Journal of Information Hiding and Multimedia Signal Processing ©2016 ISSN 2073-4212
Ubiquitous International Volume **7**, Number **2**, March **2016**

A Novel Reversible Watermarking Scheme for Relational Databases Protection Based on Histogram Shifting

Yu-Jia Ma and Yue-Sheng Zhu

Communication and Information Security Lab, Institute of Big Data Technologies
Shenzhen Graduate School, Peking University, Shenzhen, China
zhuys@pku.edu.cn

Xi-Yao Liu

School of Information Science and Engineering
Central South University, Changsha, China
lxyzoewx@csu.edu.cn

Received July, 2015; revised August, 2015

Abstract. *The watermarking technique can be used to protect the ownership of relational databases by hiding some ownership information into the relational databases. In this paper, a novel robust reversible watermarking scheme for relational database protection is proposed to increase the embedding capacity by developing an improved histogram shifting with binary tree structure and an attribute selection scheme. The iteratively embedded watermarks are utilized by a majority voting mechanism to enhance the robustness of the proposed scheme. In addition, the attribute selection and cell selection are employed to reduce the distortion caused by the watermark embedding. The experimental results show that our proposed scheme can provide higher embedding capacity and stronger robustness with low distortion compared with other watermarking schemes for relational databases.*
Keywords: Relational database, Histogram shifting, Watermark embedding, Majority voting mechanism.

1. **Introduction.** The rapid development of internet and related technologies enables easy access to databases. However, it also leads to the increasing of database copyright violation, which is a critical risk to their owners [5, 11]. As a solution to protect the ownership of databases, the watermarking technique hides some ownership information into the databases, and when the copyright needs to be verified, the ownership information can be extracted [8, 9].

Some watermarking approaches for relational databases have been developed in [1, 2, 3, 4, 6, 7, 10, 12, 13, 14, 15, 16, 17, 19]. In the groundbreak work proposed by Agrawal and Kiernan [15, 16] the watermark is embedded into numerical values in relational databases. In the method developed by Sion [12, 13] the watermark bits are hidden in selected tuples of which the modifications have insignificant effects on the contents. In these works, any modification to the watermarked tuples would destroy the whole embedded watermark, which is undesirable for protecting the ownership of databases. In Shehab et al.'s work [10] the robustness to basic attacks such as alterations and deletions is enhanced

by employing an optimization-based technique, but they are irreversible with the modification of the databases contents. Then, a reversible watermarking scheme by using prediction error expansion (PPE) was designed by Farfoura et al. [7] so that the contents of databases can be recovered after the watermark is extracted and detected completely even when 65% of the relational database has been altered. However, this scheme can use the fractional portions of the attributes of databases only. To overcome this limitation, in a semi blind reversible watermarking scheme designed by Chang et al. [1] for database protection, based on the histogram shifting by using pairs of peak and zero points [19], and by employing histogram shifting and majority voting mechanism technique (MVT), the robustness of embedded watermark is improved with a high watermark embedding capacity to ensure the effectiveness. However, this watermark embedding capacity of the scheme depends on the number of peak points and is unstable due to the randomness of the attribute and cell selections. Once the histogram of the data in a database is similar to a uniform distribution, the capacity would always be quite low even multiple pairs of peak and zero points are utilized. Thus, the robustness of the scheme will be impaired seriously. In a watermarking method for relational databases based on genetic algorithm and difference expansion (GADEW) designed by Jawad et al. [6], the drawbacks caused by the random selection of the attributes and cells are alleviated by employing of the genetic algorithm which minimizes the watermark embedding distortions and increases the embedding capacity. However, since the MVT technique is not employed, the high watermark embedding capacity cannot be fully converted to strong robustness of watermarking.

In this paper, a novel reversible watermarking scheme for relational databases is proposed to solve the above-mentioned problems. Rather than the use of the histogram shifting with peak points and zero points in Chang's method [1], the histogram shifting with tree structure [18] is employed in the proposed scheme. In general, the differences between two adjacent data in a same attribute are usually small. This situation is similar to that of two adjacent pixels in one image. Therefore, in our scheme, each attribute is considered similar to an image in Tai's scheme [18], and the watermarks are embedded in an attribute for data restoring by applying the histogram shifting with tree structure. The histogram from both sides are shifted by 2^L to avoid the underflow and overflow in Tai's scheme. But, in our scheme for relational database, the shifting of 2^L is omitted so that both low distortion and high and stable EC are obtained. In addition, new methods of attribute and cell selection are designed in our scheme. By applying the attribute selection method, our scheme not only provides more stable watermark embedding capacity compared with the random selection of attributes in Chang's method, but also reduces the distortion caused by watermark embedding. By applying the cell selection method, the performance of histogram shifting with tree structure can be improved to further reduce the watermark embedding distortion. Finally, the MVT function is employed to convert the high watermark embedding capacity to strong robustness of watermarking. Since the employment of MVT, the robustness of the proposed scheme is stronger than that in GADEW [6]. The robustness of the proposed scheme is also stronger than that in Chang's method [1] by providing higher and more stable watermark embedding capacity which can improve the effect of MVT. Furthermore, since the watermark embedding distortion are reduced by applying both attribute and cell selections, the watermark embedding procedure is imperceptible to the attackers, which can protect the relational databases well.

