FINGERPRINTING ALGORITHM BASED ON THE FIGURE'S COLLUSION DATA BASE

[1]HUIFEN HUANG, [2]DEFA HU

[1]Department of Computer, Shandong Yingcai University, Jinan250104, Shandong, China
[2]Department of Information, Hunan University of Commerce, Changsha 410205, Hunan, China

ABSTRACT

Under the application occasion of using data base as the soft products publication, there should be corresponding safety system, which could abstain the privacy actions from the betray users. A privacy tracing and solution resolution is raised in this thesis based on the digital fingerprinting relationship data base. Data fingerprinting database, which combined by patent watermarking and user's fingerprint in chaotic binary sequence, is imbedded into the data base under the control of encryption key. Based on the chaotic binary sequence's randomness, to abstract the fingerprinting and trace the betrayer. The plan has strong conclusion safety, at the same time lower the fingerprinting inspection and betray tracing algorithm complexity. The thesis describes the data base fingerprinting encode, embedment, fingerprinting inspection and abstraction algorithm, analyzes the algorithm's robustness and betray tracing ability, and has experiment testimony.

Keyword: *Relationship Data Base, Digital Fingerprinting, Collusion Safety, Betray Tracing*

1. INTRODUCTION

At present, there are many application systems give the data base to end users, which is treat as part of the soft. For example, geographic data base is usually included in the vehicle loaded GPS guide system. Another example, the companies, who are keen on map searching engineering exploration, would usually distribute the maps data base to the major web searching engineering website, such as baidu, Google, Yahoo etc. The data publisher would expect, not only the privacy data base must be undergone the patent identification, but also the collusion privacy actions could be abstained, the privacy roots could be test out, the betray behavior's protocol users could be traced from privacy copy. It requires there would be a mark to each protocol user in the carrier data base, once the privacy data is test out, the roots of privacy could be traced according to the abstracted unique remarks. The data base fingerprinting technology, which has anti collusion ability, could meet this safety requirements.

Digital fingerprinting technology embeds the iconic identification code digital fingerprinting, which corresponds to specific user corresponding, to each of the distributed digital copy, it makes the copy unique. When the digital works are detected to be broadcasted illegally, the illegal copy roots could be confirmed by abstracting privacy copy's digital fingerprinting, realize the betray tracing to the protocol users.

2. RELATIVE WORKS

2.1 Digital Fingerprinting

Digital fingerprinting mainly solves the problems of end user's encoding and tracing, strengthening fingerprinting conclusion safety ability to conclusion attacks. The beginning fingerprinting researches focus on anti conclusion fingerprinting encoding theory research. G. Blakley etc. published thesis in the CRYPTO meeting in the year 1985, is one of the first references, which explained anti conclusion fingerprinting concepts. Digital watermarking expert LCox. Etc combined the digital fingerprinting theory and digital watermarking, raised the constant finger printing coding based on random sequence and discussed the conclusion safety performance [1].

Diverse fingerprinting is usually built on the basis of algebraic structures encoding. The most remarkable diverse digital fingerprinting encoding is raised by D. bones and J. Shaw [2]. This plan is built on the basis of Marking Assumption, which assumes the conclusion enemy could only amend each other's work data's different value's corresponding location. At the same time, a Logarithmic Length C-secure Code is formulated, fingerprinting code length and users number's logarithm collusion tolerance size's proportional to the 4th power.

J.Ferrer et al raised an anti collusion encode based on robust watermarking algorithm in the year 2000, resist two collusion attacks [3]. F.Zane raised a double deck C safety encode, combine the inner liner's Cox watermarking code and out liner's mistakes correction code and adopt the minimum distance to keep watermarking anti collusion performance [4] W. Trappe etc made use of special combination, based on BIBD method, raised an anti collusion fingerprinting encode plan[5].

At present, the scholars in and aboard [6-8], whose research to digital fingerprinting encode is getting deeper and deeper, the hot points focus on the beta length, collusion tolerance size and algorithm efficiency, to find the balance point. In order to increase the algorithm efficiency, there is need to under a certain collusion tolerance size, reduce users' beta length and wide the remarks assumption. At the same time, change the tracing algorithm efficiency is also the current digital fingerprinting encoding research hot topic.

