mauro, J. **Oracle interMedia Managing Multimedia Content**, ORACLE, USA, 2008
3. Mavria, S. **Oracle interMedia Feature Overview,** ORACLE, USA, 2005
4. Saha, S. **Oracle Application Server 10g Administration I,II,** ORACLE, USA, 2004
5. Saha, S. **Oracle Application Server 10gr2 Administration I,II,** ORACLE, USA, 2004
6. Velicanu, M. and Rednic, E. **Identity Management in University System**, Revista Informatica Economica, no. 2, 2008, pp. 71-74

[1] Andrei TOMA has graduated the Faculty of Cybernetics, Statistics and Economic Informatics, Economic Informatics specialization, within Academy of Economic Studies Bucharest in 2005 and the Faculty of Law within the University of Bucharest in 2005. In present, he is taking his LLM in International and European Law at the University of Amsterdam and follows doctoral research at the Academy of Economic Studies. He is currently interested in IT Law as well as Computer Science issues and seeks an interdisciplinary approach to legal issues related to Computer Science.