



## Watermarking for Copyright Protection of Databases in Cloud Computing

\* Mrs. J. Delshi Julie

\* Bharathiar University, Department of Computer Science, Bishop Ambrose, College, Coimbatore.

### ABSTRACT

The watermarking interest is most likely due to the increase in concern over copyright protection of content with the rapid growth of the internet and the multimedia systems in distributed environments digital data owners are now easier to transfer multimedia documents across the internet. The existing technology does not protect their copyrights properly. This leads to wide interest in implementing copyright protection for database in cloud computing. In the early days many techniques were used to protect the database. Recently, the watermark techniques are utilized to keep the database in cloud. The paper will focus on using watermarking techniques of copyright protection for cloud computing.

**Keywords:** copyright protection, watermark, database, cloud watermark

### 1. INTRODUCTION

Cloud computing is a marketing term for technologies that provide computation software data access and storage services that do not require end-user knowledge. In this paper we ensure the copyright protection involves the authentication of ownership and the identification of illegal database. The watermarking technology has emerged as an database in order to avoid unauthorized users or access database duplication of their data or work.

Water marking technology has emerged as an effective means to hide original content in an database in order to avoid unauthorized users or access database duplication of their data or work. Protection of intellectual property is very important because database content can be copied and distributed quickly, easily, in expensively and with high quality and precision. To archive efficient database we improve existing proof of storage models the proposed schemes are highly efficient and can access the databases of cloud storage and access the cloud application without installing it in their own different computers.

Now, with the development of Internet and databases application techniques, the demand that lots of databases in the Internet are permitted to remote query and access for authorized users becomes common. Meanwhile in that the copyright of the data may not be protected effectively, the providers are worried about the data being burgled, illegal copy more and more. So we need find a mechanism to indicate to invading and pirating of the databases. We can solve this problem through embedding watermark into the databases.

Database watermarking consists of two basic process; watermark insertion and watermark deletion (Agrawal et al., 2003) as illustrated in figure 1. Watermark information is inserted into an original database so as to produce the watermarked database for publication or distribution. Given appropriate key and watermark information, a watermark deletion process can be applied to any suspicious database so as to determine whether or not a legitimate watermark can be detected. A suspicious database can be any watermarked database or in no cent database, or a mixture of them under various database attacks.

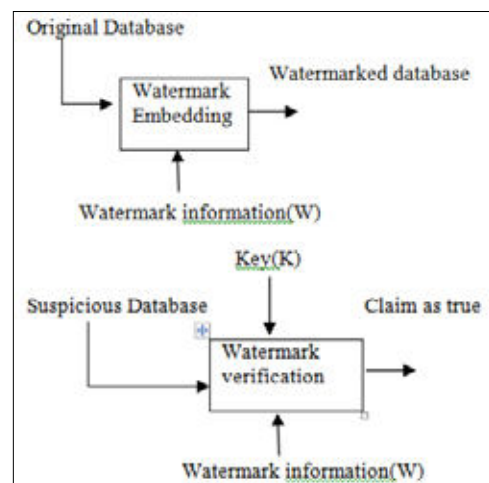


Figure 1: Basic Watermarking Technique

### 2. EXISTING SYSTEM

The existing system verified with copyright protection using watermark technique. The copyright protection is one of the best techniques used only for image with text data or audio, video etc.

Some techniques ensure that some bit positions of some of the attributes of some of the tuples contain specific values. The specific bit locations and values are algorithmically determined under the control of a secret key known only to the owner of the data. This bit pattern constitutes the watermark. Some information insertion must preserve a specific measure on data of numerical attributes.

#### 2.1 Draw backs of Existing Systems

The major problem with many of these watermarking schemes is that they are not very robust against different types of image manipulations or attacks. Moreover, some of these techniques are quite complicated to implement in real-time.

These techniques focus on databases that contain numerical content which is carefully modified to embed the watermark.

Synchronization required for watermark detection is eased by the strong structure of keys existing within databases.

Internal correlation should not be assumed for relational databases since tuples can be arbitrarily reordered.

**3. PROPOSED SYSTEM**

Cloud storage enables users to remotely store their data and enjoy the on-demand high quality cloud applications without the burden of local hardware and software management. Securing the data base in the cloud is one of the best techniques watermarking for copyright protection.

As today's techniques grow image editing become much easier and the invention of the internet provides a convenient environment for files sharing digital image are easily being copied, modified or edited. The problem of protecting database information becomes more and more important and a lot of copyright owners are concerned about protecting any illegal duplication of their database.

In the proposed system mainly focusing on the database in this system how to protect copyright of database in cloud computing.

The present a mechanism that is resilient or insensitive to additive attacks, how to embed and detect watermark in relational database. In additive attack the attacker simply inserts their own watermark in original data.

In our proposed system we can draw graphs and original ownership claim can be resolved by locating the overlapping regions of the two watermarks in which the bit values of the marks conflict and determining which owner's mark win. The attacker must have inserted the watermark later. Clearly having more marked tuples increases collisions and hence we can easily identify the owner of the data.