2.2 Data Base Fingerprinting

Since the year 2004, some scholars began to focus on the research, which related to the data base fingerprinting technology and get some initial results.

Japanese scholar K.Yoshioka et al reported a relationship for the first time in the year 2004, data base digital fingerprinting solve resolution [9].This plan, embeds some different Stealth Records to each of the distributed copy in the carrier data, as digital fingerprinting. The birth of the Stealth Records meets the restriction terms of data useable, and use the binary collusion safety encode to realize the trace to privacy actors. Under the restriction terms of keeping the data integrity, the French scholar C.Con- stantin etc made reaches to digital fingerprinting algorithm [10], which suitable to data base and XML file; to abstract the carrier data useable terms into a group of restriction rules; To search the premium finger printing embedment carrier by adopting Integer Linear Program, ILP as short, realize the tracing to the static carrier data's fingerprinting embedment and privacy tracing by combining collusion safety encoding.

Till now, the most complete reference, which discuss data base fingerprinting algorithm, is the thesis published by Singapore scholar Y. Li Fingerprinting Relational Databases -Schemes and Specialties". The thesis takes use of R.Agrawal s relation data base watermarking algorithm [11] to detect the carrier data's watermarking remark location and record value, to get the anti collusion fingerprinting code from the publisher's encryption and user sequence No., have exclusive operation

Seen from the current search situation, the in and aboard digital fingerprinting technology study is still at the very first step. The current data base fingerprinting plan is only limited in the symmetrical fingerprinting system's research. To find a balance point between the system safety and useable is the key to database fingerprinting technology.

3. COLLUSION SAFETY'S DATABASE FINGERPRINTING ALGORITHM

The algorithm takes the chaotic binary sequence born from patent encryption respectively as patent watermarking signal and fingerprinting embedment control signal. The chaotic binary sequence born from user encryption is looked as user fingerprinting. Patent watermarking and user fingerprinting combined into data base fingerprinting, embed into data base under the fingerprinting control signal. The fingerprinting test has two procedures: patent judge and fingerprinting abstract. For the suspected privacy data base, first use the patent encryption to make watermarking test. For the judged privacy data base, to abstract user fingerprinting by user encryption, trace the roots of privacy according to betray tracing algorithm.

3.1 Collusion Safety Fingerprinting Encode

The algorithm's fingerprinting taken from the random concrete sequence which obey the normal $N(\mu,\sigma^2)$, n user's system fingerprint information is $\{\mathrm{w}_1,\mathrm{w}_2,\cdots,\mathrm{w}_n\}$. In reference [12], the plan characteristics is taken, in order to reduce the fingerprinting receptiveness, increase the test efficiency, not relative to each other.

Definition 1 Make $\sum'$ to represent beta $\sum$ length is l's beta group, (l,h) fingerprinting beta menas function $\mathrm{E}(u)$ reflect $u(1\le u\le n)$ to $\sum'$, n sequences consist of code group.

Definition 2

Assumption $T=\{w^{(1)},\mathrm{w}^{(2)},\cdots,\mathrm{w}^{(n)}\}$ is a (l,n) fingerprinting code, and $C=\{u_1,\mathrm{u}_2,\cdots,\mathrm{u}_c\}$ is c

users' collusion collection. If all the betas in C has same value at the location it, $w_i^{(u_1)} = \mathrm{w}_\mathrm{i}^{(u_2)} = \cdots = \mathrm{w}_\mathrm{i}^{(u_c)}$, location I is non inspected location and it could not be amended, only the not non impenetrable location could be amended. Formulate the beta group born from collusion group C :

$$T(C) = \left\{ \left(x_1, \mathrm{x}_2, \cdots \mathrm{x}_l \right) \in \Sigma' \middle| x_j \in W_j, 1 \le \mathrm{j} \le l \right\} \quad (1)$$

Among it,

$$W_j = \begin{cases} \left\{ w_j^{(u_1)} \right\}, \mathrm{w}_\mathrm{j}^{(u_1)} = w_\mathrm{j}^{(u_2)} = \cdots = w_j^{(u_c)} \\ \left\{ w_j^{(u_i)} \middle| 1 \le i \le c \right\} \cup \{ \perp \}, \text{otherwise} \end{cases} \quad (2)$$

Among it, $r = 10$ is erasing remarks.

