

# A watermarking algorithm of database based on Improved sharing secret scheme

ZHANG Gui-fang

Hunan College of International Economics  
Changsha ,China  
[guifangzhang2006@163.com](mailto:guifangzhang2006@163.com)

PENG Pei-fu

Physics and Information Science College, Hunan Normal  
University  
Changsha ,China  
[pengpeifu@163.com](mailto:pengpeifu@163.com)

**Abstract**—Introducing improved Asmuth-bloom scheme into database watermark, can recover the watermark based on part of data. This algorithm has a good effect of security and resisting subset attack, embedded information increased, and the performance improved much. This algorithm has good application in protecting the copyright of database.

**Keywords**—relational databases; digital watermarking; database watermark; sharing secret

## I . INTRODUCTION

Digital watermarking works by embedding the number of perceived or not perceived to determine the ownership of digital products or inspection of the original digital content<sup>[1]</sup>. At present, the digital watermarking research focused on multimedia digital watermarking. In recent years, the technology of embedding watermark information into relational database is raised.

There are two major problems of Database watermark study<sup>[2]</sup>. First, the redundancy space of relational database is small. Second, the higher robustness of watermarking algorithm is required. So, how to expand space redundancy, how to improve the watermark robustness, with ensure invisibility and the premise of the database value, has been a hot researchers to explore.

With introducing Asmuth-Bloom secret sharing system to database watermarking algorithm<sup>[3]</sup>, the performance has been improved much. Sharing information, however, with the watermark data expansion, the amount of information of the database can hold relatively reduced. If the Asmuth-Bloom secret sharing system to be extended, and then applied to watermarking algorithm can not only inherit the advantages of the above, but also a significant reduction in the expansion of the watermark data, and the performance of this algorithm is further improved.

## II . THE EXPANSION OF ASMUTH-BLOOM SYSTEM

Secret sharing<sup>[4][5]</sup> was first proposed by Shamir and Blakley. Asmuth-Bloom secret sharing system was proposed by Asmuth and Bloom in 1980, based on the Chinese Remainder Theorem<sup>[6]</sup>.

**Definition 1:** Asmuth-Bloom secret sharing system<sup>[7]</sup> The basic parameters:  $p, d_1, d_2, \dots, d_n$  are positive integers to meet the following conditions: ①  $p > s$ ,  $s$  is the shared secret; ②  $d_1 < d_2 < \dots < d_n$ ; ③  $\gcd(d_i, p) = 1, i = 1, 2, \dots, n$ ; ④  $\gcd(d_i, d_j) = 1, j \neq i$ ; ⑤  $d_1 d_2 \dots d_r > p d_n - r + 2 d_n - r + 3 \dots d_n$ , that is,  $r$  of the smallest  $d_i$  product is greater than the product of  $p$  and  $r-1$  of the largest

$d_i$ .

Share allocation algorithm: Set  $D = d_1 d_2 \dots d_r$ , and  $D$  is the plot of  $r$  number of minimum  $d_i$ , then  $D / p$  is greater than any  $r-1$  of the plot of  $d_i$ . Set  $L$  is a random integer of  $[0, [D/p]-1]$ ,  $L = s + lp$ , then calculate  $L \equiv s_i \pmod{d_i}$ ,  $i = 1, 2, \dots, n$ ,  $s_i$  is decomposition of the sub-secret secret  $s$ .

**Definition 2 :** Extended Asmuth-Bloom secret sharing system The basic parameters:  $p, d_1, d_2, \dots, d_n$  are positive integers to meet the following conditions: ① In Asduth-Bloom secret sharing system requirements  $p > s$ , based on  $p$  can be extended to take any positive integer

②  $d_1 < d_2 < \dots < d_n$ ; ③  $\gcd(d_i, p) = 1, i = 1, 2, \dots, n$ ; ④  $\gcd(d_i, d_j) = 1, j \neq i$ ; ⑤  $d_1 d_2 \dots d_r > p d_n - r + 2 d_n - r + 3 \dots d_n$ , that is,  $r$  of the smallest  $d_i$  product is greater than the product of  $p$  and  $r-1$  of the largest  $d_i$ .