The rest of the paper is organized as follows: Section 2 introduces the proposed reversible watermarking scheme. In Section 3, the experimental results with respect to

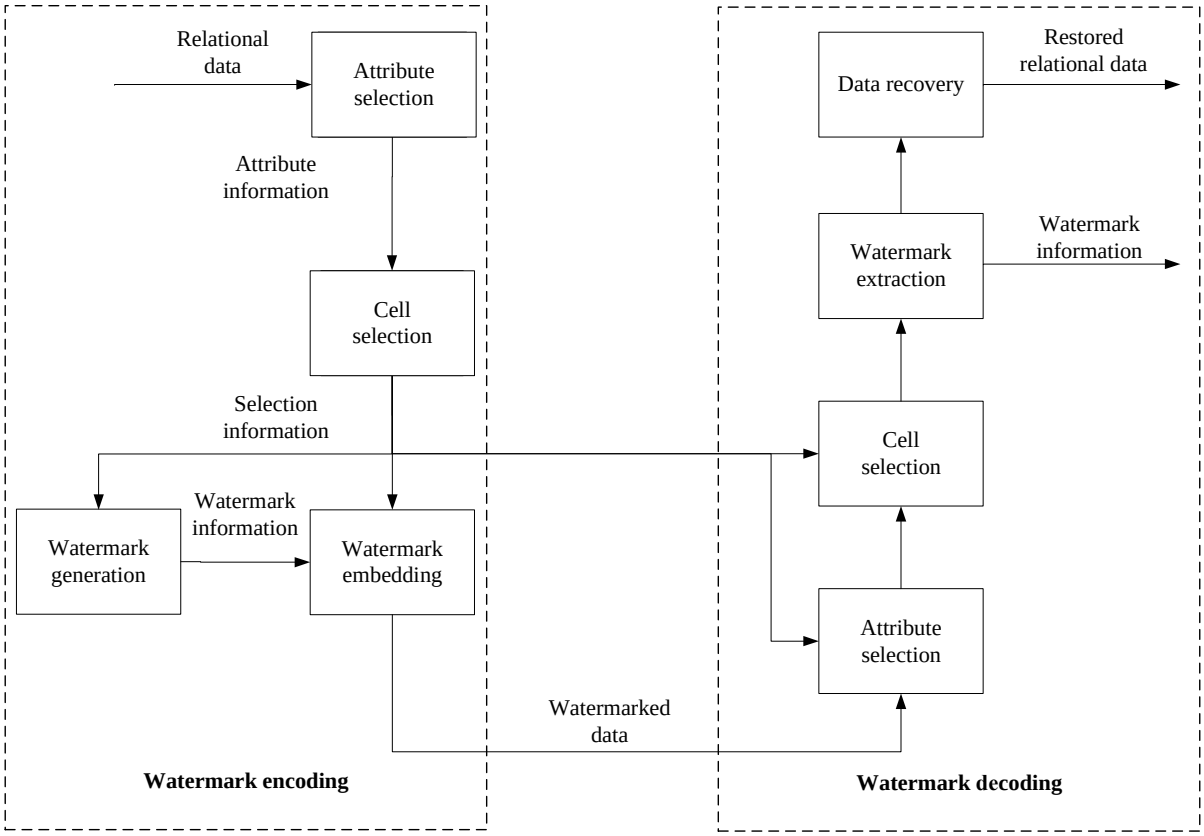

FIGURE 1. Block diagram of the proposed scheme

the embedding capacity, the robustness and embedding distortion are presented. Finally, Section 4 concludes the paper.

2. **The Proposed Scheme.** The block diagram of the proposed scheme is shown in FIGURE 1. In the encoding phase, the attributes and cells which are more suitable for watermark embedding are first selected from the relational databases according to the relational numeric data. Then, by applying our histogram shifting algorithm with tree structure, the generated watermark is embedded according to the above selection information. In the watermark decoding phase, the selected attributes and cells are found out from the selection information. Then the embedded watermark is extracted from the watermarked database. Since the watermark information is embedded several times in the watermark encoding phase, several samples of the watermark information can be extracted in the watermark decoding phase. For each watermark bit, its value is determined by the MVT technique to gain stronger robustness. In the following subsections, the watermark generation, attribute selection, cell selection, watermark embedding and watermark detection are presented respectively.

