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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 4, Issue 1, January 2016

Space Reservation in Reversible Watermarking

Nisha S Sarma, Anna Prathibha Shobak

M Tech, Dept. of CSE, Mangalam College of Engineering, Kottayam, Kerala, India

Assistant Professor, Dept. of CSE, Mangalam College of Engineering, Kottayam, Kerala, India

ABSTRACT: Relational database place an important role in the field of information technology. These databases are used to hold administrative information and more specialized data. So consequently they are vulnerable to various security threats including data tampering and ownership protection. Watermarking used in relational database is to verify the ownership protection ,integrity of data and copy right protection etc. Reversible watermarking helps to ensure the data quality along with data recovery. Many such technique will not provide data quality in a proper level. So a new technique called Space Reservation in Reversible Watermarking using Encryption (SRRWE).This technique used by reserving a space before encryption with traditional RRW technique. Experiments shows that the method can achieve real reversibility along with data quality.

KEYWORDS: Reversible watermarking,Data quality

I. Introduction

Digital watermarking is the act of hiding message related to a digital signal (an image, song, video) inside the signal itself.This hide a message inside a digital signal. However what separate them is their goal. Watermarking tries to hide a message related to the actual content , and it is commonly used as a cover to hide message content. Watermarking has been used in several countries, initially watermarks are founded in plain paper and in paper bills.The field of digital watermarking was developed during the last 5 years and it is now being used for many applications such as broadcast monitoring,owner identification etc. Watermarking has the property that it can provide ownership rights over the original data.This was provided by marking the watermarked bit to the original data which is unique to the owner.So that the embedded watermark can subsequently used for proving and claiming ownership. Watermarking has a property that it can provide ownership protection.Reversible watermarking provides data quality,which means that it can allow the original data recovery.So that it can be useful for knowledge discovery.Ability to recover the original data and watermark is a challenging task.So that reversible watermarking also ensues the original data recovery without significant loss.Based on the properties of data,the watermarking process in multimedia data and relational data are varying. This paper is organized in the following manner. Section II briefly explain the previous work in this area. The method is elaborated in Section III followed by some evaluation.The paper is concluded in Section VI.

.

II. Related work

Agarwal & Kerman proposed the first irreversible watermarking technique for relational databases in [1].This technique ensures bit positions of some of the attributes of some of the tuples contain specific values. It also uses a private key which is known only to the owner of the data. This key used for determining the tuples,attribute &specific bit values algorithmically. This technique is not robust against heavy attack.

Techniques using difference expansion of watermarking, [2] exploit methods of arithmetic operations on numeric features. For minimizing attacks watermark is embedded in the LSB positions of features in relational databases. But in robust and reversible watermarking [3] ,the selected features of the dataset have an optimum value based on the GA mechanism. Which ensures the data quality.Genetic algorithm based on difference expansion watermarking (GADEW) technique [4] reduces the drawback of distortions in the data and also increase the capacity of watermark.

Prediction-error expansion watermarking technique (PEEW) uses predictor to select features for embedding watermark information.This technique embedded the watermark information in the fractional part of numeric features. Reversible

DOI: 10.15680/IJIRCCE.2016. 0401110

watermark using difference expansion of triplet[7] using an algorithm that uses spatial and spectral triplets of pixels to hide pairs of bits. Which help to hide large amount of data.Whereas SRRW uses GA for inserting watermarked bits,which preserves the data quality.

The reversible watermark technique DEW,GADEW,PEEW in [2],[3],[4] respectively are not robust against large attacks and also these technique not consider the importance of knowledge discovery.

In SRRW technique, can handle non numerical data's in a better way.It uses GA for identifying best places for inserting watermarked bits and achieves high robustness against heavy attack. Also it uses Room Reservation Before encryption [8] technique that will ensures minimum distortions, therefore it can recover original data with data quality & lack robustness.

III. Proposed Algorithm

For improving the performance of reversible watermarking in relational database,uses a technique Room Reservation Before Encryption[8] commonly used in image.By using this technique it ensures original data recovery without loss of secrecy. Here first allocate room space for encrypting the data.Which give an excellent performance in the system. Encryption is done by using two algorithms (1)homomorphism[9] and (2) paillier[10].After that feature extraction and position of the watermarked bits are identified.