Known from the remarks assumption, collusion users compare their copy, they could only find part of the fingerprinting at the point of (copy different place (testable location), for any other place, collusion user could not find the fingerprinting. Under the terms that data useable, collusion user could not change non inspecting location fingerprinting information, which supplies reference to betray tracing.

The algorithm rose binary collusion safety fingerprinting used as data base fingerprinting basic code, combined with the data base patent watermarking, get a kind of fingerprinting code suitable to data base.

This algorithm fingerprinting code based on the remarks assumption, control through using the pseudo random sequence's repeat embedment to fingerprinting beta, realize a anti collusion ability under certain mistake rate.

The algorithm's encoding idea implied below:

(1) Each of the users is distributed with a length l's random binary beta, each beta repeat m times, beta total length of each user $L = l \times m$. Call each beta original repat embed m beta is a block.

(2) Data publishers choose a random seed number for each user, use seudo random number generator born seudo random sequence to control which beta should be embed after negated in the repeat beta.

(3) During the betray tracing, the data publiser abstract the fingerprinting location beta from the illegal copy, and revert by using control pseudo random sequence. If the users takes part in the collusion, because the illegal copy beta includes the collusioner's information at the non inpestion location, then in the blocks there would be situation "0" or "1" takes the advantage. For the good users,only if the seudo random sequence has good randomness and the m value is big enough, then the reverted block are balance and average. This encode algorithm could effectively trace the illegal publiser under a suitable collusion size.

3.2 Fingerprinting Born and Embedment

This algorithm confirms the fingerprint location data via publishers' patent encryption and data base original group main keys together, makes user fingerprinting by user encryption, and combines patent watermarking into data base finger printing. Because all the database copy uses same patent encryption, so among all the data base copy, different data base fingerprinting has same fingerprinting embedment location, meets the remarks assumption. Amend the decimal low figures parity by modifying the numeric attributes get fingerprinting carrier way under the premise of meeting certain accuracy and usability.

Definition 3 Assumption data base relationship is $R\left(P, A_1, \cdots A_j, \cdots A_v\right)$, among it, P is main key, $A_j\left(1 \le j \le v\right)$ is R original group, $r_i \cdot A_j$ is original group r_i characteristic A_j 's value. If $A_j\left(1 \le j \le v\right)$ is R 's number value characteristic, and A_j 's value accuracy has certain redundancy at the value lower location call A_j to be standby characteristic.

In order to simplify the discretion, assume all R's characteristic $A_j\left(1 \le j \le v\right)$ is into standby characteristic. At the same time, assumption the main key P in R could not be amended.

Definition 4

Standby characteristic $A_j\left(1 \le j \le v\right)$ exists accuracy redundancy. Assume is A_j standby location number ξ_j , each of the standee location number from high to low is $d_{\xi j}, \mathrm{d}_{\xi \mathrm{j\text{-}1}}, \cdots \mathrm{d}_1$.

Leering from the Definition, data base relation $R\left(P, A_1, \cdots A_j, \cdots A_v\right)$ real embeddable watermarking carrier, is standby characteristic $A_j\left(1 \le j \le v\right)$'s is $d_{kj}\left(1 \le k_j \le \xi_j\right)$.

Definition 5

Standby characteristic $A_j\left(1\le j\le v\right)$ within the useable limits the tolerable percentage is A_j allowable tolerance marks ξ_j .