2.1. **The Generation of Watermark.** To protect the relational database well, the ownership information and database information should both be contained when generating the watermark. In this paper, SHA-1 function is applied to calculate watermark information as below.

$$W = H(K||DBinfo||Ownership) \tag{1}$$

where $||$ indicates the concatenation operator and K is the secret key; $DBinfo$ is the necessary information of database; $Ownership$ represents the owner's information.

2.2. **Attribute Selection.** To select attributes which are more suitable for watermark embedding, an evaluating mechanism is designed which is expressed by three parameters. These three parameters are the watermark embedding capability (EC), the tuple-wise distortion (TWD), and the attribute-wise distortion (AWD). With a score function, attributes can be sorted by their fitness order. When the watermark needs to be embedded, the attributes with the higher scores will be selected prior.

2.2.1. *The capability parameter.* The EC is applied to judge whether the tolerance of one attribute can fulfill the size of watermark information when the embedding level is set to be L. If the size of watermark information is larger than the EC, the attribute should not be used for watermark embedding. The EC is calculated below.

$$d_k = \begin{cases} 2^L, & if \quad k = 0 \\ \mid x_{k-1} - x_k \mid, & otherwise \end{cases} \tag{2}$$

$$WME(W_k) = \begin{cases} 1, & if \quad d_k < 2^L \\ 0, & otherwise \end{cases} \tag{3}$$

$$EC = \sum_{k=1}^{n} WME(W_k) \tag{4}$$

where L is the level of binary tree, x_k is the k_{th} original cell value, the x_{k+1} is the $k+1_{th}$ original cell value. Since the MVT is applied in the proposed scheme, the higher capacity can provide stronger robustness. The attributes with higher EC are considered to be more suitable for watermark embedding to enhance the robustness of watermarking.

2.2.2. *Tuple-wise distortion rate.* In a selected attribute, the values of cells will be shifted if the cell is applied to embed watermark information which causes the tuple-wise distortion (TWD). The TWD affects the relationships of the adjacent cells in the selected attributes. The TWD of each attribute is calculated as below to demonstrate the degree of tuple-wise distortion of the attribute, which can help to evaluate the effects on the relationships of the adjacent cells.

$$distortion_k = \begin{cases} \mid x_k - y_k \mid, & if \quad \mid x_k - x_{k-1} \mid < 2^L \\ 0, & otherwise \end{cases} \tag{5}$$

$$TWD = \frac{\sum_{k=1}^{n} distortion_k}{\sum_{k=1}^{n} |x_k|} \tag{6}$$

where L is the level of binary tree, x_k is the k_{th} original cell value, and y_k is the k_{th} embedded cell value. The attributes with lower TWD are considered to be more suitable for watermark embedding to enhance the imperceptibility of watermarking.

2.2.3. *Attribute-wise distortion rate.* The distortion introduced by the watermark embedding process also affects the relationships among the embedded attributes and their neighbors. As a result, to select the attributes which are more suitable for watermark embedding, the AWD also needs to be calculated as shown in Eq.(7)-(9) for evaluating which can help to evaluate the effects on the relationships among the embedded attributes and their neighbors.

$$distortion_k^{left(right)} = \begin{cases} \left| x_k - x_k^{left(right)} \right|, & if \quad \mid x_k - x_{k-1} \mid < 2^L \\ 0, & otherwise \end{cases} \tag{7}$$

$$AWD = \frac{\sum_{k=1}^{n} distortion_k^{left} + \sum_{k=1}^{n} distortion_k^{right}}{2\sum_{k=1}^{n} \mid x_k \mid} \tag{8}$$

where L is the level of binary tree, x_k^{left} is the left neighbor of x_k and x_k^{right} is the right neighbor of x_k. The attributes with lower AWD are considered to be more suitable for watermark embedding to enhance the imperceptibility of watermarking.

