IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727
PP 35-38
www.iosrjournals.org

An Improved Watermarking Technique for Relational Data

Vineeth A V[1], Ali Akbar N[2]
[1]*Mtech Scholar, Department of Computer Science Engineering, Govt Engineering College, Mananthavady, Wayanad, Kerala, India- 670644*
[2]*Associate Professor, Department of Computer Science Engineering, Govt Engineering College, Mananthavady, Wayanad, Kerala, India- 670644*

Abstract: *The rapid development of the Internet and its related techniques has allowed the tremendous ability to access and redistribute digital multimedia contents. In which, protecting ownership and controlling the copies of digital data have great importance. Watermarking technique have ownership rights over shared relational data and providing a means for tackling data tampering. When ownership rights are imposed using water-marking, the data undergoes certain modifications. As a result, the data quality gets decreased. The main aim is to maintain the ownership of Relational Database and also minimizing distortion in the watermarked content. In this paper, robust and the reversible watermarking approach to numerical relational data based on the genetic algorithm has been proposed. Therefore, reversible watermarking is required to ensures watermark en-coding and decoding by accounting for the role of all the features in knowledge discovery and original data recovery.*

I. Introduction

Now a days digital data can be accessed and exchanged with computer through internet is very simple task. When digital data is publicly available, it can be easily changed by unauthenticated user. So, securing data is difficult task and provides variety of solutions for protection of different data formats

Watermarking is one of the popular techniques that ensure security for ownership protection and tamper proofing for different data formats. Data hashing, Fingerprinting and serial codes are other techniques used for ownership protection[1]. These techniques can identify source for data leakage but cant protect data from being leaked. Digital watermarking ensure a strong method of protecting digital data from modifications, copyright protection by a secret code directly given into the data. The secret code can be used in various applications called watermark and has the property that it can provide ownership protection to digital content. The embedded watermark can subsequently be used for claiming and proving ownership. It's important to protect the ownership of databases, many times making copy of databases may get ignored. We care only about the relational database and is authentic and un-modified. If modified discovered and recovered the contents. The watermarking is restricted only in multimedia contents such as audio, video and images[2] etc. For transmission of messages from one party to another image watermarking is used. Processing of relational database watermarking differs that of watermarking techniques that are applied to multimedia data, cause is difference in properties of data. As relational data is independent and discrete compared to multimedia data is continuous. Thus watermarking particularly for relational databases was proposed very firstly by [3]. The technique was irreversible in nature i.e. it cant regenerate original data from watermarked data using secret key. Further after few years reversible watermarking techniques get proposed by [4] that can regenerate data without comprising original quality. Watermarking techniques mainly used to protect publicly available data from being tampered, protect ownership of that data, ensure integrity [5].

II. General Structure Of Watermarking

Mainly there are four phases for watermarking. such as watermark creation, watermark encoding, watermark decoding and data recovery. Fig.1 shows the general structure of water marking. Watermark creation- First it is essential to create optimal watermark for inserting watermark into the selected data of original database. Several methods can be used to create watermark such as Genetic algorithm, simulated annealing and particle swam optimization etc.

Watermark encoding- In this phase watermark created in first phase is embedded in selected part of data from relational database. There are several methods that can be applied to encode a watermark. Watermark decoding- Decoding is third phase in watermark-ing process which is used to extract embedded watermark from data which have been undergoes through watermarking. Way and method of encoding as well as decoding changes as technique changes. Data recovery- This phase is involved in overall watermark-ing process according to nature of watermarking i.e. whether it is reversible or irreversible. If watermarking is able to

generate original data then data recovery phase is involved in watermarking process otherwise it is not.

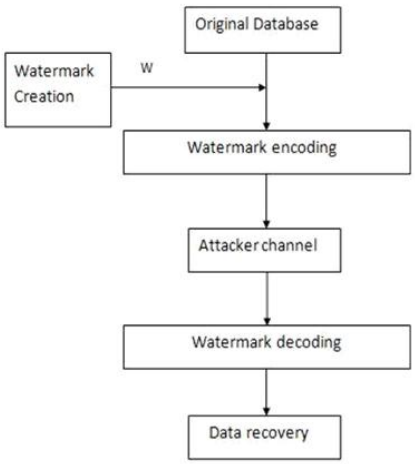

Fig. 1. General Structure Of Watermarking

III. Analysis Of Watermarking Techniques

Watermarking database relation is one of the several areas which demands research on focus owing to commercial implications of database theft. Digital watermarking for relational databases emerged as candidate solution that provides tamper detection, copyright protection, traitor tracing, and maintaining integrity to the relational data. Watermarking of relational databases can be grouped into two types based on their ability to regenerate original data. That is reversible watermarking and irreversible watermarking technique.