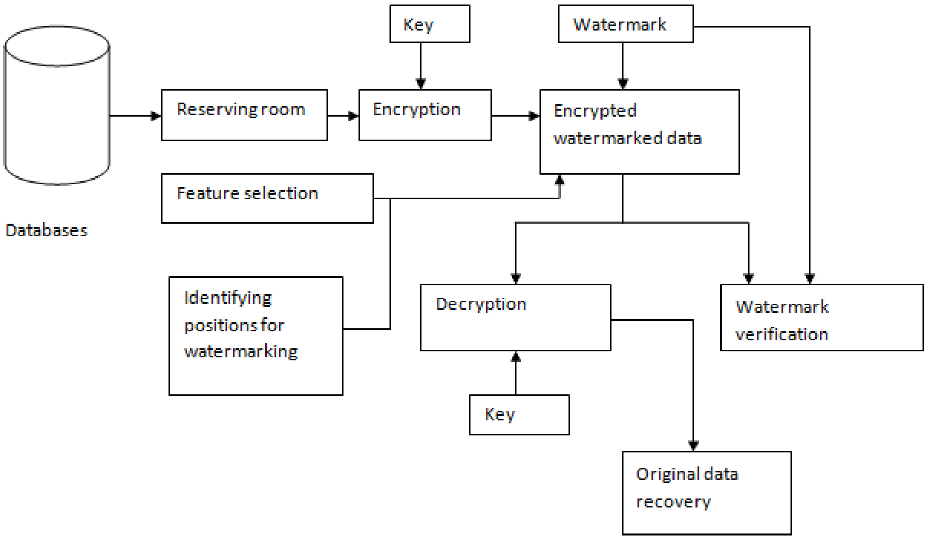
Homomorphism encryption allows the changing of different services without exposing the data to each independent services. This ensures the confidentiality of processed data. Fully homomorphic encryption scheme supports the arbitrary computation on cipher text.Since this will never decrypt its inputs.It can be run by an untrusted party without revealing its inputs and internal state.

Paillier cryptosystem is a probabilistic asymmetric algorithm for public key cryptography.This is an additive homomorphic cryptosystem which gives the public key for encryption.

IV. Architecture

A. *Architecture*

The architecture contains different databases. These databases are the input of the system.Among these one of the database is selected based on the requirement.First allocate the room for encrypting data by using LSB position after that add watermarked bit to the encrypted data.Also the feature extraction and position of watermarked bits are identified.



B. *Space Allocation*

The architecture contains different databases.These databases are the input of the system.Among these one of the database is selected based on the requirement.First allocate the room for encrypting data by using LSB position after that add watermarked bit to the encrypted data.Also the feature extraction and position of watermarked bits are identified.

C. *Data hiding in encrypted data*

Encryption can be done by using homomorphism or pailler's [9],[10] methods.After a data hider acquires the encrypted data ,he can embed some watermarked data in the LSB positions.So that no one can recovered original data.Also encryption of data can be done according to a data hiding key.If anyone who does not possess the data hiding key could not extract the original data.When one can get data hiding key he can decrypt the LSB bits and extract the additional data.The whole process is entirely operated on encrypted domain.It avoids the leakage of original content. When requesting for updating information of encrypted data's, the database manager, then, updates information through LSB replacement and encrypts updated information according to the data hiding key all over again. As the whole process is entirely operated on encrypted domain, it avoids the leakage of original content.

D. *Data Recovery*

An authorized user can recover the original data as it is by using the key.Same key issued for extracting the watermarked bits so that data recovery can be given in a better way.

V. RESULTS

Experiments are conducted on Intel Core i3 with CPU of 2.40 GHz and RAM of 4 GB. For brevity, heart disease medical dataset, containing more than 200 tuples is selected. SRRW was evaluated with respect to the data recovery and watermark detection rate.The results have shown that 100 percent accuracy in both watermark detection and data recovery than the existing method.

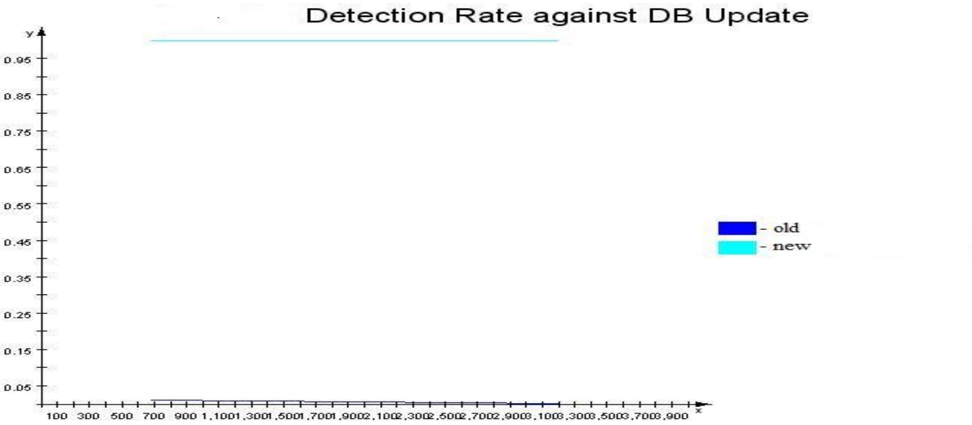


Fig.1. Detection accuracy

*Watermark detection:*Experiments shows that when more than 80% of the tuples are changed,watermark was detected with 100% accuracy.In the diagram,x axis denote number of tuples changed and y axis shows detection rate.

