J. Integr. Sci. Technol. 2021, 9(2), 107-112 Article

Journal of Integrated
SCIENCE & TECHNOLOGY

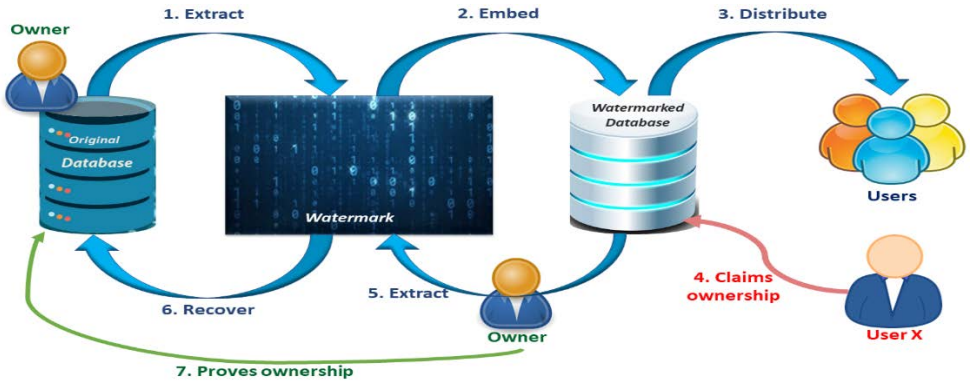
Quadratic difference expansion based Reversible Watermarking for relational database

Seema Siledar[1], Sharvari Tamane[2]

[1]Dr. Babasaheb Ambedkar Marathwada University, Aurangabad, Maharashtra, India. [2]University Department of Information and Communication Technology, MGM University, Aurangabad, Maharashtra, India.

Received on: 14-Oct-2021, Accepted and Published on: 4-Dec-2021

ABSTRACT



With the increase in use of databases over the internet, it has become difficult to recognize genuine database owner. To protect ownership, digital watermarking has emerged as an effective solution. However, embedding watermark into database would result in loss of data quality. Most state-of-the-art methods introduce distortion into the original data to a large extent. In this work, reversible watermarking technique using quadratic difference expansion has been proposed. First, the numeric attributes with highest pearson correlation coefficient are selected to reduce distortion in the database. The watermark is then generated by extracting bits from the selected attributes using quadratic difference expansion. Watermarked database is obtained after the generated watermark is embedded into the original database. To resolve ownership conflict, the genuine owner can easily extract watermark from watermarked database and recover original database. Indian Liver Patient dataset is used to conduct experiments. Results show that the proposed method is 100% robust against insertion attack. In case of 90% modification and 50% deletion attack, it is observed that around 50% of the watermark can be recovered. Moreover, watermark embedding results in only 0.02% change in the mean of original database. It demonstrates that distortion caused due to watermarking lead to negligible effect on data quality.

Keywords: reversible database watermarking, quadratic difference expansion, robust, ownership protection

INTRODUCTION

Database watermarking allows the owner to embed a watermark into database. In case of copyright infringement, the owner extracts the embedded watermark to prove ownership. Basically, watermarks are categorized as robust and fragile. If a watermark remains unaltered even after making modifications to the digital media, then it is said to be robust. If a watermark gets destroyed due to the slightest modification in digital media, then it is referred as fragile. Generally, fragile watermarks are used for integrity verification and robust watermarks for ownership protection. Watermarks may or may not add distortion into the original database leading to distortion based and distortion free watermaking techniques. Many researchers have worked on distortion-free watermarking techniques[1–9] which do not introduce any change into the original database. However, distortion-based watermarking have been area of research since the term was first coined in 2002.[10] Since then, a lot of work has been carried on distortion based watermaking.[11–18]