2.2.4. *Evaluating mechanism.* Both the EC and the watermark embedding distortion are related to the tree level L and thus merely pursuit of high EC will lead to the increases of TWD and AWD, which is undesirable. Therefore, it is important to find the balance among EC, TWD and AWD. To achieve the balance, these three parameters are used together in Eq.(10) to calculate the final evaluation score. The Wt and Wa represents the weights of TWD and AWD, which can be determined by empirical value.

$$Eva_{i,L} = \begin{cases} Invalid, & if \quad EC < 160 \\ \frac{EC}{[Wt \times TWD] + [Wa \times AWD]}, & if \quad EC \geq 160 \end{cases} \tag{9}$$

where the subscript i represents the serial number of the attributes and L is the tree level of watermark embedding process. As the SHA-1 function is applied to generate the watermark, the minimum watermark size is 160. After the evaluating process, there will be a table consist of the Eva values. Lager Eva value demonstrates better watermark embedding balance. By sorting the Eva values except the invalid ones in descending order, the attributes which can provide better watermark embedding balance with the corresponding L can be found.

2.3. **Cell Selection.** In the original histogram shifting method with tree structure [18] for watermark embedding, whether the cells are applied to embed watermark information or not, their values are all shifted. However, the cells not applied for watermark embedding require no shifting. Therefore, a large part of distortion can be reduced if the values of cells are not shifted. In our scheme, a cell selection is proposed in which the cells not applied for watermark embedding are omitted to reduce this kind of distortion. A local map is generated to mark the cells which are applied to embed watermark information. Assume the attribute A is one of the attribute selection result, the steps of cell selection are described below.

1) Generate the local map with the primary key attribute information and the attributes names. Scan the attribute A_i, mark the selected cell j with $M_{ij} = 1$.

$$M_{ij} = \begin{cases} 1 & if \quad \mid x_{j-1} - x_j \mid < 2^L \\ 0 & if \quad \mid x_{j-1} - x_j \mid \geq 2^L \end{cases} \tag{10}$$

where L is the level of binary tree, i is serial number of the selected attribute and x_j is the j_{th} original cell value.

2) Compress the local map matrix M losslessly by the run-length coding algorithm. Since the local map consists of 0 and 1, and the number of 0 is usually very large, the run-length coding algorithm can increase the compression ability greatly.

2.4. **Watermark Embedding Process.** For the selected attribute, the embedding process is:

1) Calculate the difference d_j between the adjacent cells $x_j - 1$ and x_j by Eq.(12)

$$d_j = \begin{cases} 2^L, & if \quad j = 0 \\ \mid x_{j-1} - x_j \mid, & otherwise \end{cases} \tag{11}$$

where x_j is the j_{th} original cell value.

2) If $M_{ij} = 1$, embed the watermark bit w to x_j,

$$y_j = \begin{cases} x_j + (d_j + w), & if \quad x_j \geq x_{j-1} \\ x_j - (d_j + w), & if \quad x_j < x_{j-1} \end{cases} \tag{12}$$

where y_j is the watermarked value of x_j.

3) If $M_{ij} = 0$, no watermark bit is embedded and the cell value is unchanged.

2.5. **Watermark Detection.** Given the information of selected attributes and local map M, the procedures of watermark detection are below:

1) Scan the watermarked attribute i and the i_{th} row of local map matrix M, if $M_{ij} = 1$, the watermark information bit w can be extracted.

$$w = \begin{cases} 0, & if \quad \mid y_j - x_{j-1} \mid \quad is \quad even \\ 1, & if \quad \mid y_j - x_{j-1} \mid \quad is \quad odd \end{cases} \tag{13}$$

where y_j is the j_{th} watermarked value and x_{j-1} is the $j - 1_{th}$ original value.

2) If $M_{ij} = 1$, restore the original value x_j.

$$x_j = \begin{cases} y_j + \left\lceil \frac{\mid y_j - x_{j-1} \mid}{2} \right\rceil, & if\ y_j < x_{j-1} \\ y_j - \left\lceil \frac{\mid y_j - x_{j-1} \mid}{2} \right\rceil, & if\ y_j > x_{j-1} \end{cases} \tag{14}$$

3) If $M_{ij} = 0$, no watermark bit is extracted and keep the cell value unchanged.

4) Repeat Step 1 to 3 until all the embedded watermark information bits are completely extracted.

5) Use MVT to reconstruct the watermark. The vector w_j is the different samples of the extracted watermark bit w_j and the n_{wi} is the embedded time of watermark bit w_i. If the size of w_j is larger than $n_{wj}/2$, w_j can be reconstructed as shown in Eq.(16).

$$w_j = \begin{cases} 0, & if\ \frac{Vresult(j,1)}{Vresult(j,1)+Vresult(j,2)} > \tau \\ 1, & else \end{cases} \tag{15}$$

where the $Vresult(j, 1)$ is the number of value 0 in w_j, while $Vresult(j, 2)$ is the number of value 1. The τ is vote parameter.

If the watermark embedding capacity is sufficient, the robustness of watermarking can be improved by applying the MVT.

