International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-3, September 2019

A Robust Watermarking Technique for Copyright Protection for Relational Databases

Murugan R, John T Abraham, Ibrahim Salim

Abstract*: Internet based digitization has been of rapid increase in the usage of database applications at an enormous rate in recent times. It is very difficult to secure the ownership of digital assets because all the data on the internet are available everywhere almost free of cost and anybody can access such data and claim their ownership. In current digital scenario not only images, videos, and audio are in digital form. Databases are also digitized in different models and used as a service in database applications, including areas such as finance, multimedia, personnel, etc. A huge amount of confidential and sensitive data which are available publically facing a variety of threats like illegal copying, illegal redistribution, tampering, forgery and authentication. Authenticity, integrity, confidentiality and copyright protection are most important security issues to be addressed with most importance. Copyright management is a serious issue in database applications because it is much easier for others to download and manipulate copyrighted databases from the Internet and later re-use without any control.

In this paper we proposed a robust watermarking scheme for copyright protection for relational databases, which protects the copy right information of the database even if the attacker tampers the data by changing the attribute values or reordering the tuples of the database. The proposed watermarking technique is robust since the watermark will not be lost even though the attacker tampers the data. The experiments show that the new method is efficient as well as effective for maintaining copy right information there by ensuring right protection to relational databases.

***Keywords*: Digital Watermarking, Relational Database, Copy Right Protection, Information Security, Database Attack.**

I. INTRODUCTION

The revolutionary growth of Internet offers a wide range of web-based services like database as a service, digital repositories and libraries, e-commerce, online decision support system etc. This increases the demand of protecting and authenticating the digital contents. Most of the researches are focused on the protection of images, audio, video etc. The demand for database protection and authentication using digital watermarking has started to receive attention because of its increased usage in real life applications. Inserting watermarking in relational database without losing its integrity is very difficult because databases have very little redundancy as compared to multimedia data. In other words, multimedia objects consist of large number of bits providing large cover to hide watermark; whereas the database object is a group of independent objects of tuples or attributes. The watermark has to be embedded into these tuples. Two of the main recognized application scenarios in the security of relational databases using digital watermarking are copyright protection, i.e. protecting the ownership and usage rights, and authentication, which aims at detecting and localizing malicious modifications.

In this paper, the research work proposed a robust watermarking method for copyright protection of relational databases with the following features:

- Robust:Benign updates or innocent modifications made to the watermarked relation will not affect the watermark.
- Distortion Free: The proposed scheme does not introduce any marks or errors in the underlying data. Hence this scheme is solely suitable for database applications which require zero distortion on data values. This is therefore best suitable for sensitive databases such as clinical databases.
- No Constraints in Data Type of Attributes: There is no restriction on the data type of the attribute selected for watermark insertion. The data type can be numeric, non-numeric, etc.

Tuple and attribute order independent: The embedded watermarks do not depend on a particular order of tuples or attributes.

The rest of the paper is organized as follows. Section 2 introduces the concept of digital watermarking and copy right protection and Section 3 presents an overview of related works. Section 4 demonstrates the proposed algorithms for embedding and extraction of watermark from the relational database. Section 5 describes the threat analysis and the experimental results and Section 6 concludes this paper with summaries.

II. DIGITAL WATERMARKING AND COPY RIGHT PROTECTION

Copyright protection is one of the important applications of digital watermarking. For copyright protection of databases, copyright information, copyright message, or logo image etc.

Manuscript published on 30 September 2019
* Correspondence Author
Murugan R*, Associate Professor, Department of Computer Applications, MES College Marampally, Ernakulam, Kerala, India. Email: mes.murugan@gmail.com Orcid Id: 0000-0003-3137-8236
John T Abraham, Assistant Professor in Computer Science, Bharata Mata College, Kochi, Kerala, India. Email: johntabraham@yahoo.com
Ibrahim Salim, Research Scholar, Research & Development Centre, Bharathiar University, Coimbatore, Tamilnadu, India and Assistant Professor, MES College Marampally, Ernakulam, Kerala, India. Email: mes.ibrahimsalim@gmail.com

are inserted or embedded in the commercial databases to be protected. The embedding algorithm incorporates copyright message which can then be extracted by the extraction algorithm to prove ownership. Although copyright notice does not guarantee the protection of copyright but still it is used. Generally, the digital assets like databases, software, books, images, audio and videos contain copyright notices, sometimes visible and sometimes invisible. It is necessary to achieve very high level of robustness when embedding watermark for copyright protection. Attackers can remove the copyright information through intelligent manipulation of the contents. Hence, it is necessary to embed copyright information in each and every piece of copyright content.