Corresponding Author: Seema Siledar

Email: seema.siledar@mit.asia

Cite as: *J. Integr. Sci. Technol., 2021, 9(2), 107-112.*

 ISSN: 2321-4635 http://pubs.iscience.in/jist

Reversible watermarking methods protect rights of owners and also provide recovery of original data. Many reversible database watermarking techniques have been proposed in the literature. Difference expansion and genetic algorithm (GA) are used together to improve watermark capacity and reduce distortion.[19] An idea of histogram shifting of adjacent pixel difference (APD) is suggested to obtain reversibility.[20] Reversible data-embedding technique called prediction-error expansion on integers can help achieve reversibility.[21] 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.[22] Difference expansion watermarking (DEW) with Firefly Algorithm (FFA), a bioinspired optimization technique, is utilized to embed watermark into relational databases.[23] An approach for robust and reversible database watermarking technique, Genetic Algorithm and Histogram Shifting Watermarking (GAHSW), for numerical relational database has also been put forward.[24] A low distortion reversible database watermarking method based on histogram gap is suggested in view of the large gap in histogram of database integer data.[25] A novel, robust and reversible database watermarking technique, named histogram shifting watermarking based on random forest and genetic algorithm (RF-GAHCSW) has been proposed. It would improve the watermark capacity by means of histogram width reduction and eliminates the impact of the prediction error attack.[26] A method of embedding differential expansion watermarking (DEW) based on ant colony algorithm (ACO) in relational databas has been proposed.[27] It has also been suggested to hide confidential messages into a relational database by the LSB (Least-Significant-Bit) matching method for relational databases.[28] A robust and reversible watermarking algorithm has been presented for a relational database based on continuous columns in histogram.[29] A reversible database watermarking based on difference expansion technique employing PCC has been proposed.[30]

PRELIMINARIES

In this section, we present preliminaries used in our proposed method.

Pearson Correlation Coefficient (PCC)

It is the measure of linear correlation between two variables x and y. It is the ratio between the covariance of two variables and the product of their standard deviations as shown in Eq. (1)

$$r = \frac{n(\sum xy) - (\sum x)(\sum y)}{\sqrt{[n\sum x^2 - (\sum x)^2][n\sum y^2 - (\sum y)^2]}} \quad (1)$$

'r' ranges between -1 and +1 where -1 represents the lowest correlation between variables *x* and *y* and +1 represents the highest correlation between variables *x* and *y*.

Quadratic Difference Expansion

A reversible image watermarking algorithm has recently been proposed based on quadratic difference expansion[31]. Consider two numeric attributes x and y present in the database. Positive transform is as follows:

$$avg = \lfloor (x + y)/2 \rfloor \quad (2)$$

$$diff = x - y \quad (3)$$

The obtained difference is shifted to the left by 1 bit, and the watermark b is embedded in its least significant bit as $d = 2 * diff + b$.

Inverse transform is as follows:

$$A_1' = avg + \lfloor (d+1)/2 \rfloor \quad (4)$$

$$A_2' = avg - \lfloor d/2 \rfloor \quad (5)$$

Perform the quadratic watermark embedding using difference expansion as:

$$avg' = \lfloor (A_1' + A_2')/2 \rfloor \quad (6)$$

$$diff' = A_1' - A_2' \quad (7)$$

$$d' = \lfloor diff'/2 \rfloor + b \quad (8)$$

Inverse transform is as follows:

$$A_{1-new} = avg' + \lfloor (d'+1)/2 \rfloor \quad (9)$$

$$A_{2-new} = avg' + \lfloor d'/2 \rfloor \quad (10)$$

METHODOLOGY

We propose a reversible relational database watermarking method using quadratic difference expansion. The proposed method is partitioned into two phases: Watermark Embedding and Watermark Extraction.

During the watermark embedding phase, watermark bits are generated from specific tuples and embedded into their data values. The input of this phase is original database. Following steps are carried out:

Step 1: Find Pearson Correlation Coefficient (PCC) for all the numeric attributes using Eq. (1)

Step 2: Select a pair of attributes whose Pearson Correlation Coefficient (PCC) is highest among all.

Assume that the two numeric attributes A_1 and A_2 present in the database have highest PCC and hence, this pair is selected.

