A Database Watermarking Technique for Temper Detection

Meng-Hsiun Tsai[1], Hsiao-Yun Tseng[2], Chen-Ying Lai[3]

[1]Department of Management Information Systems, National Chung Hsing University, Taiwan, 402, R.O.C.
(e-mail: mht@nchu.edu.tw)
[2]Institute of Computer Science, National Chung Hsing University, Taiwan, 402, R.O.C.
[3]Department of Information Management, National Taichung Institute of Technology, Taiwan, 404, R.O.C.

Abstract

People pay much attention to the technology of data mining recently and more and more research institutions begin to buy the databases to analyze. If it doesn't concern customer's secrets the enterprises would also like to sell their data warehouse to do the research. Therefore, it becomes an important subject to prove the integrity of the database. This paper discusses about using the digital watermarking and the public authentication mechanism to strengthen the verification of integrity of the database. First, MD5 hash algorithm is used to fetch a database feature. Second, making XOR operation of database feature and digital watermarking gets a certification number. At last, using the secret key encrypts the certification number and makes public in the network with the database. Before using this database, user needs to use database owner's public key to decrypt the ciphertext to get the certification number. Then making XOR operation of database feature fetched by MD5 algorithm and certification number gets a watermark. Finally, user can rely on the integrity of fetched watermark to understand whether the database is destroyed or not.

Keywords: database watermarking, digital watermarking, the authentication of integrity.

1. Introduction

Recently, the technology of data mining is ripe. There is a lot of recessive information hidden behind a large number of data materials. Using the technology of data mining can dig a lot of potential, worthful, and new knowledge from unregulated data materials. Applying the new knowledge can improve the work and raise the efficiency. A typical case is the relation between diaper and beer in Wal-Mart.

Because people pay much attention to data mining, more and more research institutions begin to buy the databases to analyze. For example the consumer type their personal data like name, birthday, phone number, address in the website of book stores. Besides, the website may remember their consumption ability, and consumption habit. This data maybe doesn't have any meaning for general people, but it will be the most important information about "Consumer's psychology", "Consumer behavior" for the research institutions.

In fact, the enterprises would also like to sell their data warehouses for the institutions to do their research if the data doesn't concern customer's personal data. The market of databases is flourishing because this kind of demand and supply market is developed. But the database is easier to be copy and abuse, and the internet is popular so that the information propagates more rapidly. The information passes through the internet without monitor and could be destroyed or altered. The consumer of the information would have no idea about the validity of the information received. If someone puts fake data in the information intentionally, the researcher who analyzes the data would make a misleading conclusion and it might have great effects on related research. So the public authentication which has public trust comes with the tide of fashion.

Besides using the public authentication protects the digital information on the internet, proving the copyright and integrity of digital information is most important. So digital watermarking is developed.

The concept of digital watermarking is from Information Hiding. If people argued the copyright of protected information, we can extract the embedded watermarks to prove the copyright[6]. Digital watermarking technique mainly applies to copyright protected and integrity of information content authenticated. In the copyright protected, the watermarks must have robustness. Having robustness is even if the data is altered maliciously and it could be extracted watermarks back easily. In the integrity of information content authenticated, the watermarks have to make sure whether the data is attacked. In the past, digital watermarking technique is widely used on image process. At present, it used on databases because the markets of databases is rising.

This paper applies the concept of digital watermarking and public authentication mechanism to prove the integrity of the databases. First, the owner of databases uses a watermark which can proves their copyright does operation with the feature extracted from the databases and produces a certification code. Second, using the secret key encrypts the certification code and some parameters, and then announces the cipher text on the network through a public passageway. In order to make sure the content integrity, the users have to check the databases when they get them from network. First, the users may get a public key whichever the owner of databases publics in the network to decrypt the cipher text and get the certification code and some parameters. Second, producing a feature does operation with the certification code to get the watermark back. If the watermark is complete, it can prove the databases are integrity.