A digital watermark is considered to be some kind of information that is embedded into a digital asset for tamper detection, ownership proof, traitor tracing, etc. [1]. A digital watermarking may be perceptible or imperceptible, depends on its visibility in the watermarked content [2-3]. Again, a watermark may be robust or fragile. In robust watermarking, the modification to the watermarked content will not affect the watermark and in fragile type, the watermark gets destroyed when the watermarked content is modified or tampered with. To insert watermark into a digital content, we can follow any one of the two techniques such as spatial-domain technique or transform-domain technique. On the basis of the requirements of data, watermarks can be classified into blind or informed. In process of extraction of watermark, the original content is not required in the case of blind watermarking. But in the latter case, the original content is required. The zero watermarking technique is a type of blind watermarking in which the original content is not modified while embedding the watermark.

Watermarking techniques used for text and multimedia could not be used for watermarking relational databases. The relational data defers from multimedia data in many respects: (i) Few Redundant Data: Multimedia objects consists of large number of bits providing large cover to hide watermark, whereas the database object is a collection of independent objects, called tuples. The watermark has to be embedded into these tuples, (ii) Out-of-Order Relational Data: The relative spatial/temporal positions of different parts or components in multimedia objects do not change, whereas there is no ordering among the tuples in database relations as the collection of tuples is considered as set, (iii) Frequent Updating: Any portion of multimedia objects is not dropped or replaced normally, whereas tuples may be inserted, deleted, or updated during normal database operations [4]. Similarly, watermarking techniques for text typically exploit special properties of text formatting and semantics. For example, watermarks are often introduced by altering the spacing between words and lines of text [5].

Most of the traditional watermarking techniques developed for the protection of relational databases introduce some errors to the underlying data during the watermark insertion process [6-20]. Though these distortions are assumed to be minor, they, however, inevitably reduce the quality of the protected data. For instance, attributes like salary, price and coordinates property might not tolerate such data alterations. In addition, any distortion to categorical data may be considered as significant. Another problem is the inherent conflict between robustness and imperceptibility of the watermark information. Generally, the more alterations introduced by watermark insertion, the more secure is the watermarking scheme.

III. RELATED WORKS

Many watermarking techniques have been proposed for integrity verification of relational database. Agrawal et al. introduced a watermarking technique based on numeric data type attribute and marking is done at bit-level [4]. This technique used markers to locate tuples to hide watermark bits in the least significant bits.

Sion et al. introduced a watermark technique for numerical data [3]. This technique also dependent on a secret key which used the most significant bits of the normalized data set. In this technique, the data set is divided into partitions using markers and the partition statistics is varied to hide watermark bits.

In [21], Li et al proposed a fragile scheme for tamper detection of categorical data. In this scheme, the database relation is first divided into partitions in which a watermark is embedded by physically modifying the order of tuples. The scheme does not allow any legal update.

In [22], H. M. EL-Bakry and N. Mastorakis proposed a new approach for protecting the ownership of relational databases. This approach is suitable for both textual and numeral data and this proposed technique used two different methods for generating secret function for both textual and numeric data.
A secret-key based watermarking technique for copyright protection of numeric database attributes was proposed by Ali et al. [23]. This scheme presented a combination of a hash-based message authentication code (*HMAC*) and a threshold generator based on odd numbers of register being combined in a simple way. The value “0” or “1” to be embedded in marking bit positions is determined by using the threshold generator; the idea being if more than half of the output bits are “1”, then the generator output is “1”, otherwise it is “0”.