Step 3: Apply hash on the primary key and choose a tuple whose (hash(id),16) % 11=0

Step 4: Embed watermark bits in selected tuples of original database using primary difference expansion to get watermarked database

Calculate the average and difference of attribute values for selected tuples as shown in Eq. (11) and Eq. (12)

$$avg = \lfloor (A_1 + A_2)/2 \rfloor \quad (11)$$

$$diff = A_1 - A_2 \quad (12)$$

Extract the LSB from avg to generate watermark bit b as in Eq. (13)

$$b = avg \,\&\, 1 \quad (13)$$

Embed the bit *b* in watermark string as in Eg. (5)

$$wm = wm + str(b) \quad (14)$$

Now, calculate d as shown in Eq. (15)

$$d = 2 * diff + b \quad (15)$$

Modified values denoted by A_1' and A_2' are computed using difference expansion as represented in Eq. (16) and Eq. (17)

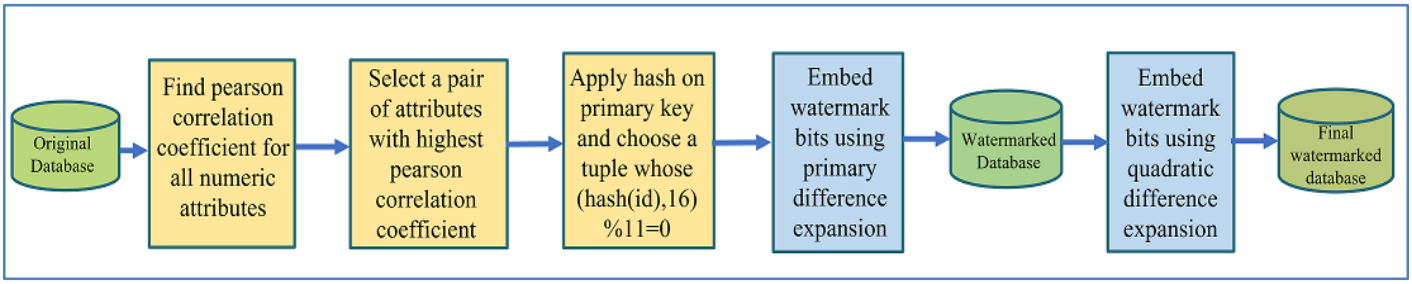


Figure 1: Watermark embedding phase

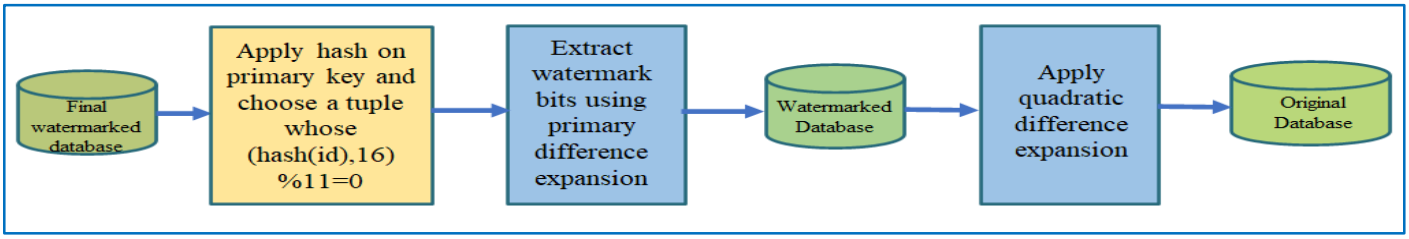


Figure 2: Watermark extraction phase

$$A_1' = avg + \lfloor (d+1)/2 \rfloor \quad (16)$$

$$A_2' = avg - \lfloor d/2 \rfloor \quad (17)$$

Step 5: Embed watermark bits in selected tuples of watermarked database using quadratic difference expansion to get final watermarked database.

Calculate the average and difference of A_1' and A_2' obtained in step 4 using Eq. (18) and Eq. (19)

$$avg' = \lfloor (A_1' + A_2')/2 \rfloor \quad (18)$$

$$diff' = A_1' - A_2' \quad (19)$$

Obtain the value of d' using Eq. (20)

$$d' = \lfloor diff'/2 \rfloor + b \quad (20)$$

New values denoted by A_{1-new} and A_{2-new} are computed using quadratic difference expansion as represented in Eq. (21) and Eq. (22)

$$A_{1-new} = avg' + \lfloor (d' + 1)/2 \rfloor \quad (21)$$

$$A_{2-new} = avg' + \lfloor d'/2 \rfloor \quad (22)$$

The output of this phase is final watermarked database. Fig. 1 depicts the working of watermark embedding phase.