**4. DATABASE WATERMARKING**

The watermarking software introduces small errors into object being watermarked. These intentional errors are called marks and all the marks together constitute the watermark. The marks must not have a significant impact on the usefulness of the data and they should be placed in such a way that a malicious user cannot destroy them without marking the data less useful. Thus, watermarking does not prevent copying, but it deters illegal copying by providing a means for establishing the original ownership of a redistributed copy.

**5. METHODOLOGY**

**5.1 Types of Digital Watermarks**

Watermarks and watermarking techniques can be divided into various categories in various ways. Watermarking techniques can be divided into four categories according to the type of document to be watermarked as follows:

1. Text water marking
2. Image water marking
3. Audio water marking
4. Video water marking

In the case of imagery, several methods enables. Watermarking in the spatial domain. An alternative to spatial watermarking is frequency domain watermarking.

**5.2. Cloud Computing**

Cloud computing is location – in dependent computing, whereby shared servers provide resources, software and data to computers and other devices on demand, as with the electricity grid.

Cloud computing is a natural evolution of the wide spread adoption of virtualization, service – oriented architecture and utility computing.

**5.2.1 Features of Cloud Computing**

1. Agility: Improves with users ability to rapidly and inexpensively re-provision technological infrastructure resources.
2. Cost: Is claimed to be greatly reduced and capital expenditure is converted to operational expenditure.

3. Device and location independence: As infrastructure is off-site and accessed via the Internet, users can connect from any where.
4. Maintenance of cloud computing applications is easier, since they don't have to be installed each user's computer

**5.3. Cloud Computing Architecture**

The two most significant components of cloud computing architecture.

1. Front end
2. Back end

The Front end is the part seen by the client i.e the computer user. This includes the client's network and the applications used to access the cloud via a user interface such as a web browser.

The Back end of the cloud computing architecture is the 'cloud' itself, comprising various computers servers and data storage devices.

**5.4 How Cloud Computing Works**

The cloud consists of layers mostly the back-end layers and the front –end or user –end layers. The front-end layers are the ones you see and interact with when you access your email on Gmail for example. You are using software running on the front-end of a cloud. The same is true when you access your facebook account. The Back-end consists of the hardware and software architecture that fuels the interface you see front end.

Because the computers are set up to work together, the applications can take advantage of all that computing power as if they were running on one particular machine. Cloud computing also allows for a lot of flexibility, depending on the demand, you can increase how much of the cloud resources you use without the need for assigning specific hardware for the job or just reduce the amount of resources assigned to you when are not necessary.

**5.3. Cloud watermark embedding algorithm**

Figure 2 is the framework of relational databases cloud watermark embedding. In the figure, the parameters of Ex, En and He is the key of cloud watermark embedding algorithm for the owners. RDB denotes original relational databases. The relational databases cloud watermark embedding algorithm in details is:

Input:  
Key:(Ex,En,He),RDB.Scale;  
Output:  
CWMRDB;  
Algorithm:

- (1) Select the numerical attribute A in the RDB;
- (2) Let S equal the number of tuples in the RDB, S is the number of generating cloud drops;
- (3) Call FCG(Ex,En,He,N) and generate N cloud drops.
- (4) RDB.First;
- (5) I=1;
- (6) If RDB.EOF then
- (7) If A.value is not null and random(0..1) is less than Scale then
- (8) A.vlaue=A.value+x;
- (9) I=i+1;
- (10) RDB.next;
- (11) end

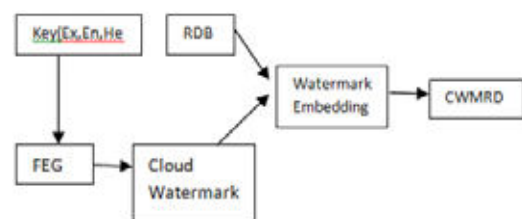


Fig 2. Cloud Watermark embedding of database

**CONCLUSION**

The client can transfer the database by using watermarking technique with copyright production. We have introduced a watermarking technique for database in cloud environment. The client can transfer their database confidentially.

**REFERENCES**

- [1]Yong ZHANG,Xiamu NIU,Dongning ZHAO,Protecting relational databases copyright with cloud. | [2] Rakesh Agrawal,Peter J.Haas,Jerry Kiernan,IBM Almaden Research Center "Watermarking relational data: framework, algorithms and analysis. | [3] Minerva M.Yeung and Fred Mintzer IBM T.J. Watson Research Center, "An invisible watermarking technique for image verification. | [4]Sukriti Bhattacharya, Agostino Cortesi, dipartimento di Informatica "watermark framework for relational databases". | [5] Raju Halder, Universita ca foscari Venezia, Italy "Water marking Techniques for Relational Database". | [6] Avani Bhatia, Mrs.Raj Kumari, U.I.E.T, Panjab University "Digital Watermarking Techniques". | [7] Jahvni Sen, IBM Kolkata, India, "An Algorithm for digital watermarking of Still imaes for copy right protection" | [8] C.Wang, Q. Wang, K. Ren, and W.Lou, "Ensuring data storage security in cloud computing", in Proc. Of IWQoS'09, July 2009. |