IDR privacy protection based on sharing watermarking

Yuancheng Li[1], Yimeng Wang[*1], Xiang Li[1]

1. School of Control and Computer Engineering, North China Electric Power University, Beijing 102206, China;

Abstract: Demand response (DR) technology is an important part of the smart grid framework during the construction of smart grids. DR can be divided into Price-based Demand Response (PDR) and Incentive-based Demand Response (IDR). For the privacy leakage problem in IDR, we combined database digital watermarking algorithm with an improved Shamir-based secret sharing algorithm, and proposed the strategy of IDR privacy protection. Firstly, the billing cycle is segmented into shorter time periods. During each time period, the sharing watermarks are embedded in the electricity consumption data, and are stored using an improved Shamir-based secret sharing algorithm. When the billing period ends, the watermarks are extracted from the electricity consumption data of each time period. Then, the total power load during the billing period is transmitted to the power company. This method makes the power company unable to obtain the specific power consumption data of the user at each moment, and avoids leakage of user privacy. Finally, we performed the comparison experiments and robustness analysis of the proposed watermarking algorithm. The experimental results show that the proposed method performs well on protecting privacy. Meanwhile, it also achieves stronger robustness and security, and lower computational overhead.

Keywords: smart grid; incentive-based demand response (IDR); privacy protection; sharing watermarking; secret sharing

1. Introduction

IDR is a policy implemented by the electric power agency based on the supply and demand situation of the power system.IDR refers to the user reduces the power demand when the system needs or the power is tight, so as to obtain direct compensation or preferential price for other time periods [1-3]. IDR technology uses a database to store the user's electricity usage data at various times to analyze the user's contribution to the electricity market. However, if these user data are illegally leaked, it will pose a threat to user privacy. At present, digital watermark is an important branch of information hiding technology researching, which is mostly used to maintain database security and privacy protection [4].

The database needs to be maintained and updated frequently, which make it easy to lose the watermark information. Therefore, the application of the secret shared watermark is more robust, and realizes the recovery of the watermark information based on the part contents of the database.

Literature [5] proposes a public database watermarking method based on independent component analysis (ICA). In [5], the watermark image is processed by ICA to obtain several independent component watermarks. The iterative hybrid method is used to embed the watermark, and then the blind source JADE algorithm is used to extract the watermark, so that the watermark information can be embedded with less carrier cost. However, whether the watermark can be successfully extracted depends on the blind source signal separation algorithm, and the blind source separation algorithm is not very mature. Literature [6] proposed a hierarchical structure error control watermark model. On the whole, the idea of dividing the secret key by the Lagrangian interpolation formula is introduced into the partitioning algorithm of the relational database digital watermark. Using the Lagrangian interpolation formula to separate the watermarks can make the watermarks more widely distributed, and only need to extract a partial sub-watermark to recover the original watermark, without extracting all the sub-watermarks. However, the repeated embedding of the watermark makes the amount of watermark information expand several times, and the modification of the database is relatively large. Literature [7] proposed a database watermarking algorithm based on Reed Solomon code. Reed Solomon error correction coding has the ability of multi-bit error correction, which is a very ideal error correction coding, and improves the self-recovery of watermark. At the same time, Reed Solomon code improves security of the watermark by using Lagrangian watermark storage technology globally. Even if the pirate knows the embedding algorithm of the watermark, it can only extract the partial watermark after the separation, and the original watermark information cannot be obtained. However, this algorithm is suitable for databases that can be embedded in smaller capacities. In [8], a relational database digital watermarking algorithm based on distributed grouping is proposed. Firstly, the watermark information is encrypted, then the encrypted watermark information is divided. Finally, the watermarked storage value is divided into bitwise unequal group sequences for watermark embedding. However, this method is relatively weak for the tuple data errors that occur during the insertion and extraction of the relational database watermark, and the protection of the watermark when the database is subjected to data tampering attacks. In [9], a database watermarking technique based on the Chinese remainder theorem is proposed. The secret sharing idea based on the Chinese remainder theorem is applied to the database watermarking algorithm, and the partial content recovery watermark information based on the database is realized. However, the algorithm expands the watermark data and relatively reduces the amount of watermark information that the database can accommodate. Literature [10] proposed a database digital watermarking algorithm combined with wavelet transform and independent vector analysis, but the system performance of the algorithm is not very high. In [11], a secret key sharing technique based on linear homomorphic equations is proposed, which implements the (t,n) threshold scheme in the form of linear equations. However, the algorithm should be at the expense of the security sacrifice of the secret key to enhance the robustness. In [12], a relational database digital watermark based on Lagrangian interpolation is proposed. The idea of Lagrange interpolation formula for secret key separation is introduced into the relational database digital watermarking algorithm. However, to the tuple data error that occurs during the insertion and extraction of the relational database watermark, and the protection of the watermark when the database is subjected to data tampering attacks, the method appears to be same weak.