During the watermark extraction phase, watermark bits are extracted from the tuples where they are embedded in watermark embedding phase. Then, the database is restored to its original state. The input of this phase is final watermaked database. Again, the numeric attributes A_1 and A_2 with highest PCC are considered.Following steps are carried out here:

Step 1: Apply hash on the primary key and choose a tuple whose (hash(id),16) % 11=0

Step 2: Extract watermark bits from selected tuples of final watermarked database using primary difference expansion.

Calculate the average and difference as shown in Eq. (23) and Eq. (24)

$$avg' = \lfloor (A_{1-new} + A_{2-new})/2 \rfloor \quad (23)$$

$$diff' = A_{1-new} - A_{2-\text{new}} \quad (24)$$

The watermark bit b can be extracted using Eq. (25)

$$b' = avg' \,\&\, 1 \quad (25)$$

Append the bit b' to get watermark string as in Eq. (26)

$$wm' = wm' + str(b') \quad (26)$$

Now, calculate d' as shown in Eq. (27)

$$d' = 2 * diff' + b' \quad (27)$$

Modified values denoted by A_1' and A_2' are computed using difference expansion as represented in Eq. (28) and Eq. (29)

$$A_1' = avg' + \lfloor (d'+1)/2 \rfloor \quad (28)$$

$$A_2' = avg' - \lfloor d'/2 \rfloor \quad (29)$$

Step 3: Apply quadratic difference expansion on database obtained in step 2 to recover the original database.

Calculate the average and difference of A_1' and A_2' using Eq. (30) and Eq. (31)

$$avg = \lfloor (A_1' + A_2')/2 \rfloor \quad (30)$$

$$diff = A_1' - A_2' \quad (31)$$

Obtain the value of d using Eq. (32)

$$d = \lfloor diff/2 \rfloor - b' \quad (32)$$

Retrieve the original values A_1 and A_2 using quadratic difference expansion as represented in Eq. (33) and Eq. (34)

$$A_1 = avg + \lfloor (d+1)/2 \rfloor \quad (33)$$

$$A_2 = avg + \lfloor d/2 \rfloor \quad (34)$$

The output of this phase is the original database. Fig. 2 depicts the working of watermark extraction phase.

To demonstrate the working of our method, consider $A_1 = 53$ and $A_2 = 58$, then, $avg = \lfloor (53+58)/2 \rfloor = 55.5 \approx 55$ and $diff = 53 - 58 = -5$ using Eq. (11) and Eq. (12). Generate watermark with the help of Eq. (13) and Eq. (14) as $b = 55 \,\&\, 1 = 1$ and $wm = 1$. Using Eq. (15), $d = 2 * (-5) + 1 = -9$ is calculated by inserting 1 as watermark bit. Now, the modified attribute values are calculated by using Eq. (16) and Eq. (17):

$A_1' = 55 + \lfloor (-9 + 1)/2 \rfloor = 55 + \lfloor (-8)/2 \rfloor = 55 + (-4) = 51$

$A_2' = 55 - \lfloor (-9)/2 \rfloor = 55 - (-5) = 55 + 5 = 60$

Apply Eq. (18) and Eq. (19) to find average and difference of A_1' and A_2' as $avg' = \lfloor (51+60)/2 = 55.5 \approx 55$ and $diff' =$

$51 - 60 = -9$. Substitute $b\ and\ diff'$ in Eq.(20) to get $d' = \lfloor -9/2 \rfloor + 1 = \lfloor -4.5 \rfloor + 1 = -5 + 1 = -4$.