A watermarking algorithm for relational database which is based on spread spectrum techniques has been presented by Fu et al. [24]. Assignment of different owners for different identification key to generate the special watermarking signal is the characteristic of this scheme. It then inserts the signal. The algorithm uses the technique of even parity checking and majority voting for the watermarking accuracy at the watermarking detection step.

The issue of joint ownership in the context of relational databases security has been explored by the watermarking scheme proposed in [25]. The database relation is first divide into logical groups in this method. The main secret (watermark) is then broken into multiple parts (which are separately concealed in the relation by LSB alteration) using Shamir’s secret sharing technique.

In [26] a better version of this scheme is offered. A method to establish proof of ownership based on the secure embedding of a robust imperceptible watermark in the relational database has been put forth by Rao and colleagues [27]. A watermarking method is formulated to achieve this process, which will watermark only the numeric attributes and introduce the traceability parameter in the watermark detection technique.

A different copyright protection watermarking method also proposed by Zhang et al. in [28] is based on the database content characteristics. The feature of this method is that some bits called local characteristics are extracted by the watermark insertion phase from the characteristic attribute of A_1 of tuple *t*. Those bits are then embedded into the watermark attribute A_2 of the same tuple.

We have deliberated on various Relational Databases watermarking techniques and categorized them in terms of robustness and fragile-ness. Robust schemes are further classified according to the data type (e.g., numeric or non-numeric), watermark information (e.g., single bit, multiple bit, image, speech, etc.), granularity level (e.g., bit level or distribution level), and watermarking errors. Fragile methods too are grouped into two classes: Distortion-based and Zero distortion. Besides, we have provided an overview of fingerprinting schemes for relational data.

IV. PROPOSED TECHNIQUE

Suppose $R(P_k, A_1, \ldots, A_n)$ is the database relation being watermarked, where P_k is the primary key attribute, and A_i $(i = 1, \ldots, n)$ are the non-key attributes. A variety of schemes is available for robust watermarking for copyright protection of relational databases. Algorithm by Li et al. [29] assumed that the relation being watermarked has a fixed order of attributes that either never change or else can be recovered. In other words, Li et al's scheme critically depends on the original order of the attributes. As a result, a modest alteration to the order of attributes will randomize the embedded watermark bits. Therefore, the scheme is vulnerable to attribute related attacks such as attribute sorting attacks which actually do not change data content. Hence specifically, the scheme is vulnerable to innocent attacks and malicious attacks. The Table- I describes the notations used in various sections of this chapter.

Table- I Notations

Symbol	Description
R	Original Relation
R_m	Marked Relation
P_k	Primary Key of the Original Relation
K	Secret Key
n	Number of Attributes
A_i	Name of i^{th} Attribute; $i = 1$ to n
H_p	Hash value of Primary Key
HA_i	Hash value of Attribute Names; $i = 1$ to n
CI	Copyright Information
WM_r	Registered Watermark
WM_c	Computed Watermark
Hash	Hash Function
CA	Certification Authority

A. Overview of the Approach

In our proposed technique, the copy right information of the database will be protected even if the attacker tampers with the data by changing the attribute values or by reordering the tuples of the database. The proposed watermarking technique is robust since the watermark will not be lost even though the attacker tampers with the data. In the proposed algorithm a watermark is logically embedded in the attribute names and not in the attribute values of the tuples. That is why even if any tampering with the data happens, the watermark is not lost. This shows its robustness. In the proposed algorithm, all the attribute names, except the primary key attribute are arranged in some order with the attribute hash value used a Hash function. After the ordering of the attributes using another Hash function, the copyright information bits are inserted in the attribute hash value, to get the Watermark Key. The Hash functions, Secret Key and the ordering of the attributes are known only to the owner of the database. This watermark key generated can be registered with a Certification Authority (*CA*) along with the Database ID, Secret Key and Primary Key of the relation, for ownership proofing.