Therefore, in view of the shortcomings in the above work, we have proposed a watermarking algorithm based on Shamir secret sharing improved algorithm, which is applied to solve the problem of smart grid IDR privacy protection.

2. Improved Shamir-based secret sharing algorithm

Shamir proposed the concept of secret sharing in 1979 [13]. The Shamir (k, n) secret sharing algorithm divides the secret S into n sub-secrets. Any k sub-secrets can recover S, and any k-1 sub-secrets cannot. In reality, there may be more than k sub-secrets in the secret recovery process, so it is necessary to improve the traditional Shamir secret sharing algorithm. The secret is restored by introducing a linear combination of shadow secrets, which is the Lagrangian factor.

The sharing scheme includes three steps of initialization, secret distribution, and secret recovery. The specific process is as follows:

(1) Initialization

The secret distributor randomly selects r(r=1, 2, . . . , n) non-zero constants x_r from the finite field GF(p) and marks U_{r}, exposing x_r and its corresponding U_{r}.

(2) Secret distribution

The secret distributor performs a shadow secret generation algorithm to generate n shadow secrets and distributes them to the corresponding U_{r}.

a. Randomly select kt(kt>n-1) non-zero coefficients

$\{a_{lm} | a_{lm} \in GF(p); 1 \le l \le k, 0 \le m \le t-1; a_{lm} \neq 0\}$ constitutes k (k is a constant) (t-1) order polynomial:

$$f_l(x) = \sum_{m=0}^{t-1} a_{lm} = a_{l0} + a_{l1}x + \cdots + a_{l(t-1)}x^{t-1} \quad (1)$$

b. Calculate the shadow secret $f_l(\mathrm{x}_r)$(l = 1, 2, ... k)of U_{r}. That is:

$$f_l(x_r) = (\sum_{m=0}^{t-1} a_{1m} x_r^m, \sum_{m=0}^{t-1} a_{2m} x_r^m, \dots, \sum_{m=0}^{t-1} a_{km} x_r^m)(2)$$

c. For any secret S, the secret distributor can always find the integers d_l and w_l in the finite field GF(p) (where l=1, 2,...,k;$\mathrm{w}_i \neq \mathrm{w}_j$; $\mathrm{w}_i \notin \{x_1, x_2, \dots, x_n\}$) satisfied:

$$\mathrm{S} = \sum_{l=1}^{k} d_l f_l(w_l) = d_1 f_1(w_1) + d_2 f_2(w_2) + \cdots + d_k f_k(w_k) \quad (3)$$

d. Send $f_l(\mathrm{x}_r)$ to the corresponding U_{r} through the private security channel, and broadcast the integers d_l and w_l.

(3) Secret recovery

The participant P_{r} who needs to recover the secret S sends a recovery secret request to the participant members $\{P_1, P_2, \dots, P_j\}(t \le j \le n)$, and receives the Lagrangian factor $C_{\mathrm{r}}^{\emptyset}$ sent by the j-1 participants. The Lagrangian factor $C_{\mathrm{r}}^{\emptyset}$ is a linear combination of the secret $\mathrm{S} = \sum_{\mathrm{l}=1}^{k} d_l f_l(w_l)$.The opponent can't restore the true effective shadow secret and recovering the secret S in the secret sharing process when gets the Lagrangian sent by the remaining participants. Thus, this method can improve the security of shadow secrets and secrets. In addition, the Lagrangian factor in secret recovery can directly prevent the problem of spoofing, so that the shadow secrets of each participant need not be verified one by one, which improves the efficiency of secret recovery. Let the authorization subset consisting of j participants in U_{r} be $\emptyset$, and its execution operation is as follows.