Now, the new values are calculated by using Eq. (21) and Eq. (22):

$A_{1-new} = 55 + \lfloor (-4 + 1)/2 \rfloor = 55 + \lfloor -1.5 \rfloor = 55 + (-2) = 53$ and $A_{2-new} = 55 - \lfloor (-4)/2 \rfloor = 55 - (-2) = 55 + 2 = 57$

From the above values, calculate the average and difference using Eq. (23) and Eq. (24) as $avg' = \lfloor (53 + 57)/2 \rfloor = 55$ and $diff' = 53 - 57 = -4$. Using Eq. (25) and Eq. (26), extract watermark bit $b' = 55 \,\&\, 1 = 1$ and watermark string as $wm' = 1$. Find $d' = -4 * 2 + 1 = -7$ by Eq. (27). Modified values are recovered with the help of Eq. (28) and Eq. (29):

$A'_1 = 55 + \lfloor (-7 + 1)/2 \rfloor = 55 + \lfloor -3 \rfloor = 52$

$A'_2 = 55 - \lfloor (-7/2) \rfloor + 1 = 55 - \lfloor -3.5 \rfloor = 55 + 4 = 59$

Apply Eq. (30) and Eq. (31) to find average and difference of A'_1 and A'_2 as $avg = \lfloor (52 + 59)/2 \rfloor = 55.5 \approx 55$ and $diff = 52 - 59 = -7$. Substitute $diff$ in Eq.(32) to get $d = \lfloor -7/2 \rfloor - 1 = \lfloor -3.5 \rfloor - 1 = -5$.

Now, the original values are calculated by using Eq. (33) and Eq. (34):

$A_1 = 55 + \lfloor (-5 + 1)/2 \rfloor = 55 + \lfloor -2 \rfloor = 55 + (-2) = 53$ and $A_2 = 55 - \lfloor (-5)/2 \rfloor = 55 - \lfloor -2.5 \rfloor = 55 + 3 = 58$

RESULTS AND DISCUSSION

Intel Core i3 CPU of 2.00GHz and 4GB RAM has been used to conduct experiments on Indian Liver Patient Dataset with 583 tuples. This dataset contains 10 attributes, namely Age, Gender, Total Bilirubin, Direct Bilirubin, Alkaline Phosphatase, Alamine Aminotransferase, Aspartate Aminotransferase, Total Proteins, Albumin, Albumin and Globulin Ratio. A primary key attribute has been added named as ID having values from 1 to 583. Gender is a categorical attribute and hence, it is excluded from Pearson Correlation Coefficient (PCC) matrix.

The attributes ID, Age, Total Bilirubin, Direct Bilirubin, Alkaline Phosphatase, Alamine Aminotransferase, Aspartate Aminotransferase, Total Proteins, Albumin, Albumin and Globulin Ratio are renamed as A, B, C, D, E, F, G, H, I, J.

The Pearson Correlation Coefficient (PCC) for all the numeric values are as shown in Table 1. The attributes with highest PCC value are F and G i.e., Alamine Aminotransferase and Aspartate Aminotransferase. Out of 583 tuples, 59 are considered for watermarking. These are 10% of the total tuples.

Robustness Analysis

Different types of attacks can be used to perform robustness analysis. Three types of attacks: insertion, deletion, and modification are considered for experimentation. Assume that an attacker attempts to insert, delete, or modify the tuples of the database. Experiments are conducted to simulate all these attacks with attack rate of 10%, 20%, up to 90%. Fig. 3 depicts attack ratio and watermark detection rate on on X-axis and Y-axis respectively.

First experiment is performed to demonstrate insertion attack. Hash function of the primary key is computed and based on its value, the tuples are selected for watermarking. When attacker inserts new tuple into the database, the watermark remains unchanged. Thus, the proposed method is robust to insertion attack as shown in Figure 3

Second experiment is conducted to determine the robustness of the proposed method under deletion attack. In this type of attack, the attacker attempts to randomly delete tuples from the database.

As the attack rate increases from 10% to 90% by deleting 59 tuples to 525 tuples respectively, the watermark detection rate decreases from 92% to 10%. It means that the chance of watermark detection decreases as we increase the deletion attack percentage.This can be observed in Fig. 3. Moreover, it is not possible to recover the complete watermark when many tuples containing watermark information get deletedThe third experiment is performed to demonstrate modification attack. In modification attack, the attacker attempts to randomly modify tuples in the database. Fig. 3 shows that the increase in attack rate from 10% to 90% leads to detection rate of 95% to 49% respectively. It means that there is almost 50% chance of watermark detection with higher attack rate. From Fig. 3, it can be observed that around 50% of the watermark can be recovered even in case of 90% modification attack.