A. Irreversible watermarking techniques

Agrawal and kierman[6] proposed conventional irreversible database watermarking scheme for watermarking numerical values in databases. The assumption is watermark database can tolerate a small amount of errors. In this, the private key K is used for copyright verifiability and concatenated with primary keys of the tuple and is the seed for the pseudo random number generator algorithm. Then it decides the tuples, attributes with inside a tuple, and bit positions within an attribute to be marked. when the chances of attacker have access to the private key, it also detects the watermark with high possibility. The method survives several attacks and preserves mean and variance of numerical attributes. This scheme cannot be directly applied to watermarking categorical data.

Sion.R [7] introduced a novel method involves watermark-ing of categorical attribute by changing some of its value to other value to the attribute if such change is tolerable in certain applications. New watermark embedding channels were used for relational data with categorical types. Algorithm like, Novel watermark encoding algorithms are designed and analyzed important theoretical bounds including mark vulner-ability in this scheme.

B. Reversible watermarking

Recently, there has been little progress in database water-marking, most of the watermarking schemes modeled irreversible database watermarking scheme firstly proposed by Agrawal and Kiernan[8]. Reversibility is the potentiality to generate the original relation from the watermarked relation using a secret key. There are several techniques to implement reversibility, some of them have been mentioned below.

Techniques for handling ownership protection/copyright protection

A. Fr. Zung and Jun Ziang Pinn[1] proposed an efficient watermarking algorithm on the basis of inserting binary im-age watermarks in numeric mutilator attributes of selective database tuples. Here proposed technique is suitable for differ-ent area like e-banking, film industry and multimedia industry etc.

Tzouramanis[9] Proposed a watermarking technique that identifies true owner of database and results in resilience to range of attacks. Here algorithm presented in paper works on bits of tuples in relational data. After analysis of results produced, proposed technique protect embedded data from errors.

G.Shyamla[10] proposed a security mechanism, helps to resolve ownership conflicts over watermarked dataset in case of additive attacks. This method provides maximum accuracy and less distortion for decoding. It proves the robustness of watermarking scheme by analyzing its decoding accuracy under different types of malicious attacks using a real world dataset. It also provides solutions to resolve conflicting ownership issues in case of the additive attack.

Histogram expansion

Zhang et al[11] proposed first reversible watermarking of relational database to achieve less as well exact authenticate of relational databases via expansion on data error histogram. This method has distributive error within two evenly distributed variable as some initial nonzero digits of errors to form histograms. Histogram expansion technique reversibly watermark the selected nonzero initial digits of errors. This technique uses overhead information to authenticate data quality and it is not robust against heavy attacks.

DEW (Difference expansion watermarking technique)

Difference expansion refer to series of arithmetic operator on two integer value and a bit that result into a pair of modified integer from the original pairing integer the bit would be regenerated [8][9]. Difference expansion has previously been applied in image watermarking, but application in database watermarking introduction with an additional constraint of limiting distortion. Initially DEW was applied to secure image and after when it is needed to provide security to relational database it was applied to it. Proposing a high capacity algorithm based on the different expansion of triplets which is developed for embedding reversion watermark with reasonable level of image distortion. The algorithm uses a spatial and spectral tripling of pixel to hide a pair of bit which allows the algorithm to hide a large amount of data. But the methods arent either reversible or completely blind in nature.

SVR (Support Vector Regression)

Jung-Nan Chang and Hsien-Chu Wu [12] proposed scheme that detects database tamperer by embedded importance characterize of the originality of database. as ore additive with support vector regression (SVR) is applied to get the predicted each protective attributed value. The association rule of frequent pattern tree (FP-tree) data mining is used to detect the relationship existing with the protected attribute and others

as well in the database. Support vector regression (SVR)
is to be applied to predict each protective attribute value.

If the protective database is distort then SVR function will still predict the protected values. Then, an examination of the difference between original protective and predicted value allow the extraction of the watermark. Here such techniques are vulnerable to modication attacks because change in the expanded value will fail to detect information about watermark and original data.

GADEW (Genetic Algorithm based on Difference Ex-pansion Watermarking)

Asifullah Khan and Khurram Jawad[13] introduced new robust technique for reversible watermarking approach for the protection of relational databases. The approach utilizing genetic algorithm (GA) to reduce distort error and to improve watermark capacity. The proposed approach is reversible and therefore, distortion introduced after watermark insertion can be fully restored. GA introduces some randomness in DEW technique, thus making it is difficult to the attacker to pre-dict attribution. Security of the watermarking system is also enriched by reduction on the distort and minimize abrupt changes caused by DEW. They have achieved this by two measures added in the fitness function of GA, first by using the knowledge of their neighbor value of the relational database as well in second by minimizing the distortion introduced while selecting attributes resulting with minimum distortion.