Through the shadow secret $f_l(\mathrm{x}_r)$ sent by the secret distributor, the participant P_{r} obtains its unique Lagrangian factor $C_{\mathrm{r}}^{\emptyset}(1 \le \mathrm{r} \le \mathrm{j})$ using equation (4).

$$C_{\mathrm{r}}^{\emptyset} = \sum_{l=1}^{k}(d_l f_l(x_r) \prod_{v=1, v\neq r}^{j} \frac{w_l - w_v}{x_r - x_v} \qquad (4)$$

Where $\{\emptyset \in 1,2, \dots, \mathrm{n}\}, |\emptyset| \ge t$.

After receiving the secret recovery application sent by the member, the participant P_{r} sends its Lagrangian factor $C_{\mathrm{r}}^{\emptyset}$ to the remaining j-1 participants through the secret channel.

P_{r} uses the received j-1 Lagrangian factors $C_{\mathrm{r}}^{\emptyset}$ to calculate the secret S using equation (5).

$$\mathrm{S} = \sum_{\mathrm{r}=1}^{j} C_{\mathrm{r}}^{\emptyset}(5)$$

3. IDR privacy protection method based on sharing watermarking

In this section, we combine database digital watermarking algorithm with the improved Shamir-based secret sharing algorithm, and propose the strategy of IDR privacy protection. We introduce the sharing watermarking privacy protection algorithm, and the process of watermark embedding algorithm and extraction algorithm in detail.

3.1 Sharing watermarking privacy protection algorithm

In our proposed method, each billing cycle is time-segmented, and the sharing watermark is embedded in the segmented power consumption data. Based on the Shamir-based secret sharing improvement algorithm, the basic idea of secret sharing is introduced into the database digital watermarking algorithm, and the watermark information is divided into n sub-watermarks. At the end of the billing cycle, watermarks are extracted for the data of each time period, and the original watermark can be restored by accurately extracting the r(r≤n) sub-watermark from the watermark carrier. Then, the total power consumption load in the user billing cycle is transmitted to the power company. This process can make the power company unable to obtain the specific power consumption data of the user at various moments, so as to prevent the privacy of the user and the integrity of the database.

A relational database to be embedded with watermark information is represented by R(P, $A_1, A_2, \dots, A_v$). Among them, P is the primary key, $A_1, A_2, \dots, A_v$ is a numerical attribute column of v watermark embedding, R is composed of n tuples $r_1, r_2, \dots, r_n$, each tuple has 1 primary key r.P and v numerical attribute values $\mathrm{r}.A_1, r.A_2, \dots, r.A_v$. In this way, the embedding of the watermark information can be realized by changing the least significant bits of the n*v attribute values. Before embedding the watermark, it is necessary to introduce constraints, and the algorithm only embeds the watermark information for the attribute values that satisfy the constraint. To determine a length value L, only the numeric attribute value, whose valid digits greater than or equal to L, can be used to embed the watermark information. Through the above calculation, find out all the attribute values that can be embedded in the watermark, and number them. The number of each available attribute value depends on its attribute name, the primary key value of the own tuple, and a certain key, that can be calculated with the hash function: index=hash(key, r.P, A_j). The Hash function is a one-way hash function that can transform an input of arbitrary length into a fixed-length output through a hashing algorithm. It has the characteristics of simple forward calculation and difficult reverse calculation.

3.2 Watermark embedding algorithm

The watermark information can be any form such as an image, a string, or a random sequence [14]. In the design of digital watermark, the original watermark is often encrypted in advance to improve the security of the watermark. The encrypted watermark can effectively resist the guessing attack. In view of this, we use a unipolar logistic chaotic sequence, which is sensitive to the initial value, to encrypt the watermark, as defined below:

$$x_{i+1} = \mu x_i (1 - x_i)(6)$$

Where $0 \leq \mu \leq 4$, $x_i \in (0,1)$. When $3.56945 \leq \mu \leq 44$, the logistic mapping works in a chaotic state. The sequence generated by different x_0 is aperiodic, irrelevant, non-convergent, and very sensitive to the initial value.