Take the user u published data base copy as an example, the fingerprinting birth and embed algorithm as follow:

Input patent encryption K_c , take $NRM(K_c)$ initial value get Logistic chaotic binary value sequence $c\left[l_1+1+m\right]$:

$$\begin{aligned} w\left[l_1\right] &= c\left[l,\mathrm{l}_1\right] \\ e\left[l_1\right] &= c\left[l_1+1,\mathrm{l}_1+1\right] \\ r\left[m\right] &= c\left[l_1+l+1,\mathrm{l}_1+1+\mathrm{m}\right] \end{aligned} \quad (3)$$

Input user encryption K_u , take $NRM(K_u)$ as initial value get Logistic chaotic binary value sequence $pp\left[l_2\right]$:

$$p\left[l\right]=\left\{w\left[l_1\right]\ ,\mathrm{pp}[\mathrm{l}_2]\right\} \quad (4)$$

Repeat each original group $r_i\left(1\le i\le n\right)$ of R

If $LGS\left(NRM\left(K_c\|P_i\right)\right)\bmod r=0$,then

$$\begin{aligned} k &= NXT\left(LGS\left(NRM\left(K_c\|P_i\right)\right)\right)\bmod 1+1 \\ q &= NXT\left(LGS\left(NRM\left(K_c\|P_i\right)\right)\right)\bmod 1+1 \\ p\left(k\right) &= p\left(k\right)\oplus r\left(q\right) \\ j &= NXT\left(LGS\left(NRM\left(K_c\|P_i\right)\right)\right)\bmod v+1 \\ d &= NXT\left(LGS\left(NRM\left(K_c\|P_i\right)\right)\right)\bmod \xi\left(j\right)+1 \end{aligned} \quad (5)$$

If $r_1\cdot\delta\left(j\right)\ge 10^{d\text{-}1}$, then confirm standby location do's value by $\left(P\left(k\right),\mathrm{e}\left(\mathrm{k}\right)\right)$ and updates $r_1\cdot A_j$.

In the algorithm 1, l_1 is the patent watermarking length, l_2 is user fingerprinting length, m is fingerprinting retro control sequence length, data base copy fingerprinting beta length $l=l_1+l_2$. r is the interval value of original group mark. $\xi\left[v\right]$ is each standby characteristic's stand by location number group, $\delta\left[v\right]$ is each standby characteristic's allowable tolerance group. Number group $\xi\left[v\right]$, $\delta\left[v\right]$ and remark interval value r and patent encryption K_c and user encryption K_u ,form together the input parameter,form the system's complete encryption. Logistics $NMR\left(x\right)$ deals to x through normalizations deal, $0\le NMR\left(x\right)\le 1$. Logistic $LGS\left(x\right)$ takes x as Logistic Formula's initial valued to birth the random chaotic sequence, and take off the point, deal the sequence value as round figures. Logistics $NXT\left(LGS\left(x\right)\right)$ takes one of the values from chaotic sequence. Logistic chaotic sequence born algorithm refer to the [11]. Make 0 to the values in chaotic sequence, which is smaller than 0.5, other side, make it 1, give birth to pseudo random binary value sequence.

Take patent encryption to give birth to chaotic two value sequence take chaotic sequence's sub sequence as patent watermarking remarks $w\left[l_1\right]$ respectively fingerprinting embedment strategic control signal $e\left[l\right]$, and fingerprinting retro control signal $r\left[m\right]$.Take user encryption to give birth to chaotic binary sequence as user's personal fingerprinting $pp\left[l_2\right]$ .Patent watermarking $w\left[l_1\right]$ and user personal fingerprinting $pp\left[l_2\right]$ location connect to be data base copy basic fingerprinting beta $p\left[l\right]$.

During the fingerprinting embed process, patent encryption K_c and current original group main key P_i together confirm the pending embed basic fingerprinting code $p\left[l\right]$'s corresponding location the embed location according to fingerprinting take retro control signal $r\left[m\right]$ and adjust basic fingerprinting code embed value at the same time according to the allowable tolerance's requirements to judge whether the embed or not. For the confirmed stand by location, amend the stand by location deity to embed fingerprinting, according to the corresponding embed strategic control signal location.