Table 1. Pearson Correlation Coefficient (PCC) for all numeric attributes

	A_1	A_2	A_3	A_4	A_5	A_6	A_7	A_8	A_9	A_{10}
A_1	1									
A_2	-0.052385	1								
A_3	0.1015259	0.011763	1							
A_4	0.1362854	0.007529	0.874618	1						
A_5	-0.078805	0.080425	0.206669	0.234939	1					
A_6	-0.12486	-0.08688	0.214065	0.233894	0.125680	1				
A_7	-0.094106	-0.01991	0.237831	0.257544	0.167196	0.791966	1			
A_8	0.189634	-0.18746	-0.0081	-0.000139	-0.028514	-0.042518	-0.025645	1		
A_9	0.0656466	-0.26592	-0.22225	-0.228531	-0.165453	-0.029742	-0.085290	0.784053	1	
A_{10}	-0.024123	-0.21853	-0.20595	-0.199745	-0.235087	-0.002821	-0.070033	0.239690	0.691239	1

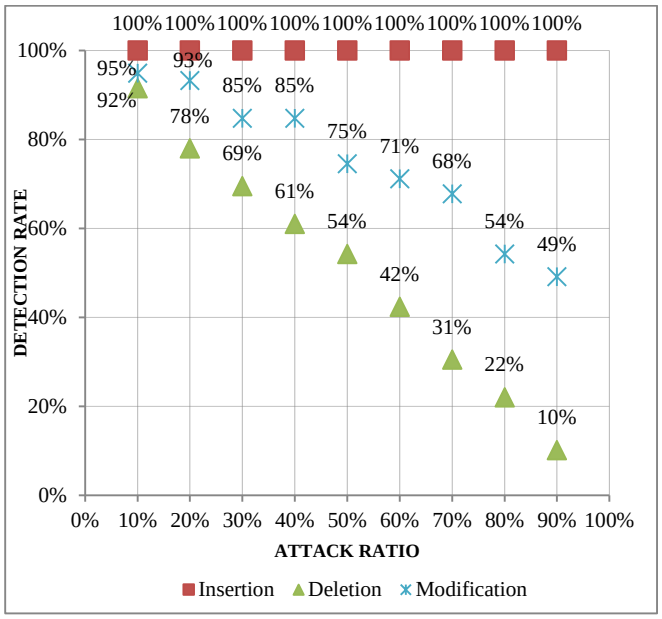


Figure 3: Watermark Detection Rate

Statistical Distortion

Statistical distortion through mean absolute error and variations of mean and standard deviation between the attributes before and after watermark insertion.

Mean Absolute Error (MAE)

Mean Absolute Error (MAE) can be calculated as:

$$MAE = \frac{\sum_{i=1}^{n} |A_i - A_i^W|}{n} \quad (35)$$

where, n is the total number of tuples in the database, A_i is the attribute of original database and A_i^W is the attribute of watermarked database.

Table 2. Mean Absolute Error (MAE)

Attribute name	MAE
Alamine Aminotransferase (F)	0.018
Aspartate Aminotransferase (G)	0.029

Table 2 shows the mean absolute error for the selected attributes. MAE value represents that embedded watermark introduce minor or negligible distortion into the database.

Mean and Standard Deviation

Table 3 provides the mean and standard deviation obtained for the selected attributes Alamine Aminotransferase and Aspartate Aminotransferase. These measures are computed for the original as well as the watermarked database as seen in Table 3.

Table 3. Mean and Standard Deviation

Attribute name	Original Database		Watermarked Database	
	Mean	Std	Mean	Std
Alamine Aminotransferase (F)	80.71	182.62	80.73	182.63
Aspartate Aminotransferase (G)	109.91	288.91	109.88	288.92

To see the change of mean and standard deviation, the difference in mean and the difference in standard deviation for the watermarked attributes are calculated as in Eq. (36) and Eq. (37):

$$Difference\ in\ mean = |Mean_{Db} - Mean_{WDb}| \quad (36)$$

$$Difference\ in\ standard\ deviation = |Std_{Db} - Std_{Wdb}| \quad (37)$$

where, $Mean_{Db}$ and Std_{Db} represent the mean and standard deviation of the original database. $Mean_{WDb}$ and Std_{WDb} represent mean and standard deviation of the watermarked database.