3. **Results and Discussions.** In this section, three datasets are used in our experiments. One is a Random-dataset(R-dataset) generated by the authors, which contains 10 attributes and 30000 tuples and the values of cells in the relational database is generated randomly ranging from 1 to 100. The other two datasets are the Forest Cover Type dataset (FCT-dataset) and Shuttle dataset which are provided by University of California. The FCT-dataset contains 581012 tuples and 54 attributes while Shuttle contains 58000 tuples and 9 attributes. Their subsets with different numbers of tuples are randomly selected and applied for the experiments to better demonstrate the performances of the proposed scheme and each experiment is repeated 100 times to ensure the accuracy.

3.1. **Capacity Analysis.** If the L is sufficiently large, the capacity of our proposed scheme can be theoretically close to the number of the cells in the selected attributes, but the distortion will be very high. When the L is smaller, the distortion will be lower while fewer attributes can be used for watermark embedding which leads to lower EC and weaker robustness. As a result, for different applications, the L can be chosen to be different values. In this paper, the L is set to be 3 as a tradeoff between the capability and distortion. The comparisons of capacity between our scheme and Chang's scheme [1] are shown in FIGURE 2, FIGURE 3 and FIGURE 4.

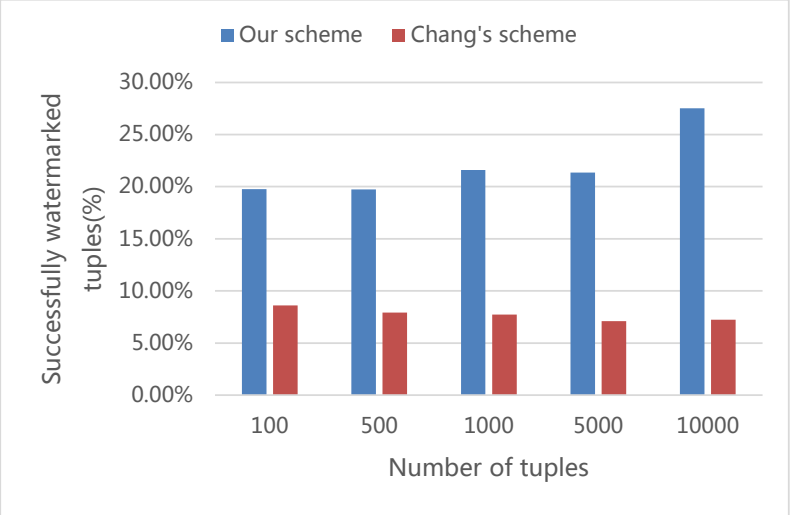

FIGURE 2. Performance on FCT-dataset

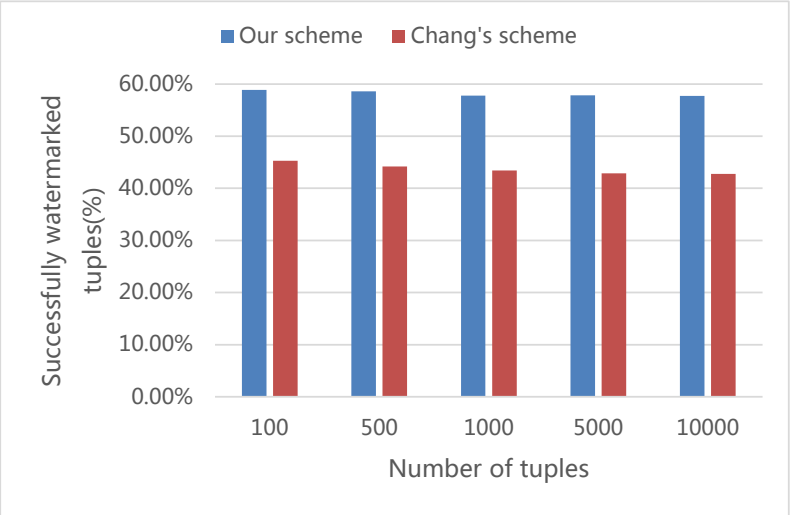

FIGURE 3. Performance on Shuttle-dataset

The watermark embedding capacity performances of our proposed scheme on the three datasets are 14.27%, 14.45% and 10.51% higher than Chang's scheme [1] by applying the improved histogram shifting with tree structure and attribute selection. In addition, when the number of tuple for watermark embedding is not large, our proposed scheme can fulfil the size of a hash message while Chang's scheme cannot. For example, if the number of tuple is set to be 1000, the average EC of our proposed scheme is 219.9 on the FCT-dataset whereas the average EC of Chang's scheme is merely 77.3.