It is easy to learn under the situation that all the standby location meet embed terms, when the embeddable standee location is bigger than the copy fingerprinting code matrix $P\left[m,l\right]$'s factor number, this algorithm realizes the finger printing's repeat embedment the repeated embedment times of fingerprinting matrix is

$$rep = floor\left(\frac{n}{r \times m \times l}\right) \qquad (6)$$

Among it, $floor(x)$ is into function, no bigger than x round figures.

3.3 Collusion Inspection

The thesis uses two inspection methods: the maximum value inspection and threshold inspection. These two inspections, when the publisher finds ill eagle copy, under the situation of non blind inspection, abstract the fingerprinting information from ill eagle copy, make relevant calculation inspects to all the users' fingerprinting information in the database.

Here use a T_N to reserve each of the relevant value the j user's relevant value formulated as:

$$T_N(j) = \frac{(y\text{-}x)^T w_j}{\sqrt{\sigma_d^2}\,\|w_j\|} \qquad (7)$$

（1）The maximum value inspection

Considering that if more and more collusion are traced, more and more innocent users would be mistaken. The maximum inspection is to trace only a situation, and then this user's mistaken rate is very low. After calculation to the relevant value of all the user fingerprinting and collusion fingerprinting, make compurgation to the maximum value and threshold, if the maximum value is bigger than the threshold, then this relevant value is maximum value's user must be the collusion. The definition represents:

Assume the collusion group is the first $1,2,3,\cdots,k$ user, collusion group is represented by S_C , user number n .

$$T\max = \max_{j=1}^{n} T_N(j) \begin{cases} j = \arg\max_{j=1}^{n} T_N(j) & if \quad T_{\max} \ge h \\ j = \varphi & if \quad T_{\max} \prec h \end{cases} \qquad (8)$$

The algorithm's performance:

False alarm rate:

$$\begin{aligned} p_{fp} &= p\{T_{\max} \succ h, j \notin S_C\} = p\{T_1 \prec T_2, T_2 \succ h\} \\ &= p(T_1 \prec h, T_2 \succ h) + p(T_1 \prec h, T_2 \succ T_1) \\ &= p(T_2 \succ h)\, p\{T_1 \prec h\} + \int_h^\infty p\{T_2 \succ T_1\}\, p(T_1)\, dT_1 \end{aligned} \qquad (9)$$

Among it, $T_1 = \max_{j=1}^{K} T_N(j)$, $T_2 = \max_{j=n+1}^{n} T_N(j)$, $p(T_1)$ is random variables T_1 Probability Density Function.

Inspection rate:

$$\begin{aligned} p_d &= 1\text{-}p_{fn} = p\{T_{\max} \succ h, j \in S_C\} \\ &= p\{T_1 \succ T_2, T_1 \ge h\} \\ &= p\{T_1 \ge h\}\, p\{T_2 \prec h\} + \int_{j=n+1}^{n} p\{T_1 \succ T_2\} p(T_2)\, dT_2 \end{aligned} \qquad (10)$$

Among it: because the orthogonal finger printing relative value.

$$T_N(i) = \begin{cases} N\left(\frac{\|w_i\|}{k}, \sigma_d^2\right) & if \quad j \in S_C \\ N(0, \sigma_d^2) & if \quad otherwise \end{cases}$$

$$p(T_1 \le l) = \left(1\text{-}Q\left(\frac{l\text{-}\frac{\|w\|}{k}}{\sigma^d}\right)\right)^k \qquad (11)$$

Because:

$$p(T_2 \le l) = \left(1\text{-}Q\left(\frac{l}{\sigma^d}\right)\right)^{n\text{-}k} \qquad (12)$$

Among it:

$$Q(l) = \int_l^\infty \frac{1}{\sqrt{2\pi}} e^{\frac{x^2}{2}} dx \qquad (13)$$

(2) Threshold inspection

From the point of publisher, it is better to trace as much as possible collusion while keep the false alarm rate lower. Threshold inspection method is to trace all the possible collusion. After calculation to all the users' relevant value, if this users' relevant value is bigger than certain gate limits value, then the user is deemed to join illegal copy abbreviation.

$$j = \arg_{j=1,2,\cdots,n} \{TN(j) \ge h\} \qquad (14)$$

This algorithm's performance:

