ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

A Survey on Secure Watermarking Technique for Relational Data

Uzma A. Shaikh[1], Prof. Kishor N. Shedge[2]

M.E. Student, Dept. of Computer Engineering, SVIT, Chincholi, Nashik, Maharashtra, India[1]

Assistant Professor, Dept. of Computer Engineering, SVIT, Chincholi, Nashik, Maharashtra, India[2]

ABSTRACT: The rapid development of the Internet and related technologies has allowed for the tremendous ability to access and redistribute digital multi media contents. In such a context, protecting the ownership and controlling the copies of digital data have become very important. Watermarking technique is used to impose ownership rights over shared relational data and for providing a means for tackling data tampering. When ownership rights are imposed using watermarking, the underlying data undergoes certain modifications; as a result of which, the data quality gets compromised. The main aim is to maintain the ownership of Relational Database and also minimizing distortion in the watermarked content. Therefore, reversible watermarking is required that ensures watermark encoding and decoding by accounting for the role of all the features in knowledge discovery and original data recovery.

KEYWORDS: Reversible Watermarking, Data Tampering, Relational Database, Distortion.

I. INTRODUCTION

Due to the rapid growth of the Internet, the wide development of digital multimedia contents, and the easier distribution, copyright protection of owners is becoming more important. Digital watermarking is an important area in information hiding, thus providing a promising method of protecting digital data from illegitimate copying, and manipulation by embedding a secret code directly into the data. Digital watermarking allows the user to add a layer of protection to the digital media content by identifying copyright ownership and delivering a tracking capability. Accordingly, it monitors and reports where the user's digital media contents are being used.

Cryptography allows secure delivery of content to the consumers only. All legitimate consumers are not trustworthy, and untrustworthy consumers may modify or copy the decrypted contents illegally. However, cryptography provides no protection once the content is decrypted, which is required for human perception. Watermarking complements cryptography by embedding a message within the content

Digital watermarking was exploited in other digital media like protecting software , natural language and sensor data. The basic watermarking procedures like watermark insertion and detection to multimedia objects cannot be applied directly to watermarking relational databases due to the differences in the characteristics of multimedia and relational data. Unlike highly correlated multimedia data whose relative positions are fixed, database relations contain independent tuples with little redundancy. The tuples can be added, deleted or modified frequently in either benign updates or malicious attacks.

In the conventional irreversible watermarking schemes, only the embedded watermark information can be extracted from the suspected data; however, in reversible watermarking schemes, the original objects can be recovered along with the embedded watermarks.

Most watermarking schemes have been irreversible (the original relation cannot be restored from the watermarked relation). One major motivation for reversible watermarking is some real-life applications such as outsourced medical and military data. These kinds of data do not allow any losses.

In this, a reversible method for watermarking relational data is proposed which proves the true ownership of the database owner. This method tries to overcome the problem of data quality degradation by allowing recovery of original data along with the embedded watermark information.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

II. RELATED WORK

Agrawal and Kiernan [10] proposed the first irreversible watermarking technique for relational databases. They presented an effective watermarking technique geared for relational data. This technique uses the pseudo-random distribution of watermark based on keyed-hash function. This technique ensures that some bit positions of some of the attributes of some of the tuples contain specific values. The scheme does not provide security against secondary watermark attacks.

Y. Zhang, B. Yang, and X.-M. Niu [14] proposed the first reversible watermarking scheme for relational databases. In this technique, histogram expansion is used for reversible watermarking of relational database. Zhang et al. proposed a method of distribution of error between two evenly distributed variables and selected some initial nonzero digits of errors to form histograms. Histogram expansion technique is used to reversibly watermark the selected nonzero initial digits of errors. This technique keeps track of overhead information to authenticate data quality. However, this technique is not robust against heavy attacks.

R. Sion, M. Atallah, and S. Prabhakar [4] proposed an encoding method for rights protection for categorical data.In this technique, if watermarks are altered then the percentage of data loss increases.