PEEW (Prediction Error Expansion Watermarking Tech-nique)

M. E. Farfoura and S.-J. Horng, [11] presented a novel blind reversible watermarking method that ensures us the ownership of protection in the area of Relational Database of water marking. Whereas previous technique has been mainly concerned with introducing permanent errors in the actual data, as our approach assure 100 percent recovery of the original database. In the proposed method, as using a reversing data embedding technique so called prediction error expansion on the integers as well to achieve its reversible action. The watermark detection can be successfully completed even on 70 percent of watermarked relation tuples are deleted.

In the proposed procedure we're utilizing Genetic algorithm. Reversible watermarking manner (RRW) proposed to gain a most appropriate resolution that's attainable for the current issue what's more, does not abuse the characterized requirements. An ideal watermark worth is made through the GA and embedded into the chose highlight of the social database in one of this approach that the information satisfying and stay the undamaged. In RRW, shared data is utilized to choose a suitable (applicant) highlight from the database for watermarking. By, existing reversible watermarking methods, don't consider the shared data measure for deciding relative significance of highlights. In RRW, the learning of common data for each competitor highlight is likewise utilized to figure the watermark data. Consequently, it is guaranteed that the information quality won't be

influenced. Hence, RRW gives a powerful answer for information recuperation that is off learn-ing quality furthermore A robust regain the first information that is strong contrary to subset adjustment, subset cancellation and subset insertion assaults. The configuration of an astute reversible watermarking process for social information that guarantees information recovery without trading off learning quality furthermore A robust regain the first information that is strong contrary to subset adjustment, subset cancellation and subset insertion assaults.

IV. Conclusion

In this paper we proposed robust reversible watermarking techniques for numerical relational dataset. Irreversible watermarking techniques will make modification in such a way that the data quality will get negotiated. But for the proposed reversible watermarking technique, the data quality remains intact even after embedding watermark information. Here GA is proposed to find the optimum for the selection of features based on MI. Here we mainly focus on watermarking numerical data of the relational databases. Even after being subjected to heavy attacks large portion of the data is able to recover from the original data. This is the main contribution of this paper. This approach improves the performance by combining all the efficient features of the previous techniques.

References

[1]. Jun Ziang Pinn and A. Fr. Zung, "A new watermarking technique for secure database", International Journal of Computer Engineering Applications, Vol. I, No. I.

[2]. P. W. Wong and N. Memon, "Secret and public key image watermarking schemes for image authentication and ownership verification", IEEE Trans. Image Process., vol. 10, no. 10, pp. 15931601, Oct. 2001.

[3]. 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.

[4]. Udai Pratap Rao, Dhiren R. Patel, Punitkumar M. Vikani, "Relational Database Watermarking for Ownership Protection", 2nd International Conference on Communication, Computing and Security ,2011.

[5]. G.Shyamala, I.Jasmine Selvakumari Jeya, M.Revathi "Secure and Reliable Watermarking in Relational Databases", International Journal of Computer Trends and Technology (IJCTT) volume 11 number 1May 2014

[6]. Rakesh Agrawal Jerry Kiernan, Watermarking Relational Databases", Proceedings of the 28th VLDB Conference,Hong Kong, China, 2002

[7]. Sion, R. "Proving ownership over categorical data", In Proceedings of the 20th IEEE international conference on data Engineering ICDE, April 2004

[8]. Yong Zhang, Bian Yang, and Xia-Mu Niu "Reversible Watermarking for Relational Database Authentication", IEEE International Conference on Control System, Computing and Engineering, Volume 1 Issue 2,2014.

[9]. Theodoros Tzouramanis "A Robust Watermarking Scheme for Relational Databases", 6th International Conference on Internet Technology and Secured Transactions, 11-14 December 2011, Abu Dhabi, United Arab Emirates 2011 IEEE

[10]. G. Shymala, C. Kanimozhi, S. P. KAVYA "An Efficient Distor-tion Minimizing Technique for Watermarking Relational Databases", International journal of scientific research and Technology research, Vol.04, Issue. 11, May 2015

[11]. J.-N. Chang and H.-C. Wu "Reversible fragile database watermarking technology using difference expansion based on SVR prediction", in Proc. IEEE Int. Symp. Comput., Consum. Control, 2012, pp. 690693

[12]. K. Jawad and A. Khan "Genetic algorithm and difference expansion based reversible watermarking for relational databases", in Proc. IEEE Int. Symp. Comput., Consum. Control, 2012.

[13]. 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.