False alarm rate:

$$pf_p = p\left\{ j \cap \overline{S}_C \neq \varphi \right\} = 1-\left(1-Q\left(\frac{l}{\sigma^d}\right)\right)^{n-k} \qquad (15)$$

Inspection rate:

$$p_d = 1-p_{fn} = p\left\{ j \cap S_C \neq \varphi \right\} = 1-\left(1-Q\left(\frac{h-\frac{\|w\|}{k}}{\sigma^d}\right)\right)^{k} \qquad (16)$$

3.4 Algorithm Analysis and Choice

Learn from the above inspection rate and the false alarm rate definition: the most important is the threshold value's assumption in these two inspection methods. If the threshold value's assumption is too big, although there are much collusion is traced out, but the false alarm rate is high; if the threshold value's assumption is too small, the false alarm rate is lower, but there are many collusion is missed. But under general situation, while we are keeping the false alarm rate smaller, (general set it 0.01) trace as many as possible collusion.

The specific threshold calculation method as below:

During the threshold inspection:

$$p_{fp} = 1-\left(1-Q\left(\frac{l}{\sigma^d}\right)\right)^{n-k} = 0.01$$
$$\Rightarrow h = \sigma_d \cdot Q^{-1}\left(1-0.99^{\frac{l}{n-k}}\right) \qquad (17)$$

Different threshold could be set under differ collusion group according to the above definition, thus ensure the false alarm rate is 0.01 to trace as many as possible collusion.

The algorithm is easy to realize on coding, inspection algorithm is also easy, has well anti collusion performance, but the encode efficiency is not high, maximum 1. When the user number is very big, beta length is long; the system reservation number is also big.

4. EXPERIMENTAL RESULTS

The experiment adopts Forest Cover Type data base group. This data base group in the form of binary sheet's form described the forest coverage situation in USA 1999, take 571912 inspection points, total 54 characteristics, all are value type. Take the first 10 characteristic as experimental data, transform them into MS SQL Server data base, and add the inspection point number to be main key.

Experiment 1

Fingerprinting robust characteristic attacks. Take the fingerprinting embedment original group remarks interval value $r=10$ .Embed fingerprinting into the database by different fingerprinting basic code length take retro control sequence length. For the obtained fingerprinting included data base copy, takes random value replace 50% data base original group. After attacked data base copy's fingerprinting inspection rate as figure 1 shows.

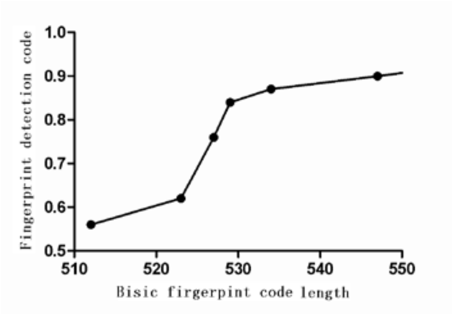

Figure 1: Fingerprinting Inspection Rate To Sub Group Replace Attacks

Random sub group replacement attacks has higher robustness, under the sub group replacement attacks, fingerprinting inspection rate will become low as the embedded fingerprinting factor's growth. Notice that when the fingerprinting basic beta length is 512, fingerprinting takes retro control sequence length is 235, system robustness comes down greatly under the sub group replace attacks. This is because the factors number of fingerprinting commix already overgrows experimental data base group, under which term when the original group interval value is 10, could supply fingerprinting embed location number. This also gives the restrict term from the other point of view to carrier data base choice and the basic fingerprinting beta, fingerprinting take retro control sequent size choice.

Experiment 2

collusion attacks and betray tracing. Take the data base patent watermarking length 16, use fingerprinting encode length $T_2 = 128$, fingerprinting retro control sequence length $m = 64$,fingerprinting embedment original group remarks interval value $r = 10$, take 4 different user encryption to obtain 4 different fingerprinting included data base copy. To intimate collusion attacks by using different user number, examine under the different collusion number advantage beta rate and the judge able beta original rate change situation. The experiment results shown as the figure 2.

