International Journal on Applications in Engineering and Technology
Volume 2: Issue 2: February 2016, pp 5-6 www.aetsjournal.com ISSN (Online) : 2455-0523

A Robust And Reversible Watermarking (Rrw) Technique Based On Genetic Algorithm

Anitha.T,Bhuvaneshwari.N,Krithicka.S,Nathiya.C,Nithya.L

Abstract— Over the past few years, reversible watermarking techniques for relational databases have been proposed to provide protection of ownership rights, data tempering and data integrity. The reversible watermarking has emerged as a solution for the protection of ownership rights of data. Reversible watermarking is employed to ensure ownership rights of data, data quality along-with data recovery. However, such techniques are usually not robust against malicious attacks and do not provide any mechanism to selectively watermark a particular attribute by taking into account its role in knowledge discovery. Therefore, reversible watermarking is required that ensures; (i) watermark encoding and decoding by accounting for the role of all the features in knowledge discovery; and, (ii) original data recovery in the presence of active malicious attacks. A robust and semi-blind reversible watermarking (RRW) technique for numerical relational data has been proposed that addresses the above objectives. Watermarking techniques have historically been used to ensure security in terms of ownership protection and tamper proofing for a wide variety of data formats. Reversible watermarking techniques can ensure data recovery along with ownership protection. The embedded watermark can subsequently be used for proving and claiming ownership**.** Experimental studies prove that reversible watermarking and data recovery is robust and efficient comparing to the existing system.

Keywords: *Data tampering, data integrity, Genetic algorithm, RRW, ownership.*

I.INTRODUCTION

In the digital world of today, data is stored in different digital formats such as images, audio, video, natural language texts and relational data. Relational data in particular is shared extensively by the owners with research communities and in virtual data storage locations in the cloud. The purpose is to work in a collaborative environment and make data openly available so that it is useful for knowledge extraction and decision making.

In shared environments such as that of the cloud, security threats that arise from un-trusted parties and relational databases one need to be addressed along with the enforcement of ownership rights on behalf of their owners.

Watermarking is used to protect the ownership of data.

II. EXISTING SYSTEM

From past few decades, digital watermarking techniques are being used for ownership protection of images, audio, video and natural language processing software's. Data owners allow their data to be accessed and used remotely; therefore, may become a victim of data theft. Although, watermarking technology helps them to prove their ownership through identifying data piracy, yet introduces permanent modifications into the data which are irreversible and the watermarked data is different from the original content. Reversible watermarking of relational databases is a candidate solution to ensure data ownership protection as well as data integrity. However a major drawback of these techniques is that they modify the data to a very large extent which often results in the loss of data. There is a strong need to preserve the data quality in watermarked data so that it is of sufficiently high quality and fit for use in decision making as well as in planning processes in different application domains. There is no work has been conducted on overcoming the problems of reversible watermarking techniques in the presence of malicious attacks

Disadvantages

- Not robust against heavy attacks.
- Achieving robustness in the presence of reversibility is a challenging task.

III.PROPOSED SYSTEM

Ownership rights of the databases need to protect from malicious recipients; in the presence of data quality constraint. GA—an optimization algorithm is employed in the robust and reversible watermarking technique (RRW) proposed in this paper to achieve an optimal solution that is feasible for the problem at hand and does not violate the defined constraints. An optimal watermark value is created through the GA and inserted into the selected feature of the relational database in such a way that the data quality remains intact.

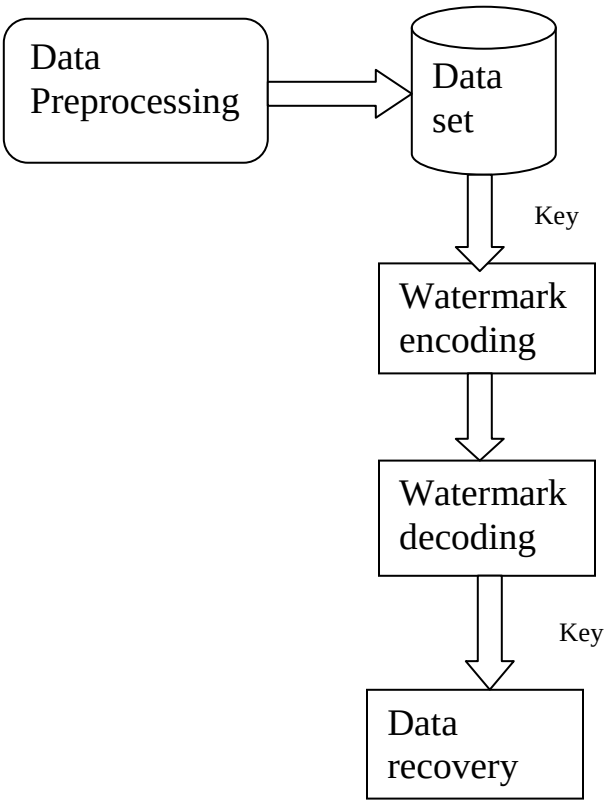
Advantages

- It allows recovery of a large portion of the data even after being subjected to malicious attacks.
- RRW is also evaluated through attack analysis where the watermark is detected with maximum decoding accuracy.