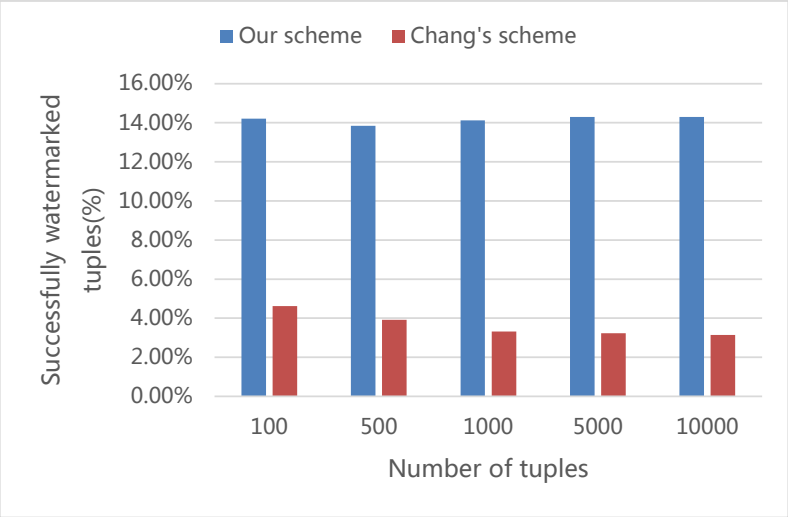

FIGURE 4. Performance on R-dataset

3.2. **Robustness Analysis.** The robustness performances of our proposed and Chang's scheme under different attacks are compared in this section. The weight vector in Eq.(9) is adjusted as $Wt = 0.4$ and $Wa = 0.6$ according to the experimental experience. In the experiment, the size of database is set to 5000 tuples because that the robustness performances of both the two schemes are strong and close for comparing when the size of database is huge. The vote parameter τ is set to 0.5 in the experiment. Assume that the attackers do not drop the primary key attribute or modify the values of the primary keys since they are valuable information and any modification of them will reduce the usefulness of the relational database. In addition, attackers do not know the information about the selected attributes or cells for watermark embedding. Four types of attacks are designed in our paper. In the alteration attack, the values of cells in the relational database are randomly altered to render the watermark unusable. In the deletion attack, the attacker wants to destroy the watermark by randomly drop several tuples in the relational database. In the addition attack, some new tuples are inserted to affect the watermark detection process. In the sorting attack, the attacker wants to resort the attributes and tuples. Benefiting from the application of local map, we can use the primary key information to determine the selected tuples and resort the attributes and tuples with the primary key information and attribute names. Thus, our scheme can withstand both the addition and the sorting attacks. The average watermark matching rates of watermark of our proposed and Chang's scheme under alteration and deletion of tuples are compared in FIGURE 5 and FIGURE 6. The robustness of our scheme is stronger than that of Chang's scheme from the FIGURE 5 and FIGURE 6. In the alteration attack, 93% of the watermark can be recovered using our scheme when 30% tuples are altered, whereas the recovery rate of Chang's scheme is merely 83%. In the deletion attack, the watermark recovery rate is 90.1% in our scheme when 30% tuples are deleted, while only 74.8% of watermark can be recovered in Chang's scheme. The reason for the experimental results is that the robustness of both these two schemes are mainly based on the MVT which relies on watermark embedding capacity, and our proposed scheme outperforms the Chang's scheme in terms of watermark embedding capacity as demonstrated in the former part.

3.3. **Imperceptibility Analysis.** If the attackers can predict the selected attributes and cells for watermark embedding and modify the cells, most of the embedded watermark is

