IGI PUBLISHING **ITJ 4724**

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.igi-global.com

This paper appears in the publication, International Journal of Digital Crime and Forensics, Volume 1, Issue 2
edited by **Chang-Tsun Li © 2009, IGI Global**

Reversible and Blind Database Watermarking Using Difference Expansion

Gaurav Gupta, Macquarie University, Australia

Josef Pieprzyk, Macquarie University, Australia

ABSTRACT

There has been significant research in the field of database watermarking recently. However, there has not been sufficient attention given to the requirement of providing reversibility (the ability to revert back to original relation from watermarked relation) and blindness (not needing the original relation for detection purpose) at the same time. This model has several disadvantages over reversible and blind watermarking (requiring only the watermarked relation and secret key from which the watermark is detected and the original relation is restored) including the inability to identify the rightful owner in case of successful secondary watermarking, the inability to revert the relation to the original data set (required in high precision industries) and the requirement to store the unmarked relation at a secure secondary storage. To overcome these problems, we propose a watermarking scheme that is reversible as well as blind. We utilize difference expansion on integers to achieve reversibility. The major advantages provided by our scheme are reversibility to a high quality original data set, rightful owner identification, resistance against secondary watermarking attacks, and no need to store the original database at a secure secondary storage. We have implemented our scheme and results show the success rate is limited to 11% even when 48% tuples are modified.
[Article copies are available for purchase from InfoSci-on-Demand.com]

Keywords: *Copyright Protection; Database Security; Reversibility; Watermarking*

INTRODUCTION

Electronic communication, faster internet data transfer speed, and peer-to-peer communication facilities enable the convenient transfer of multimedia objects. However, they also open up the possibility of copyright violations. Publishers need to insert ownership marks in the media object to discourage users from illegally downloading multimedia and thereby protect copyright. This process is referred to as *watermarking*. The major requirements of a watermarking algorithm are that the watermark should not be noticeable (imperceptibility), the watermark should survive possible attacks (robustness), successful recognition and extraction of watermark in a watermarked copy, watermark detection should require only the

watermarked copy and a secret key (blindness), and the multimedia object should have high watermark-carrying capacity.

Images, video, audio, software, natural language documents, and databases are the usual candidates for watermarking. Images are the primary contenders (Bors and Pitas, 1996; Braudway, 1997; Cox et. al, 1997) given that changing the characteristics of a pixel does not substantially degrade image quality and the watermarking capacity in millions of pixels is very high. The insertion algorithm selects the pixels that will carry the watermark using pseudo random generators with a secret seed. Thus an attacker's task is made even harder by requiring him to find out the watermark location. Comparatively, database watermarking is a new field where research interest has risen recently (Agrawal and Kiernan, 2002, Agrawal et. al, 2003; Sion et. al, 2004; Gross-Amblard, 2003; Fei et. al, 2006; Yingjiu et. al, 2006; Yingjiu and Deng, 2004; Zhang et. al, 2004; Zhang et. al, 2006). A typical database watermarking scenario is when a publisher *C* creates a database relation *R* and sells it to *O*. If *O* is a traitor, it illegally sells the relation to others. To prevent this, *C* embeds a watermark *W* in *R*. Similarly, if a data provider *D* uploads relation *R* for remote query process, an attacker might reconstruct the original relation by assembling query results. Hence, *D* uploads a watermarked relation. A blind watermarking scheme requires only the watermarked object and a secret key to detect the watermark while a non-blind watermarking scheme requires the unmarked multimedia object in addition to the first two inputs. The major disadvantage of a non-blind watermarking scheme is that one needs to store the unmarked object at a secure secondary storage location and feed it back to the detection algorithm later. Reversible watermarking provides a mechanism to revert the watermarked relation back to the original unmarked relation using a secret key. The key advantages of reversibility are that it:

1. allows for trial version of multimedia content that can be later upgraded to the full version by reversing it. A company may want to distribute low quality relations free of cost and then require customers to purchase a key using which they can revert the relation to high quality original relation.
2. allows introducing higher distortion in the data since original data can be regenerated by reversing the watermarking.

In this article, we determine the requirements of database watermarking model, feasible attacks, and propose a reversible and blind database watermarking scheme addressing these concerns.

Notation

The following notations are used in the article:

- R: a Relation,
- r: tuple,
- $r.A_i$: i^{th} attribute in tuple r,
- $r.A_i^j$: j^{th} LSB of i^{th} attribute in tuple r,
- $r.P$: primary key of tuple r,
- ||: concatenation,
- $H()$: one-way hash function,
- $R \xrightarrow{ins(p)} R_w$: R_w is the watermarked relation upon party p watermarking relation R,
- $R_w \xrightarrow{\det(p)} R$: Original relation R is restored by the party p from the watermarked relation R_w, $\lfloor x \rfloor$: floor function, *size(x)*: size of x in bits, *abs(x):* absolute value of x.

Organization of Article

We organize our articles as follows: The following section contains related work. The model of the adversary is then given and potential attacks against database watermarking schemes are described. We then present our watermarking scheme, discuss our experimental results and analyze the model in terms of capacity and security. The article is concluded with a note on future research direction.