Table 1: The definitions of the notations

Notation	Meaning
T	The table of database owner gets the feature
t	The tuple of table T
N	Total tuples of the database
WM	Exclusive digital mark of database owner
WM'	The designed watermark which is hid in the feature
C_i	The feature of table T *and* tuple i
C	A set of all features of table T
R	The certification code produced by watermark WM' XOR feature C
M_i	The result of tuple i in table T dealt with MD5
b_i	Bisect M_i into the same length, the front 64 bits
f_i	Bisect M_i into the same length, the last 64 bits
X_i	The result *of* b_i XOR f_i
S_{key}	The database owner's secret key
SD	Ciphertext
P_{key}	Public key
T'	The table obtained on the internet
t'	The tuple of T'
C_i'	The feature of table T' *and* tuple i
C'	A set of all features of table T'
M_i'	The result of tuple i in table T' dealt with MD5
b_i'	Bisect M_i' into the same length, the front 64 bits
f_i'	Bisect M_i' into the same length, the last 64 bits
X_i'	The result *of* b_i' XOR f_i'
WM''	The watermark produced by feature C' XOR certification code R

2. Method

2.1 Notation

The definitions of the notations used in this paper are shown in Table 1.

2.2 Produce the certification code

It assumed that the relation of a tuple in table T is t(P, $A1$, $A2$, ..., Aj). P is the primary key and $A1$, $A2$, ..., Aj means that there are j attributes. In order to prove the integrity, we use all tuples in the table to fetch the features. The treatment step is as follows.

Step 1： Because the number of tuples in the table is very huge and the watermark length is not as long as it, our method designed the number of tuples as N.

$$N = \lceil \sqrt{N} \rceil \times \lceil \sqrt{N} \rceil . \quad (1)$$

Using the integer character of $\lceil \sqrt{N} \rceil$ makes a $\lceil \sqrt{N} \rceil \times \lceil \sqrt{N} \rceil$ watermark and produces WM', a white image besides four corners having mark.

Step 2： Using MD5(Message-Digest algorithm 5) hash algorithm [1] deals with all tuples(t) and gets a fixed 128 bits length as M_i. And then bisect M_i into the same length. That the front 64bits be b_i and the last 64 bits be f_i. Making XOR operation of b_i and f_i gets a value X_i. The purpose of this step is in order to shorten the result after hashing. And it doesn't affect the unique characteristic about MD5 operation.

$$M_i = \text{MD5}(t_i) . \quad (2)$$

$$X_i = b_i \oplus f_i . \quad (3)$$

Step 3： Fetching a remainder of X_i divided by 256 is named C_i, and the value is between 0 and 255. The purpose of this step is in order to control the feature in the range of gray image and change the feature into gray image in following steps.

$$C_i = X_i \bmod 256 . \quad (4)$$

Step 4： Repeat Steps 2-3 until all features C_i are fetched and combined as C in order. Making XOR operation of C and WM' gets a certification code R. Changing R into a $\lceil \sqrt{N} \rceil \times \lceil \sqrt{N} \rceil$ gray image looks like a hash chart. It is whole database feature after adding watermark and just like a shadow of database. At last, using the secret key S_{key} encrypts the certification image named SD and makes public in the network with the database.

$$SD = S_{key}(R) . \quad (5)$$

2.3 The verification process of database integrity

When the database owner makes public the database feature and SD, any user can use database owner's public key P_{key} to decrypt SD and to get the certification image R. And then it can fetch the feature C' of table T' and makes XOR operation of C' and R. If user can fetches complete watermark, it will be prove T' integrity. The detailed process is as follows.

Step 1： The user uses database owner's public key P_{key} to decrypt *SD* and to get the certification image *R*.

$$R = P_{key}(SD) . \quad (6)$$

Step 2：The same step as fetching feature on the original database that use MD5(Message-Digest algorithm 5) hash algorithm[1] to deal with all tuples(t') and to get a fixed 128 bits length as M_i'. And then bisect M_i' into the same length. That the front 64bits be b_i' and the last 64 bits be f_i'. Making XOR operation of b_i' and f_i' gets a value X_i'. After fetching a remainder of X_i' divided by 256 is named C_i', and the value is between 0 and 255.

$$M_i' = MD5\ (t_i'). \quad (7)$$

$$X_i' = b_i' \oplus f_i' . \quad (8)$$

$$C_i' = X_i' \bmod 256 . \quad (9)$$

Step 3： Until all features C_i' are fetched and combined as C' in order. Making XOR operation of *C* and *R* gets a watermark *WM″*. If user can fetches complete watermark, it will be prove the database integrity.