A. M. Alattar [12] proposed watermarking algorithm based on difference expansion of colored images. The algorithm uses spatial and spectral triplets of pixels to hide pairs of bits, which allows algorithm to hide large amount of data.

G. Gupta and J. Pieprzyk [13] proposed an improvement over the reversible and blind watermark scheme proposed by Gupta, G., Pieprzyk, J. In Reversible and blind database watermarking using difference expansion.

K. Jawad and A. Khan [15] proposed a Difference Expansion Watermarking based on Genetic Algorithm (GADEW), a reversible solution for relational database. GADEW improves upon the drawbacks mentioned by G. Gupta and J. Pieprzyk, in Reversible and blind database watermarking using difference expansion by minimizing distortions in the data, increasing watermark capacity and lowering false positive rate.

M. E. Farfoura and S.-J. Horng proposed a reversible data embedding technique called Prediction-error Expansion (PE) on integers to achieve reversibility. This technique is fragile against malicious attacks as the watermark information is embedded in the fractional part of numeric features only.

Diljith M. Thodi and Jeffrey J. Rodriguez [5] proposed a prediction-error expansion and histogram shifting technique as an alternative to embedding the location map. The proposed technique improves the distortion performance at low embedding capacities and mitigates the capacity control problem.

III. FRAMEWORK

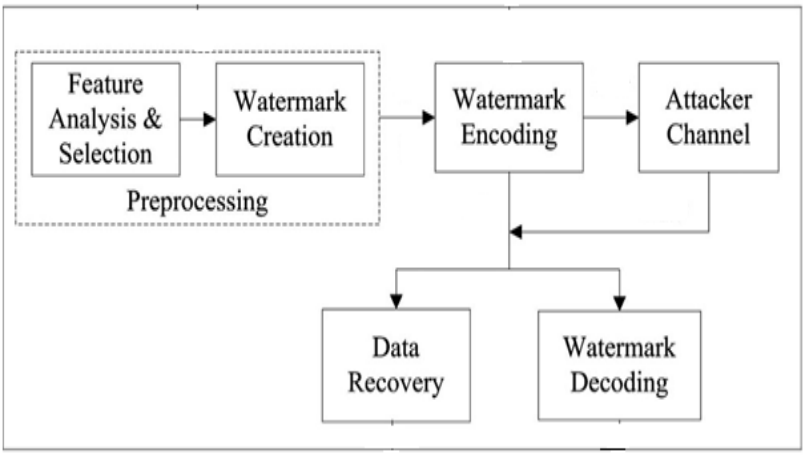

Figure 1: Architecture

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

There are four major phases: 1. watermark preprocessing; 2. watermark encoding; 3. watermark decoding; and 4. data recovery.

1. **Watermark Preprocessing:** In the watermark preprocessing phase, two tasks are accomplished. In this firstly, the suitable features for watermark embedding are selected and analysed. After feaure selection, the watermark is created.

2. **Watermark Encoding:** The main focus of watermark encoding phase is to embed watermark information in such a way that it does not affect the data quality. Watermark embedding phase embeds the watermark in accordance with the encoding strategies and data usability.

   After watermarking, the data is released to the attacker channel. The attacker channel refers to all such possible attacks. The attacks can modify some contents of the data with an aim to corrupt the embedded watermark; making the data suspicious.

3. **Watermark Decoding:** The Watermark decoding phase recovers watermark information effectively for detection of the embedded watermark. Data recovery phase mainly comprises the important task of successful recovery of the original data.

4. **Data Recovery:** After detecting the watermark string, some post processing steps are carried out for error correction and data recovery.The main responsibility of postprocessing is to use the decoded watermark bits, and convert these bits into the watermark information that was embedded as the watermark.