Share allocation algorithm: Set  $D = d_1 d_2 \dots d_r$ , and  $D$  is the plot of  $r$  number of minimum  $d_i$ , then  $D / p$  is greater than any  $r-1$  of the plot of  $d_i$ . Set  $L$  is a random integer of  $[0, [D/p]-1]$ ,  $L = s + lp$ , then calculate  $L \equiv s_i \pmod{d_i}$ ,  $i = 1, 2, \dots, n$ ,  $s_i$  is decomposition of the sub-secret secret  $s$ .

## III. DATABASE WATERMARKING ALGORITHM

Watermark Embedding and recovering algorithm are both based on extended Asmuth-Bloom secret sharing system.

### A. Watermark Embedding

Setup1 Encryption of the watermark information.

Setup2 Watermark information will be encrypted first character code is converted to ASC II form ( $s$  with that).

Setup3 According to Definition 2, select the appropriate parameter values of  $s$  sub-survival, to be kept at the value of  $s_i$ , respectively, will be converted to a fixed 0,1-digit sequence.

Setup4 Repeat Setup2, Setup3, followed by watermark information obtained at the value of the binary sequence

Setup5 Effective screening database the numeric field  $r.A_i$  (indicated by  $v$ ). Index = Hash (Key, Primary,  $A_i$ ).

Setup6 Index values in accordance with sub-keeping value of the order of the binary sequence to replace the special bit of the  $v$ .

## B. Watermark recovering

Setup1 Screening  $v$  from the database, Index = Hash (Key, Primary,  $A_i$ ).

Setup2 According to the index value extracts the special bit of  $v$ .

Setup3 Calculate the all shared information; select  $r$  higher accuracy of shared information, and then recover the watermark information.

## IV. SIMULATION AND PERFORMANCE ANALYSIS

when do experiment, the median filter effectively greater than or equal to 5 numeric field is used to watermark embedding, the field values in line with the requirements of a total of 41,169; embedded watermark information for "the copyright of database". From the light of the definition 2 of parameter values:  $r = 2$ ,  $n = 4$ ,  $p = 7$ ,  $d_1 = 11$ ,  $d_2 = 13$ ,  $d_3 = 14$ ,  $d_4 = 15$ ,  $l = 0$ . Simulation of a subset of attack, according to the proportion of randomly selected, modify database records, a random increase in records, and then extract and restore the watermark. Select a subset of the proportion of attacks  $\geq 20\%$ 、 $17\%$ 、 $14\%$ 、 $11\%$ 、 $8\%$  ; accurate restoration of the ratio of  $100\%$ 、 $89\%$ 、 $73\%$ 、 $52\%$ 、 $22\%$  ; Subset of the ratio of increase in attacks  $\leq 85\%$ ,  $88\%$ ,  $91\%$ ,  $94\%$ ,  $97\%$ , accuracy of the restoration of the ratio of  $100\%$ ,  $90\%$ ,  $76\%$ ,  $60\%$ ,  $41\%$ ; subset modified attack ratio of  $\leq 50\%$  ,  $53\%$ ,  $56\%$ ,  $59\%$ ,  $62\%$ , the proportion of accurate restoration of  $100\%$ ,  $86\%$ ,  $71\%$ ,  $47\%$ ,  $18\%$ .