3. Experiments

3.1 Emulation experiment

In order to discuss the feasibility of our method, we design an emulation experiment to test. Our database source is "ProQuest Digital Dissertations (PQDD) ", an on-line database about master's theses and theses for the doctorate in American and Canadian area. We build a table in Microsoft SQL 2000 Sever. There are nine attributes in the table and they are **"Index", "Publication number", "Title", "Author", "Degree", "School", "Pages", "Date", "Digital formats"**. "Index" is the primary key, the value which is greater than zero and isn't repeated. Besides "Pages" is numerical, other attributes are character.

The digital mark of owner is a 30×30 gray image. There are 10,000 tuples in the table. The *WM'* is a 100×100 white image besides four corners having 30×30 mark. (Fig 1.(a))

We get the certification image *R* through method 2.2, and change *R* into a 100×100 gray image which is look like a hash chart. (Fig 1.(b)) At last, we use secret key S_{key} to encrypt the certification image.

In the fetch back step, we use public key P_{key} to decrypt *SD* and to fetch the certification image *R*. Next, we fetch the feature *C'* of table *T'* and make XOR operation of *C'* and *R*. If the experiment can get back complete watermark, it will be prove the database integrity and our method is feasible scheme.

3.2 Attacks

The most common attacks on the database are addition, deletion, and alteration. It can be detected by counting tuples of table on addition and deletion. Our scheme focuses on the most difficult alteration attack. We design some update attacks as follows.

Experiment 1:

Revise 30 Publication numbers. The purpose is finding out the result of small alteration.

Result 1:

It can find out three clear hashes on the fetched watermark.(Fig. 1(c))

We can find out the database be destroyed by naked eyes, but it isn't accurate. So we design a program to compare the fetched watermark and original watermark. The result of it finds out 30 tuples to be destroyed. The accuracy rate is 100%.

Experiment 2:

Revise the front 2000 Author. The purpose is finding out the result of character alteration.

Result 2:

It can find out the clear hashes on the top half fetched watermark.(Fig. 1(d))

We use the program to compare the fetched watermark and original watermark. The result of it finds out 1,991 tuples to be altered. The accuracy rate is 99.55%.

Experiment 3:

Revise the last 3000 Pages. The purpose is finding out the result of numerical alteration.

Result 3:

It can find out the clear hashes on the foot half fetched watermark.(Fig. 1(e))

We use the program to compare the fetched watermark and original watermark. The result of it finds out 2,991 tuples to be altered. The accuracy rate is 99.7%.

Experiment 4:

Delete Digital Formats attribute and replace with Degree attribute. The purpose is finding out the result of huge alteration.

Result 4:

It can find out the clear hashes on the whole fetched watermark. (Fig. 1(f))

We use the program to compare the fetched watermark and original watermark. The result of it finds out 9,965 tuples to be altered. The accuracy rate is 99.65%.

3.3 Feasibility analysis

Shown by the experiment, when altering huge data, the accuracy reduces a little. The false positive probability is 0.35%. It is less than 5/1000. All of the

experiment above calculates their accuracy rate, and the average value is 99.725% and the average false positive probability is 0.275%. Therefore it can prove our scheme's feasibility fairly high.