IV. SCOPE

Irreversible watermarking techniques make changes in the data to such an extent that data quality gets compromised. 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. In this, a novel robust and reversible technique for watermarking of relational databases is used. The main contribution of this is :

1. To overcome the problem of data quality degradation by allowing recovery of original data along with the embedded watermark information.
2. To achieve robustness in the presence of reversibility (ability to recover the watermark and the original data)
3. To keep the data useful for knowledge discovery.
4. To achieve an optimal solution that is feasible for the problem at hand and does not violate the defined constraints.
5. Allows recovery of a large portion of the data even after being subjected to malicious attacks.

V. CONCLUSION

Nowadays the security of data is becoming important especially in the collaborative environments. In irreversible watermarking techniques the data quality gets degraded and the original data could not be recovered.
In this the reversible watermarking technique has been proposed that is capable of recovering the original data. It allows recovery of a large portion of the data even after being subjected to malicious attacks.

REFERENCES

[1] Saman Iftikhar, M. Kamran, and Zahid Anwar, "RRW—A Robust and Reversible Watermarking Technique for Relational Data," IEEE Transactions on Knowledge and Data Engineering, vol. 27, no. 4, April 2015.
[2] F. A. Petitcolas, "Watermarking schemes evaluation," IEEE Signal Process. Mag., vol. 17, no. 5, pp. 58–64, Sep. 2000.
[3] J. T. Brassil, S. Low, and N. F. Maxemchuk, "Copyright protection for the electronic distribution of text documents," Proc. IEEE, vol. 87, no. 7, pp. 1181–1196, Jul. 1999.
[4] R. Sion, M. Atallah, and S. Prabhakar, "Rights protection for categorical data," IEEE Trans. Knowl. Data Eng., vol. 17, no. 7, pp. 912–926, Jul. 2005.
[5] D. M. Thodi and J. J. Rodriguez, "Expansion embedding techniques for reversible watermarking," IEEE Trans. Image Process., vol. 16, no. 3, pp. 721–730, Feb. 2007.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

[6] Y.-R. Wang, W.-H. Lin, and L. Yang, "An intelligent watermarking method based on particle swarm optimization," Expert Syst. Appl., vol. 38, no. 7, pp. 8024–8029, 2011.
[7] G. Gupta and J. Pieprzyk, "Database relation watermarking resilient against secondary watermarking attacks," in Information Systems and Security. New York, NY, USA: Springer, 2009, pp. 222–236.
[8] E. Sonnleitner, "A robust watermarking approach for large databases,"in Proc. IEEE First AESS Eur. Conf. Satellite Telecommun.,2012, pp. 1–6.
[9] Y.-C. Liu, Y.-T. Ma, H.-S. Zhang, D.-Y. Li, and G.-S. Chen, "A method for trust management in cloud computing: Data coloring by cloud watermarking," Int. J. Autom. Comput., vol. 8, no. 3,pp. 280–285, 2011.
[10] R. Agrawal and J. Kiernan, "Watermarking relational databases,"in Proc.28th Int. Conf. Very Large Data Bases, 2002, pp. 155–166.
[11] M. E. Farfoura and S.-J. Horng, "A novel blind reversible method for watermarking relational databases," in Proc. IEEE Int. Symp. Parallel Distrib. Process. Appl., 2010, pp. 563–569.
[12] A. M. Alattar, "Reversible watermark using difference expansion of Y. triplets," in Proc. IEEE Int. Conf. Image Process., 2003, pp. I–501,vol.1.
[13] G. Gupta and J. Pieprzyk, "Reversible and blind database watermarking using difference expansion," in Proc. 1st Int. Conf. Forensic Appl. Tech. Telecommun., Inf., Multimedia Workshop, 2008, p. 24.
[14] Zhang, B. Yang, and X.-M. Niu, "Reversible watermarking for relational database authentication," J. Comput., vol. 17, no. 2,pp. 59–66, 2006.
[15] K. Jawad and A. Khan, "Genetic algorithm and difference expansion based reversible watermarking for relational databases," J. Syst. Softw., vol. 86, no. 11, pp. 2742–2753, 2013.