The watermark embedding steps are as follows:

(1) First, pre-process the watermark, and convert it into a binary sequence w. Then, generate a unipolar logistic sequence L with the private key $k$as the initial value, select the front $|w|$ bit of L, and set a threshold to binarize L. After that, make the binarized logistic sequence perform bitwise XOR with the watermark w, and obtain an encrypted watermark sequence $w_e = w_1 w_2 \dots w_n$;

(2) Convert the first character in the sequence w_e to the decimal ASCII code form (indicated by d);

(3) Using Shamir-based secret sharing improvement algorithm, take appropriate parameter values to divide d, and obtain the shared value d_i (i = 1, 2, ... n). Then, convert d_i into binary form;

(4) Repeat steps (2) and (3), and sequentially obtain the binary sequence of the shared value of each character in w_e;

(5) Group the binary sequences obtained in step (4) in order. Perform RS error correction coding, and generate a new sequence of 0 and 1;

(6) Screen the numerical property value (indicated by q) in the database that satisfies the constraint, and calculate its number index=hash(k2, r.P, A_j);

(7) According to the index value, the lowest bit of the least significant bit of each q is replaced with the 0, 1 sequence generated in step (5).

The watermark embedding process is shown in Figure 1:

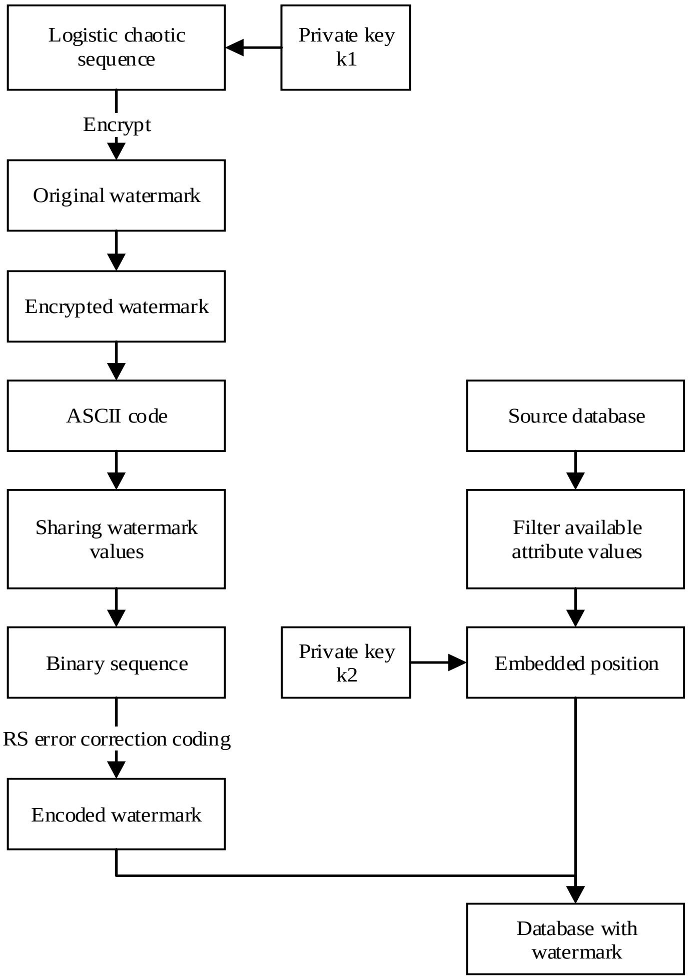

Figure 1. Watermark embedding flow chart

3.3 Watermark extraction algorithm

The recovery of the watermark information is performed character by character. When a character is restored, as long as ≥k(k≤n) of the shared values are accurately extracted, the watermark character can be accurately restored.

The watermark extraction steps are as follows:

(1) Find the numerical attribute value q in the database that satisfies the constraint, and calculate its number index=hash(key, r.P, A_j);

(2) According to the index value, sequentially extract the lowest bits of the least significant bits of each q, and obtain a binary sequence;

(3) Decodethe binary sequence obtained in the step (2) by using RS error correction, and obtain the sharing stored value of each component. Select the highest ksharing values of each component for recovering the watermark characters, and obtain the information sequence w'.