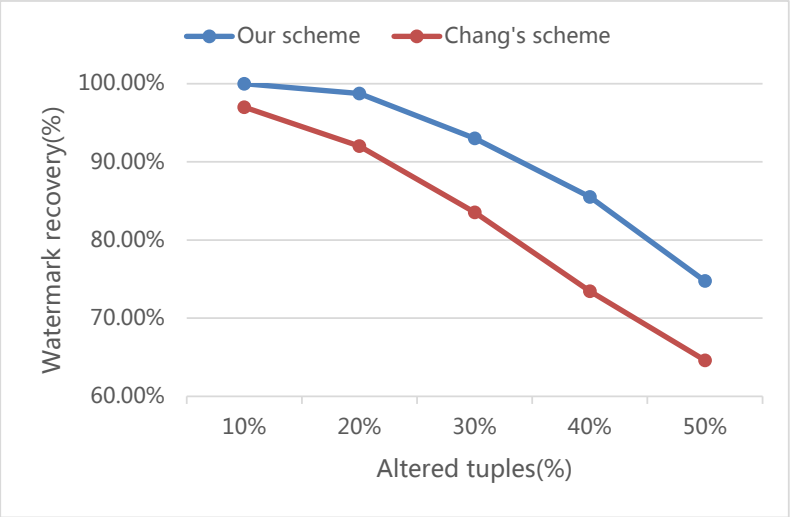

FIGURE 5. Robustness to the alteration attack

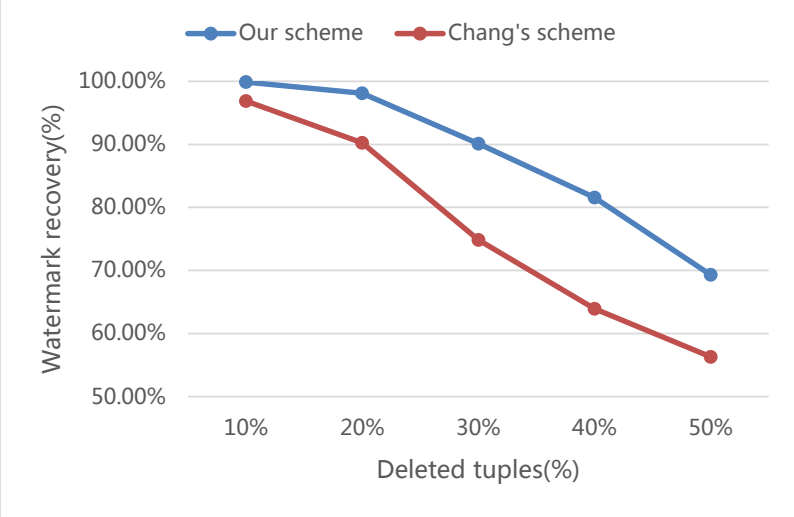

FIGURE 6. Robustness to the deletion attack

unusable. Since the distortion caused by watermark embedding may provide information of selected attributes, the reduction of this kind of distortion can help to avoid the attacker's prediction. TABLE 1 shows the comparison of average tuple-wise distortion and

TABLE 1. Performance of selection method

	FCT-dataset		Shuttle-dataset		R-dataset	
	TWD	AWD	TWD	AWD	TWD	AWD
Without selection	6.4%	2.3%	21.2%	13.1%	14.7%	22.1%
With selection	0.4%	0.3%	4.0%	3.0%	1.1%	1.6%
Reducing rate	93.8%	87.2%	81.2%	77.0%	92.8%	92.9%

attribute-wise distortion with and without the attribute and cell selection processes.

By applying the attribute and cell selections, both the TWD and AWD are reduced since the more suitable attributes and cells for watermark embedding are selected. The reducing rates of the three datasets are considerable and the best one reaches as high as

93.8%. Moreover, by applying the attribute and cell selections, the distortions caused by watermark embedding are sufficiently low to avoid the attacker's prediction.

Table 2. Comparison with other schemes

	Blind	Reversible	EC	Robustness	Data type
Our scheme	Semi	Yes	Sufficient	Strong	Numeric
Shehab's scheme [10]	Semi	No	Sufficient	Strong	Numeric
Farfoura's scheme [7]	Semi	Yes	Insufficient	Medium	Fractional
Chang's scheme [1]	Semi	Yes	Insufficient	Medium	Numeric
Jawad's scheme [6]	Semi	Yes	Sufficient	Weak	Numeric

3.4. **Comparison with Other Schemes.** In this experiment, the comparison with the other four database watermarking schemes [1, 6, 7, 10] are conducted respectively in terms of five aspects: 1) whether the watermarking scheme is blind, 2)whether the watermarking scheme is reversible, 3)whether the watermark embedding capacity is sufficient, 4) whether the robustness of watermarking scheme is strong, 5) suitable data type. The results are shown in TABLE 2.

As shown in TABLE 2, our proposed scheme outperforms these methods. Compared with the Shehab et al.'s method [10], our scheme is reversible. Compared with the Farfoura's scheme, our scheme can use all numeric data while the Faroura's [7] can only deal with the fractional portions. Compared with the Chang's [1] scheme, the application of tree structure provides high and stable EC which also ensures a strong robustness. Compared with Jawad's [6] scheme, the robustness of our scheme is significantly enhanced by applying the MVT and the EC of our scheme is also higher. In addition, the experiment results show that the utilization of attribute and cell selection increases robustness and decreases distortion effectively. Compare with the increased robustness and decreased distortion, the gained side message is acceptable because the local map is compressed significantly by using the run-length coding algorithm.