In the same circumstances, with reference to the definition 1 from the parameter values:  $r = 2$ ,  $n = 4$ ,  $p = 127$ ,  $d_1 = 139$ ,  $d_2 = 143$ ,  $d_3 = 145$ ,  $d_4 = 147$ , The experimental results are as follows: select a subset of the attack were selected for the proportion of  $\geq 35\%$ ,  $32\%$ ,  $29\%$ ,  $26\%$ ,  $23\%$ , accuracy of the restoration of the ratio of  $100\%$ ,  $91\%$ ,  $80\%$ ,  $67\%$ ,  $43\%$ ; subset increase attack ratio of  $\leq 70\%$ ,  $73\%$ ,  $76\%$ ,  $79\%$ ,  $82\%$ , accuracy of the restoration of the ratio of  $100\%$ ,  $92\%$ ,  $75\%$ ,  $51\%$ ,  $23\%$ ; subset modified attack ratio of  $\leq 37\%$ ,  $40\%$  ,  $43\%$ ,  $46\%$ ,  $49\%$ , accurate restoration of the ratio of  $100\%$ ,  $87\%$ ,  $70\%$ ,  $52\%$ ,  $25\%$ .

Experiments, the reference parameter values from the definition of 2, select a subset of the resumption of attacks on  $100\%$  accurate information on the proportion of watermark to  $15\%$ , a subset modified attack  $15\%$  increase in attacks on a subset of the high  $13\%$ . As follows:

Experiment with the watermark information is the actual meaning of the string. ASC II code value of each character that is embedded in the algorithm have to keep Setup3 the  $s$  value ( $s \leq 122$  ).

the value of parameter  $p$ : the experimental value of the first set of parameters in accordance with the definition of 2,  $p$  can take any positive integer,  $p = 7k$ , to meet the requirements;

The median sub-watermark bit: in the first set of parameters  $d_1 = 11$ ,  $d_2 = 13$ ,  $d_3 = 14$ ,  $d_4 = 15$ , to meet the requirements of the definition 2. According to the share allocation algorithm for keeping the value of sub- $s_i$  (), will be converted to  $s_i$ , respectively, of the four sequences can be 0, 1. The second group of parameter values, by definition 1, we can see,  $d_i > p = 127$ , keep the value of sub- $s_i$  (), will be converted to 0, 1

sequence  $s_i$ , the median should not be less than 8. Thus, the number of 0,1 bits of watermark information based on definition 2 is half of that based on definition 1.

Database watermarking algorithm based on definition 2, the watermark information embedded in the redundant space needs for the system based on definition 1. Embedded information bit less attack, the watermark to the probability of attack on the small. Therefore, Database watermarking algorithm based on definition 2, has better robustness and anti-attack capability.

## V. CONCLUSION

Database watermarking technology is a new thing the field of database security. This research has wide application prospects. Database watermarking algorithm proposed by this paper, not only has good security and a subset of anti-attack capability, but also a significant reduction in the expansion of the watermark data. Theoretical analysis and experimental results show that the algorithm can actually be a very good database application.

- [1] Chen minch, NIU Xin-xin, YANG Yi-xian. The progress of digital watermarking research and application [J]. Journal of Communication, 2001.5,22 (5) :71-79.
- [2] Rakesh Agrawal, Jerry Kiernan. Watermarking Relational Databases[C]. Proceeding of the 28th VLDB Conference. Hong Kong, China, 2002, pp155-156.
- [3] Zhang Guifang, Sun Xing-ming, Xiao Rong, Peng Pei-fu. Based on Chinese Remainder Theorem Watermarking database [J]. Computer Engineering and Applications, 2006.3,42 (7) :135-136.
- [4] A.Shadir. How to Share a Secret. Communications of the ACD,24(11),1979,pp.612-613.
- [5] G. R. Blakley. Safeguarding Cryptographic Keys. Proceedings of the National Computer Conference, 1979, American Federation of Information Processing Societies, 48,1979,pp.313-317.
- [6] Chen Jing-run . Elementary number theory I [D]. Beijing Science Press ,1978,17-22.
- [7] C.Asduth, J.Blood. A Modular Approach to Key Safeguarding. IEEE Transactions on Information Theory, 1983,29(2):208-210.