(4) Generate a unipolar logistic sequence L with the private key*k* as the initial value, and select the front $|w'|$ bit of L. Then, binarize L by setting a threshold, and make the binarized logistic sequence perform bitwise XOR with the watermark w. After that, obtain the decrypted binary sequence $w'_d = w'_1 w'_2 \ldots w'_n$ and convert it into watermark information.

The watermark extraction process is shown in the figure 2:

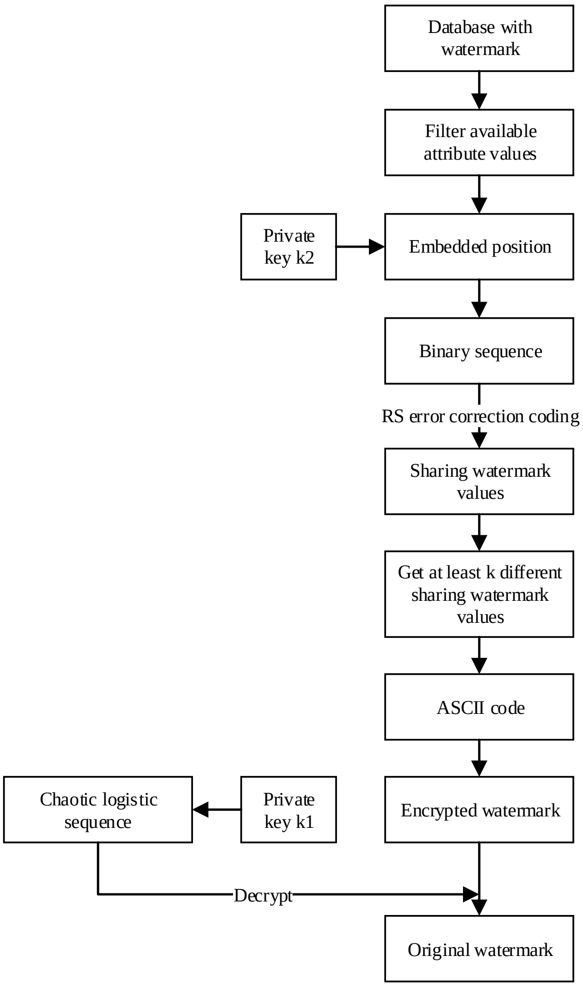

Figure 2. Watermark extraction flow chart

4. Experimental results and analysis

In order to verify the effectiveness of the proposed sharing watermarking algorithm, we conducted experiments on the home user smart meter database, which is selected bythe energy regulation committee [15] from the Irish Power Company. These data record the user's electricity load data every 30 minutes from July 14, 2009 to December 31, 2010. In this paper, the smart meter data of 3,000 home users at 8 moments is randomly selected as experimental data.

The hardware environment is composed of processor frequency 2.1GHz, 4GB memory, 750G hard disk, and Windows 10 operating system. The software environment is consist of Microsoft Visual C++ 6.0, and SQL Server 2008.

We have set the experimental parameters as L=3, secret key k1=256, k2=2464, x_0=0.236, μ=3.97465, k=4, n=8, and the watermark information is "watermark".

In order to test the robustness of the IDR privacy protection method based on sharing watermarking, the experiment will perform several common attacks on the relational database with the watermark added by the algorithm, including subset deletion attack, subset replacement attack and subset addition attack. The experimental results are shown in Figures 3, 4 and 5.