Table 4. Difference in mean and difference in standard deviation

Attribute name	Proposed method	
	Difference in mean	Difference in std
Alamine Aminotransferase (F)	0.018	0.009
Aspartate Aminotransferase (G)	0.029	0.002

Table 4 shows the difference in mean and standard deviation for the selected attributes. The difference in mean and standard deviation between original and watermarked database is 0.018 and 0.029 for attributes F and G respectively. Similarly, difference in standard deviation is 0.009 and 0.002 for attributes F and G respectively.

CONCLUSION

In this paper, a reversible watermarking technique has been proposed using quadratic difference expansion. Pearson Correlation Coefficient is used to find the highly correlated numeric attributes. Then, quadratic difference expansion is applied on these selected attributes to embed watermark. Once the watermark is extracted, it is possible to recover the original database from the watermarked one. This technique causes low distortion in the database leading to minor impact on data quality. This is backed up by the obtained statistical results. It has been observed that there is only 0.02% change in the mean of original and watermaked database. Also, the mean absolute error is 0.018 and 0.029 for the selected attributes. Experimental results show that the proposed method is robust against insertion attacks. Results also show that our method can recover around 50% of the watermark even with 90% of modification attack rate. As the attack rate increases from 10% to 90%, the watermark detection rate decreases from 92% to 10% in case of deletion attack.

CONFLICT OF INTEREST

Authors declared no conflict of interest.

REFERENCES

1. W. Yaqub, I. Kamel, Z. Aung. Toward watermarking compressed data in columnar database architectures. *Secur. Priv.* **2020**, 3 (4), 1–17.
2. S.M. Darwish, H.A. Selim. Design and Analysis of an Intelligent Integrity Checking Watermarking Scheme for Ubiquitous Database Access. *Int. J. Artif. Intell. Res.* **2018**, 3 (1), 1–10.
3. L. Camara, D. Coulibaly, A. Hamadou, J. Li. An Effective Approach for Non-Numeric Relational Database Verification. *Int. J. Database Theory Appl.* **2017**, 10 (6), 35–46.