4. **Conclusions.** In this paper, a novel reversible watermarking scheme for relational databases is proposed. Our analysis and experimental results have demonstrated that our scheme has significant advantages over existing schemes: the EC of our scheme is increased by applying the binary tree structure and the attribute selection method; the robustness of the proposed scheme is strong against various database attacks by utilizing the MVT with the high and stable EC; lastly, the watermark imperceptibility of the proposed scheme is enhanced by modifying the histogram shifting with tree structure method and designing the attribute and cell selection methods.

Acknowledgment. This work was supported by Shenzhen Engineering Laboratory of Broadband Wireless Network Security, and the Science and Technology Development Fund of Macao SARFDCT056/2012/A2 and UM Multi-year Research Grant MYRG144(Y1-L2)-FST11-ZLM.

REFERENCES

[1] C. C. Chang, T. S. Nguyen, and C. C. Lin, A blind reversible robust watermarking scheme for relational databases, *The Scientific World Journal*, 2013.

[2] C. C. Lin, C. C Chang ,and Y. H. Chen, A Novel SVD-based watermarking Scheme for Protecting Rightful Ownership of Digital Images, *Journal of Information Hiding and Multimedia Signal Processing*, vol. 5, no. 2, pp. 124-143, 2014.

[3] F. Guo, J. M. Wang, Z. H. Zhang, X. J. Ye, and D. Y Li, An improved algorithm to watermark numeric relational data, *In Information Security Applications*, pp. 138–149, 2006.
[4] H. C. Huang, and F. C Chang, Robust Image Watermarking Based on Compressed Sensing Techniques, *Journal of Information Hiding and Multimedia Signal Processing*, vol. 5, no. 2, pp. 275-285, 2014.
[5] J. Fridrich, M. Goljan, and A.C. Baldoza. New fragile authentication watermark for images, *Image Processing, 2000. Proceedings. 2000 International Conference*, vol.1, pp.446–449, 2000.
[6] K. Jawad and A. Khan, Genetic algorithm and difference expansion based reversible watermarking for relational databases, *Journal of Systems and Software*, vol. 86, no. 11, pp. 2742–2753, 2013.
[7] M. Farfoura, S. J. Horng, J. L Lai, R. S. Run, R. J. Chen, and M.K. Khan, A blind reversible method for watermarking relational databases based on a time-stamping protocol, *Expert Systems with Applications*, vol. 39, no.3, pp. 3185–3196, 2012.
[8] M. Wu, H. Yu, and B. D. Liu, Data hiding in image and video. i. fundamental issues and solutions, *Image Processing*, vol.12, no. 6, pp.685–695, 2003.
[9] M. Wu, B. D. Liu, Data hiding in image and video. ii. designs and applications, *Image Processing*, vol.12, no. 6, pp.696–705, 2003.
[10] M. Shehab, E. Bertino, and A. Ghafoor, Watermarking relational databases using optimization-based techniques, *Knowledge and Data Engineering*, vol. 20, no. 1, pp. 116–129, 2008.
[11] P. W Wong and N.Memon,Secret and public key image watermarking schemes for image authentication and ownership veri
cation, *Image Processing*, vol.10, no.10, pp.1593–1601, 2001.
[12] R. Sion., Proving ownership over categorical data, in *Data Engineering, 2004. Proceedings. 20th International Conference*, pp.584–595, 2004.
[13] R. Sion, M.J. Atallah, and S. Prabhakar, Rights protection for relational data, *Knowledge and Data Engineering*, vol.10, no.12, pp.1509–1525, 2004.
[14] R. Halder, S. Pal, and A. Cortesi, Watermarking techniques for relational databases: Survey, classification and comparison, *J. UCS*, vol. 16, no. 21, pp. 3164–3190, 2010.
[15] R. Agrawal and J. Kiernan, Watermarking relational databases, in *Proceedings of the 28th international conference on Very Large Data Bases*, pp.155–166, 2002.
[16] R. Agrawal, P.J Haas, and J. Kiernan, Watermarking relational data: framework, algorithms and analysis,*The VLDB journal*, vol.12, no. 2, pp.157–169, 2003.
[17] S. W Weng, and J. S. Pan, Reversible Watermarking Based on Eight Improved Prediction Modes, *Journal of Information Hiding and Multimedia Signal Processing*, vol. 5, no. 3, pp. 527-533, 2014.
[18] W. L. Tai, C. M. Yeh, and C. C. Chang, Reversible data hiding based on histogram modification of pixel differences, *Circuits and Systems for Video Technology*, vol. 19, no. 6 pp. 906–910, 2009.
[19] Y. C. Li, C. M. Yeh, and C. C. Chang, Data hiding based on the similarity between neighboring pixels with reversibility, *Digital Signal Processing*, vol. 20, no. 4, pp. 1116–1128, 2010.