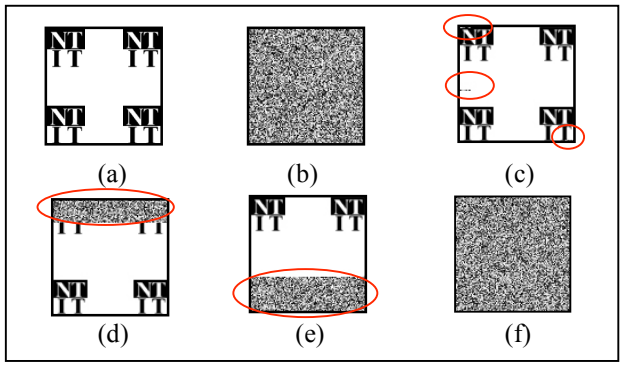

Fig. 1 Experiment results of extracted watermarks: (a) watermark WM′ with size $\lceil \sqrt{100} \rceil \times \lceil \sqrt{100} \rceil$; (b) Change R into a 100×100 gray image; (c) Fetched watermark in Experiment 1; (d) Fetched watermark in Experiment 2; (e)Fetched watermark in Experiment 3; (f) Fetched watermark in Experiment 4.

Table 2: Experiment Results

Attack	Accuracy rate
small alteration	100%
character alteration	99.55%
numerical alteration	99.7%
huge alteration	99.65%.
Average	**99.725%**

4. Method analysis

One of the essential properties that a good watermarking scheme must have is transparency. It means the embedded watermark must be perceptually invisible. In other words, it must have less and less difference between the original information and information embedded a watermark. On the other hand, network is developed and the altered data will be spread easily through Internet. So it is important to protect the integrity and security of original information. This paper has analyses about "transparency" and "integrity" as follows.

1. Transparency: One of the essential properties that a digital watermarking scheme must have is transparency. But most of data in the databases is objective. It will lose the meaning when the data is altered. In fact, not all of the records in databases must be definitely accurate. For example, the generally experimental records may produce the error in the course of experiment. These kinds of errors are produced from faults of the measuring instrument. And there are some small modification spaces because of these errors.[6] It doesn't affect the value and usability of whole records when we modify the value in this small space and it also satisfy the condition of transparency. The method of our paper is lossless and satisfies the condition of transparency easily.

2. Integrity: The internet development is rapid. Enterprises can sell the authorization numbers to research institutions to offer them remote access service besides selling the warehouses directly. Although remote access service brings much more convenience to research institutions, there are more risks in the network transmitting. The method of our paper can distinguish the integrity from extent of extracted watermark.

5. Conclusion

This paper applies the concept of digital watermarking and public authentication mechanism not only to prove the integrity of the database but also to preserve a lossless database. Users can make sure the integrity of the database before analyzing and increase their authentic degree of research.

In the future, we can hide *SD* in the database and restore an lossless database. It means to design a restored technique of database watermarking.

6. References

[1] http://en.wikipedia.org/wiki/MD5

[2] P. W. Wong and N. Memon, "Secret and public key image watermarking schemes for image authentication and ownership verification," *IEEE Transactions on Image Processing*, Vol. 10, No. 10, 2001, pp. 1593-1601.

[3] H. Zhong, F. Liu and L. Jiao, "A new fragile watermarking technique for image authentication," *Proceeding of the 6th IEEE International Conference on Image Processing*, 2002, pp. 792-795.

[4] H. Lu, R. Shen and F. Chung, "Fragile watermarking scheme for image authentication," *IEE Electronics Letters*, Vol. 39, No. 12, 2003, pp. 898 -900.

[5] K. -C. Lee, C. -Y. Su, and W. -C. Chi, 2004, "Color Image Authentication Using Dynamic Bit-Plane Checked Fragile Watermarking," *Proceedings of 17th IPPR Conference on Computer Vision, Graphics and Image Processing*(CVGIP'04), Hualien, Taiwan, 2004, pp. 15-17.

[6] Y. -Y. Yang, "A Study on Database Watermarking," A Thesis Submitted to Department of Information Management National Kaohsiung First University of Science and Technology.

[7] R. Sion, M. Atallah, and S. Prabhakar, "Rights Protection for Categorical Data," *IEEE Transactions on Knowledge and Data Engineering*, Vol. 17, No.7, 2005, pp. 01-15.