4. S. Rani, D.K. Koshley, R. Halder. Partitioning-insensitive watermarking approach for distributed relational databases. *Lect. Notes Comput. Sci. Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinforma.* **2017**, 10720 LNCS, 172–192.
5. L. Camara, J. Li, R. Li, W. Xie. Distortion-free watermarking approach for relational database integrity checking. *Math. Probl. Eng.* **2014**, 2014 (i).
6. I. Kamel, W. Yaqub, K. Kamel. An empirical study on the robustness of a fragile watermark for relational databases. *2013 9th Int. Conf. Innov. Inf. Technol. IIT 2013* **2013**, No. July, 227–232.
7. A. Khan, S.A. Husain. A fragile zero watermarking scheme to detect and characterize malicious modifications in database relations. *Sci. World J.* **2013**, 2013.
8. J. Guo. Fragile watermarking scheme for tamper detection of relational database. *2011 Int. Conf. Comput. Manag. CAMAN 2011* **2011**, 1–4.
9. S. Bhattacharya, A. Cortesi. A generic distortion free watermarking technique for relational databases. *Lect. Notes Comput. Sci. Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinforma.* **2009**, 5905 LNCS (December 2009), 252–264.
10. R. Agrawal, P.J. Haas, J. Kiernan. Watermarking relational data: Framework, algorithms and analysis. *VLDB J.* **2003**, 12 (2), 157–169.
11. S. Iftikhar, M. Kamran, E.U. Munir, S.U. Khan. A Reversible Watermarking Technique for Social Network Data Sets for Enabling Data Trust in Cyber, Physical, and Social Computing. *IEEE Syst. J.* **2017**, 11 (1), 197–206.
12. J. Franco-Contreras, G. Coatrieux. Robust Watermarking of Relational Databases with Ontology-Guided Distortion Control. *IEEE Trans. Inf. Forensics Secur.* **2015**, 10 (9), 1939–1952.
13. J. Franco-Contreras, G. Coatrieux, N. Cuppens-Boulahia, F. Cuppens, C. Roux. Ontology-guided distortion control for robust-lossless database watermarking: Application to inpatient hospital stay records. *2014 36th Annu. Int. Conf. IEEE Eng. Med. Biol. Soc. EMBC 2014* **2014**, No. July 2016, 4491–4494.
14. V. Khanduja, S. Chakraverty, O.P. Verma, R. Tandon, S. Goel. A robust multiple watermarking technique for information recovery. *Souvenir 2014 IEEE Int. Adv. Comput. Conf. IACC 2014* **2014**, 250–255.
15. L. Camara, J. Li, R. Li, F. Kagorora, D. Hanyurwimfura. Block-based scheme for database integrity verification. *Int. J. Secur. Its Appl.* **2014**, 8 (6), 25–40.
16. J. Franco-Contreras, G. Coatrieux, F. Cuppens, N. Cuppens-Boulahia, C. Roux. Robust lossless watermarking of relational databases based on circular histogram modulation. *IEEE Trans. Inf. Forensics Secur.* **2014**, 9 (3), 397–410.
17. M. Kamran, M. Farooq. A formal usability constraints model for watermarking of outsourced datasets. *IEEE Trans. Inf. Forensics Secur.* **2013**, 8 (6), 1061–1072.
18. M. Kamran, S. Suhail, M. Farooq. A robust, distortion minimizing technique for watermarking relational databases using once-for-all usability constraints. *IEEE Trans. Knowl. Data Eng.* **2013**, 25 (12), 2694–2707.
19. K. Jawad, A. Khan. Genetic algorithm and difference expansion based reversible watermarking for relational databases. *J. Syst. Softw.* **2013**, 86 (11), 2742–2753.
20. C.-C. Chang, T.-S. Nguyen, C.-C. Lin. A Blind Reversible Robust Watermarking Scheme for Relational Databases. *Sci. World J.* **2013**, 2013, 12.
21. M.E. Farfoura, S.J. Horng, X. Wang. A novel blind reversible method for watermarking relational databases. *J. Chin. Inst. Eng. Trans. Chin. Inst. Eng. A* **2013**, 36 (1), 87–97.
22. Y.-J. Ma, Y.-S. Zhu, X.-Y. Liu. A Novel Reversible Watermarking Scheme for Relational Databases Protection Based on Histogram Shifting. *J. Inf. Hiding Multimed. Signal Process. C* **2016**, 7 (2).
23. M.B. Imamoglu, M. Ulutas, G. Ulutas. A New Reversible Database Watermarking Approach with Firefly Optimization Algorithm. *Math. Probl. Eng.* **2017**, 2017.
24. D. Hu, D. Zhao, S. Zheng. A new robust approach for reversible database watermarking with distortion control. *IEEE Trans. Knowl. Data Eng.* **2019**, 31 (6), 1024–1037.
25. Y. Li, J. Wang, S. Ge, X. Luo, B. Wang. A reversible database watermarking method with low distortion. *Math. Biosci. Eng.* **2019**, 16 (5), 4053–4068.
26. C. Ge, J. Sun, Y. Sun, et al. Reversible Database Watermarking Based on Random Forest and Genetic Algorithm. *Proc. - 2020 Int. Conf. Cyber-Enabled Distrib. Comput. Knowl. Discov. CyberC 2020* **2020**, 239–247.
27. J. Lian. A new reversible database watermarking approach with ant colony optimization algorithm. In *Journal of Physics: Conference Series*; IOP Publishing, **2020**; Vol. 1616, p 12040.
28. M.-S. Hwang, M.-R. Xie, C.-C. Wu. A Reversible Hiding Technique Using LSB Matching for Relational Databases. *Informatica* **2020**, 31 (3), 481–497.
29. Y. Li, J. Wang, H. Jia. A Robust and Reversible Watermarking Algorithm for a Relational Database Based on Continuous Columns in Histogram. *Math.* **2020**, 8 (11), 1994.
30. S. Siledar, Dr.S. Tamane. Reversible Database Watermarking With Distortion Control. *Indian J. Comput. Sci. Eng.* **2021**, 12 (5), 1503–1509.
31. Z. Zhang, M. Zhang, L. Wang. Reversible image watermarking algorithm based on quadratic difference expansion. *Math. Probl. Eng.* **2020**, 2020.