Anitha T,Bhuvaneshwari N,Krithicka S,Nathiya C,UG student,Department of Computer Science and Engineering, Nehru Institute of Technology,Coimbatore,India(anithat061994@gmail.com,bhuvaneshwarinsp@gmail.com,krithickasedhube12@gmail.com,cnathiya12@gmail.com)

Nithya L,Assistant Professor,Department of Computer Science and Engineering,Nehru Institue of Technology,Coimbatore,India(nithyalbe@gmail.com)

IV.SYSTEM ARCHITECTURE



V.SYSTEM IMPLEMENTATION

Implementation is the process that actually yields the lowest-level system elements. The system elements are made, bought, or reused. Production involves the hardware fabrication processes of forming, removing, joining, and finishing; or the software realization processes of coding and testing; or the operational procedures development processes for operators' roles.

System Implementation is the stage in the project where the theoretical design is turned into a working system.

The proposed system was developed using ASP.NET. The existing system caused long time transmission process but the system developed now has a very good user-friendly tool, which has a menu-based interface, graphical interface for the end user. After coding and testing, the project is to be installed on the necessary system. The executable file is to be created and loaded in the system. Again the code is tested in the installed system. Installing the developed code in system in the form of executable file is implementation.

VI.CONCLUSION

Reversible Watermarking techniques are used to cater to such scenarios because they are able to recover original data from watermarked data and ensure data quality to some extent. However, these techniques are not robust against malicious attacks—particularly those techniques that target some selected tuples for watermarking. A novel robust and reversible technique for watermarking numerical data of relational databases is presented. The results of the experimental study show that, even if an intruder deletes, adds or alters up to 50 percent of tuples, RRW is able to recover both the embedded watermark and the original data. RRW is compared with recently proposed state-of-the-art techniques such as DEW, GADEW and PEEW to demonstrate that RRW outperforms all of them on different performance merits.

VII.FUTURE ENHANCEMENT

One of our future concerns is to watermark shared databases in distributed environments where different members share their data in various proportions. We also plan to extend RRW for non-numeric data stores. Reversible watermarking techniques can ensure data recovery along with ownership protection. Fingerprinting, data hashing, serial codes are some other techniques used for ownership protection. Fingerprints also called transactional watermarks are used to monitor and identify digital ownership by watermarking all the copies of contents with different watermarks for different recipients.

VIII.REFERENCES

1. Agrawal, R. and Kiernan, J. (2002)"Watermarking relational databases," in Proc. 28th Int. Conf. Very Large Data Bases, pp. 155–166.
2. Alattar, A.M. (2003)"Reversible watermark using difference expansion of triplets," in Proc. IEEE Int. Conf. Image Process., pp. I–501, vol. 1.
3. Bache, K. and Lichman, M. (2013). UCI machine learning repository [Online]. Available: http://archive.ics.uci.edu/ml.
4. Bhatia, S. Prakash, P. and Pillai, G. (2008) "Svm based decision support system for heart disease
classification with integer-coded genetic algorithm to select critical features," in Proc. World Congr. Eng.
Comput. Sci., pp. 22–24.
5. Brassil, J.T. Low, S. and Maxemchuk, N.F (1999) "Copyright protection for the electronic distribution of text documents," Proc. IEEE, vol. 87, no. 7, pp. 1181–1196.
6. Chang, J.N. and Wu, H.C. (2012) "Reversible fragile database watermarking technology using difference expansion based on SVR prediction," in Proc. IEEE Int. Symp. Comput., Consum. Control, pp. 690–693.
7. Cox, I.J. Kilian, J. Leighton, F.T and Shamoon, T. (1997) "Secure spread spectrum watermarking for multimedia," IEEE Trans. Image Process., vol. 6, no. 12, pp. 1673 –1687.
8. Cox, I. Miller, M. Bloom, J. and Miller, M. (2001) Digital Watermarking. Burlington, MA, USA: Morgan Kaufmann.,
9. Cover, T.M. Thomas, J.A and Kieffer, J. (1994) "Elements of information theory," SIAM Rev., vol. 36, no. 3, pp. 509–510.
10. Cover, T.M and Thomas, J.A. (2012) Elements of Information Theory. NewYork, NY, USA: Wiley-Interscience.
11. Farfoura, M.E and Horng, S.J. (2010) "A novel blind reversible method for watermarking relational databases," in Proc. IEEE Int. Symp.Parallel Distrib. Process. Appl., pp.563–569.
12. Li, X. Yang, B. and Zeng, T. (2011) "Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection," IEEE Trans. Image Process., vol. 20, no. 12, pp. 3524–3533.Syst. Appl., vol. 38, no. 7, pp. 8024–8029.