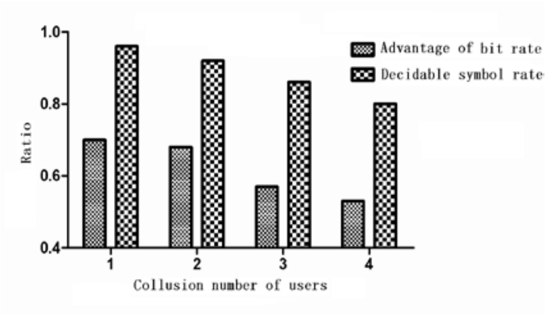

Figure 2: The Different Collusion User Number's Finger Printing Inspection

Learn from the figure 2, fingerprinting inspection advantage beta rate decreases as the collusion user number's growth, the judge able beta original rate also comes down accordingly. Learn from the experiment results, this fingerprinting plan has higher fingerprinting inspection rate and betray tracing accuracy rate when the collusion user number is within 4 fingerprinting attacks.

5. CONCLUSION

This thesis raises a kind of data base fingerprinting encode plan and relevant algorithm combined with patent watermarking, realize the betray tracing to the privacy data base copy. This plan has higher collusion safety, compare with the current data base fingerprinting plan, it keeps higher fingerprinting inspection rate and betray tracing accuracy, lowers fingerprinting inspection rate and betray tracing calculation complexity.

ACKNOWLEDGMENTS

This work was supported by Ministry of Science and SME Technology Innovation Fund (12C26243704086), Natural Science Foundation of Shandong Province (ZR2012FQ006), Colleges and universities in Shandong Province scientific research plan (J12LN58) and National Natural Science Foundation of China(61202464).

REFERENCES:

[1] Cox I J, Kilian J, Leighton F T, et al, "Secure spread spectrum watermarking for multimedia", *IEEE Trans. on Image Processing*, Vol. 6, No. 12, 2007, pp.1673-1687.

[2] Boone D, Shaw J, "Collusion Secure Fingerprinting for Digital Data", *IEEE Trans. Information Theory*, Vol.44, No. 5, 2008, pp. 1897-1905.

[3] Ferrer J D, Joancomarti J H, "A Simple Collusion Secure Fingerprinting Schemes for Images", *Proceedings of the IEEE International Symposium on Information Technology*, 2009, pp.128-132.

[4] Zane F, "Efficient watermark detection and collusion security", *LNCS Springer Verlag*, 2011, pp. 21-32.

[5] Trappe W, Wu M, Wang Z J, et al, "Anti-collusion Fingerprinting for Multimedia", *IEEE Trans. Signal Processing*, Vol. 51, No. 4, 2003, pp.1069-1087.

[6] Gao Ren, Zhao Yongxiang, Tang Long, "The Research on RSS Filter for Indoor Positioning System Based on Wireless LANs", *Advances in Information Science and Service Sciences*, Vol.3, No.4, pp.1-9, 2011.

[7] Bo Cheng, Xiangtao Lin, Junliang Chen, "Context-Aware Web Services Orchestration for Multimedia Conference Process Management", *Advances in Information Science and Service Sciences*, Vol.3, No.4, pp.59-67, 2011.

[8] Gao Ren, Tang Long, Wu Juebo, "A Novel Recommender System Based on Fuzzy Set and Rough Set Theory", *Advances in Information Science and Service Sciences*, Vol.3, No.4, pp.100-109, 2011.

[9] Yoshioka K, Shikata J, Matsnmoto T, "A Method of Database Fingerprinting", *Proceedings of the 2004 Workshop on Information Security Research*, 2004, pp.120-130.

[10] Constantin C, Gross-Amblardet D, Guerrouani M. Watermill, "an Optimized Fingerprinting Tool for Highly Constrained Data H", *Proceedings of ACM Workshop on Multimedia and Security (MMSec)*, USA, August 2005, pp. 143-155.

[11] Agrawal R, Kieman J, "Watermarking Relational Databases", *Proceedings of the 28th VLDB Conference*, Hong Kong, China, 2002, pp.223-231.