4.1 Subset delete attack

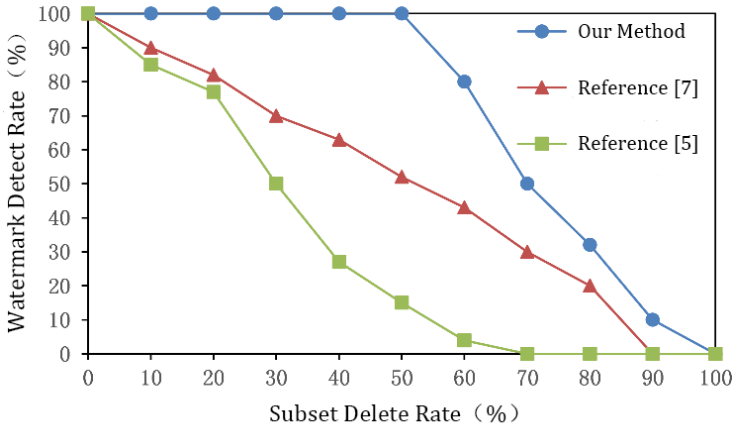

Figure 3. Subset delete attack

It can be seen from Fig. 3 that as the subset deletion rate increases, the watermark detection rates of the three algorithms decrease. When the subset deletion rate is less than 50%, the proposed algorithm can completely recover the watermark information. When the subset deletion rate is greater than 50%, the watermark detection rate of the proposed algorithm is higher than the other two algorithms. It is obvious that the proposed algorithm has strong robustness against the subset deletion attack.

4.2 Subset replacement attack

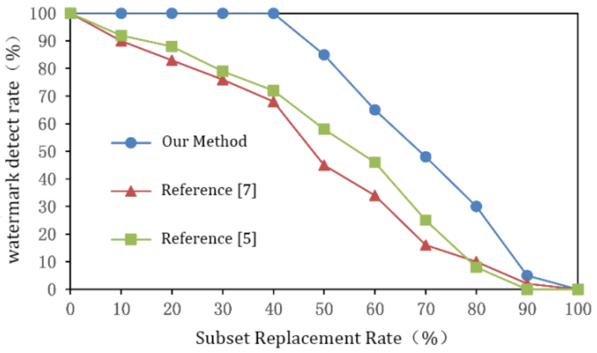

Figure 4. Subset replacement attack

It can be seen from Fig. 4 that as the subset replacement rate increases, the watermark detection rates of the three algorithms decrease. When the sub-group replacement rate is less than 40%, the proposed algorithm can completely recover the watermark information. When the sub-group replacement rate is greater than 40%, the watermark detection rate of the proposed algorithm is higher than the other two algorithms. It is obvious that the proposed algorithm is robust against subset replacement attacks. This is because the Shamir-based secret sharing improvement algorithm is used when watermark embedding. When extracting watermarks, only k can be used to reconstruct the embedded watermark, so that the proposed algorithm can still completely extract complete watermark information when replacing a large amount of data.

4.3 Subset add attack

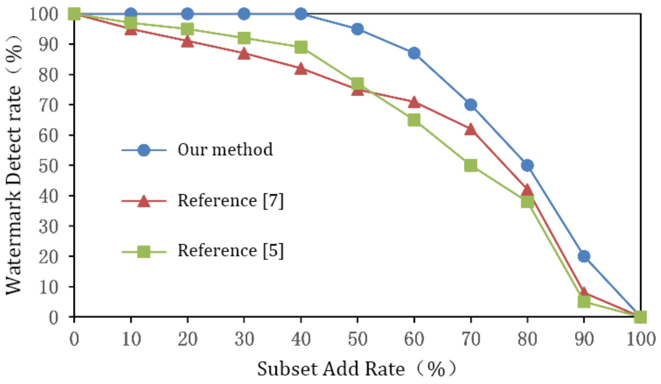

Figure 5. Subset add attack

It can be seen from Fig. 5 that as the addition rate of the subset increases, the watermark detection rates of the three algorithms decrease. When the sub-set addition rate is less than 40%, the proposed algorithm can completely recover the watermark information. When the sub-set addition rate is greater than 40%, the watermark detection rate of the proposed algorithm is higher than the other two algorithms. It is obvious that the proposed algorithm has strong robustness when adding attacks against subsets.

Finally, the proposed database digital watermarking algorithm and the encryption method AES are compared. The experimental results are shown in Figure 6:

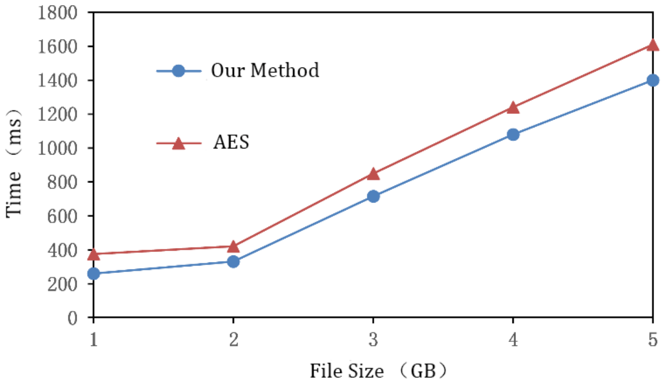

Figure 6. Database watermarking and encryption time comparison

It can be seen from Fig. 6 that, compared with AES, our database digital sharing watermarking algorithm has lower computational overhead and achieves the same effect, with less system overhead, avoiding user privacy leakage and ensuring database integrity.