This algorithm enables the owner of the database to allow the intended users of the database for reordering or even modification of tuples without affecting the Copyright Information. This also helps the data owner to define a secret order of the attributes during watermark insertion phase that can be used to recover at watermark detection phase. The proposed watermarking process involves two phases:

- ***Watermark Insertion***
- ***Watermark Detection***

B. The Process of Watermark Insertion

The algorithm which is used to insert watermark in the database is described in the watermark insertion phase. In fact, the inputs in the insertion phase are the original database, secret key and the copyright information. The secret key can be a logo or any image provided by the owner of the database and the copyright information can be a string of characters. The primary key will be extracted from the metadata of the Relational Database. The embedding process is depicted in Fig. 1 below.

The watermark insertion phase can be described by the following steps:

Step-1. Input the Original Database (*R*), Secret Key *(K)* and the Copyright Information *(CI)*.

Step-2. Find the combined Hash value of the Database, Primary Key with the Secret Key which is known only to the owner of the database.

Step-3. Find the Hash name value of all the non-key attributes based on the combined Hash value of the Database, Primary Key with the Secret Key.

Step-4. Sort the non-key attributes in the ascending or descending order of Hash name value.

Step-5. Obtain the watermark (WM_r) by combining the Hash name values of all the attributes.

Step-6. Register the Database, Secret Key *(K)*, Copyright Information *(CI)* along with the Watermark (WM_r) with the Certification Authority *(CA)*.

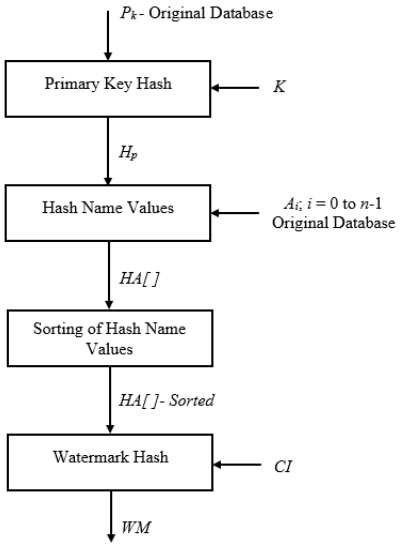

Fig. 1. Process of Watermark Insertion

C. Watermark Insertion Algorithm

The watermark insertion algorithm is shown in Algorithm-1. The Relational Data, Secret Key and the Copyright Information are the inputs and the Watermark Key is the output.

Algorithm-1. Watermark Insertion Algorithm

// Inputs are the Relational Data, Secret Key and Copyright Information //

1 Input R, K,CI

2 Obtain the Primary Key P_k

3 H_p = Hash(R || P_k || K)

4 For i = 0 to n-1

$HA[i]$ = Hash(A_i || H_p);

5 Sort $HA[i]$ in Ascending or Descending Order

6 WM_r = Hash(Combined $HA[i]$ for all i from 0 to n-1)

7 Register R, P_k, CI and WM_r with CA

D. The Process of Watermark Insertion

In detection phase, the extracting algorithm is something which extracts the watermark that can be used for verification of copyright information. The watermark key generated from the marked database is compared with the registered key for verification. Fig. 2 shows the watermark detection process.

The watermark detection phase can be described by the following steps:

Step-1. Input the Marked Database *(R_m)*.

Step-2. Obtain the Secret Key *(K)*, Copyright Information *(CI)* and the Original Watermark Key *(WM_r)* from the *CA*.

Step-3. Find the combined Hash value of the Marked Database, Primary Key with the Secret Key.

Step-4. Find the Hash name value of all the non-key attributes based on the combined Hash value of the Database, Primary Key and the Secret Key.

Step-5. Sort the non-key attributes in the ascending or descending order of Hash name value.

Step-6. Obtain the New Watermark (WM_n) by combining the Hash name values of all the attributes.

Step-7. Compare the generated Watermark from the marked database with the registered watermark (compare WM_n with WM_r).

Step-8. If there is similarity exists, then the output will be "Copyright Verification is Successful".
Or else if the keys are dissimilar then the out will be "Ownership Rejection Happened".