DOI: 10.15680/IJIRCCE.2016. 0401110

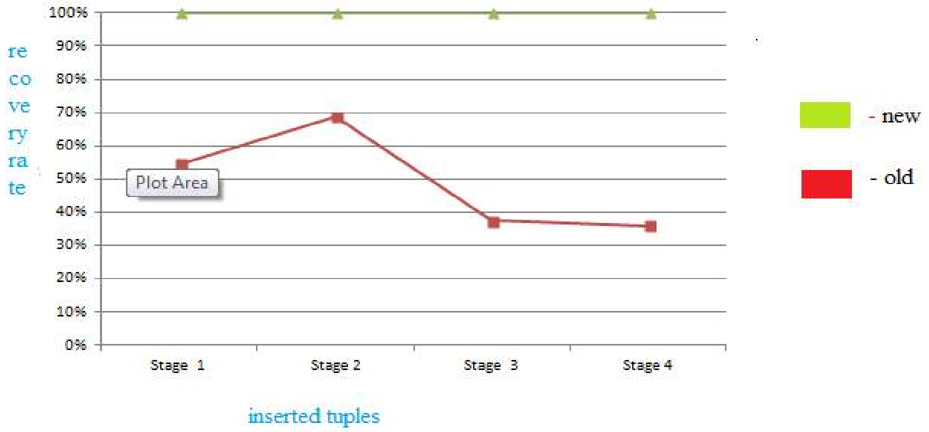


Fig.1. Data recovery

Data recovery:When an attacker tries to insert 50 percent tuples within the range of values of the watermarked feature,100 percent data is recovered in the proposed method. In this system, an attacker tries to insert, alter and delete 10, 20, 30, 40, 50,60,70 percent and up-to 100 percent of the data and the results are plotted in the graphs above.

VI. Conclusion and Future Work

The SRRW technique can prove the true ownership of the database's owner and provide full recovery of original databases with data quality. This technique provides robust and reversible watermarking for non numeric data of relational databases.The main contribution of this technique is that it can recover original data even after it is being subjected to malicious attack.

References

1. R. Agrawal and J. Kiernan, "Watermarking relational databases,"*in Proc. 28th Int. Conf. Very Large Data Bases*, 2002, pp. 155–166.
2. G. Gupta and J. Pieprzyk, "Reversible and blind database watermarking using difference expansion"*,in Pro. 1st Int.Conf.Forensic Appl.Tech Telecommun*.,*Inf.*,*Multimedia Workshop*,2008,p. 24.
3. A. M. Alattar, "Reversible watermark using difference expansion of triplets,"*in Pro. IEEE Int. Conf.Image Process*.,2003,pp. I-501,vol. 1.
4. G. Gupta and J. Pieprzyk, "Database relation watermarking resilien against secondary watermarking attacks," *in Information Systems and*
   a. *Security*.New York ,NY,USA:Springer,2009,pp,. 222-236.
5. 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. 690–693.
6. 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.
7. Adnam M .Alattar, "Reversible watermark using difference expansion of triplets",*Diagimarc corporation*,19801 SW 72nd Ave.Suite 25, Tualatin,OR 97062
8. Kede Ma, Weiming Zhang, Xianfeng Zhao, *Member, IEEE*, Nenghai Yu, and Fenghua Li " Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption", *IEE transactionns on information forensics and security* ,vol.8,no.3,march 2013 553.
9. Ron Rothblum, "Homomorphic Encryption: from Private-Key to Public-K Electronic Colloquium on Computational Complexity, "Report No. 146 (2010) September 21, 2010.
10. Pierre-Alain Fouque,Guillaume Poupard and Jacques Stern "Sharing Decryption In The Context Of Voting or Lotteries",*Ecole Normale Superieure Laboratoire d"infoematique* 45,rue d'Ulm F-75230 Paris Cedex 05.

BIOGRAPHY

Nisha S Sarma doing M Tech in Computerscience And Engineering at Mangalam College of Engineering. She receives B Tech degree in 2013 at saintgits college of engineering.Area of interest are datamining and security.

Anna Prathibha Shobak Assistant professor in mangalam college of engineering.She received M E ,CSE from Anna university.Publications are Secure multimatch packet classification based on signature toe (IJCSIT) and International Journal of computer Science and Information Technology vol-6(2),2015,1677-1679.