5. Conclusion

For the issue of IDR privacy protection, we have proposed a method based on sharing watermarking to protect user private data, and avoid user privacy leakage. In our method, we proposed an improved Shamir-based secret sharing algorithm to store the watermarks. The method can use small part of the watermark to restore the whole information, and better defend against multiple forms of attacks in the database. We combined database digital watermarking algorithm with the improved Shamir-based secret sharing algorithm, and proposed the strategy of IDR privacy protection. Our method not only can protect the private data of users in dataset, but also ensure the database integrity authenticated. The comparative experiments show that our sharing watermarking method is robust and safe. Meanwhile, the computational overhead of the method is also small.

References

[1]. M. Shafie-khah, P. Siano, and J. P. S. Catalao, "Optimal Demand Response Strategies to Mitigate Oligopolistic Behavior of Generation Companies using a Multi Objective Decision Analysis," IEEE Transactions on Power Systems, vol. PP, pp. 1-1, 2017.

[2]. H. Mortaji, S. H. Ow, M. Moghavvemi, and H. A. F. Almurib, "Load Shedding and Smart-Direct Load Control Using Internet of Things in Smart Grid Demand Response Management," IEEE Transactions on Industry Applications, vol. 53, pp. 5155-5163, 2017.

[3]. A. Eshraghi, M. Motalleb, E. Reihani, and R. Ghorbani, "Frequency regulation in Islanded microgrid using demand response," in 2017 North American Power Symposium (NAPS), 2017, pp. 1-6.

[4]. GONG Kangli， ZHANG Xueping. Research of digital watermarking technology for relational

database[J]. Computer Technology and Development，2013，23(3)：125-128.

[5]. LIU Weiqun, Research on Digital Watermarking Algorithm Based on Independent Component Analysis[D], Central South University, 2009.

[6]. ZHENG Guangming, and SUN Xingming, Relational Database Digital Watermarking Based on Error Control, Computer Engineering and Applications, pp. 166-168+203, 2005.

[7]. PAN Jifang, LI Junyi, and XIANG Yue, Research on Watermark of Reed Solomon Code Database, Computer Engineering and Applications, pp. 156-159, 2010.

[8]. WANG Zhen, LI Jianmin, ZHOU Nanrun, and LIN Zhenrong, Relational Database Digital Watermarking Algorithm Based on Separated Grouping, Communication technology, pp. 132-134+138, 2009.

[9]. ZHANG Linfang, Database Digital Watermark Research[D],Hunan University, 2006.

[10]. XIA Ting, Database Watermarking Technology Based on Wavelet Transform and Independent Vector Analysis, Journal of North China University of Technology, pp. 13-17+27, 2010.

[11]. T. Veugen, "Linear Round Bit-Decomposition of Secret-Shared Values," IEEE Transactions on Information Forensics and Security, vol. 10, pp. 498-506, 2015.

[12]. S. Kyriakopoulos, T. Tzouramanis, and Y. Manolopoulos, "The dbMark: A benchmarking system for watermarking methods for relational databases," in 2017 11th International Conference on Research Challenges in Information Science (RCIS), 2017, pp. 110-119.

[13]. SHAMIR A. How to share a secret[J].Communications of the ACM, 1979, 22(11):612-613.

[14]. Y. Şahi□n, G. Ulutaş and M. B. İmamoğlu, "An effective database watermarking method based on histogram of pairs," *2016 24th Signal Processing and Communication Application Conference (SIU),* Zonguldak, 2016, pp. 353-356.

[15]. Commission for Energy Regulation (CER). (10 July 2015). Smart Metering Trial Data Publication. Available online: http://www.cer.ie/electricity-gas/smart-metering (accessed on).