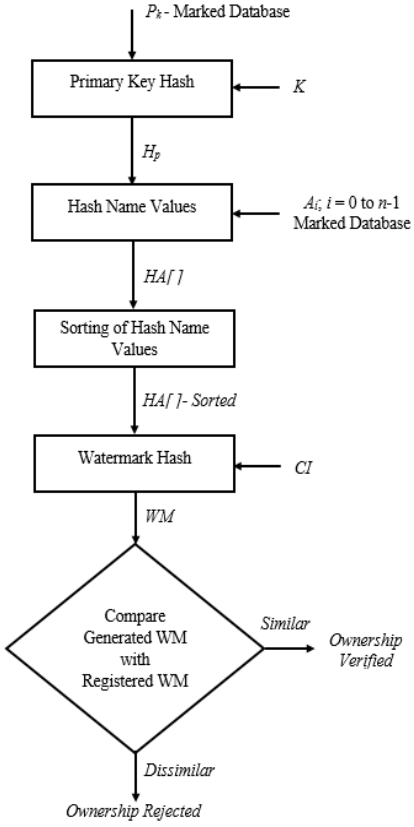

Fig. 2. Process of Watermark Detection

E. Watermark Detection Algorithm

The Marked Data is the only input for this algorithm. The Primary Key, Secret Key and the Copyright Information are fetched form the resource center. The output of this algorithm is also a Watermark, which can be used for comparison with the registered Watermark Key of the original database. Algorithm 2 describe the watermark detection algorithm.

V. THREAT ANALYSIS

The proposed scheme is of Robust type, that is the longevity of the watermark is not vulnerable to any type of attacks on the data values of the relation. This new method is useful for both innocent and malicious types of attacks of the data values. Reordering of attributes and sorting of tuples in a desired order constitute innocent attack since it does not change the data values.

But changing the values of an attribute, addition and deletion of tuples are malicious in nature. Generally, the attackers will not change the attribute names, they may instead change the values of the attributes or reordering of attributes/tuples. The research work analyzed the probability that the proposed scheme fails to detect the following typical database attacks: *innocent attack*, *attribute value modification*, *subset attack* and *superset attack*. A comparison has been done with work proposed by Ali Al-Haj and Ashraf Odeh [30] for above said attacks.

Algorithm 2 Watermark Detection Algorithm

// Input – Marked Database//

1 Input Marked database R_m

2 Obtain the *Primary Key* (P_k), *Secret Key (K), Copyright Information (CI) and registered* (WM_r) from resource center

3 H_p = Hash(R_m || P_k || K)

4 For i = 0 to n-1

$HA[i]$ = Hash(A_i || H_p);

5 Sort $HA[i]$ in Ascending or Descending Order

6 WM_n = Hash(Combined $HA[i]$ for all i from 0 to n-1)

7 If WM_n == WM_r then

Output *"Copyright Verification is Successful";*

Output *"Database Owner is :", CI;*

Else

Output *"Ownership Rejection Happened";*

A. Innocent Attacks

In innocent attacks, there will not be any change in the data values. The attacker may change the order of the tuples and/or change the order of attributes. But in the proposed scheme, finding the watermark key occurs only after sorting of the tuples and/or attributes in a predefined order that is known only to the owner. Hence the watermark scheme is robust to innocent attacks.

B. Attribute Value Modification Attack

In attribute value modification, data values of one or more attributes can be modified maliciously. Fig. 3 shows the watermark detection percentage of the proposed technique with the compared method. The changes in the data values of the tuples do not lead to changes in the resultant watermark and this makes the watermark scheme robust.

C. Subset Attack

Subset attack considers deletion or updating of a subset of the tuples or attributes of a watermarked relation. This type of malicious attack will not make any alterations in the watermark. It is presumed that the watermark has not been lost by deleting or updating the tuples on them. The watermark detection rate on subset attack is shown in Fig. 4.

D. Superset Attack

In this attack, some new tuples or attributes are added to a watermarked database. This causes no modification to the watermark during the detection process and the watermark scheme becomes robust. Fig. 5 depicts the watermark detection rate in the proposed technique.

The research work conducted and tested the algorithm of the new proposed scheme using java as the host language and MySQL as the Database Management System on a workstation with a non-transactional data, from GitHub, available at https://github.com/datacharmer/test_db. There are 300,024 tuples in the dataset, with 5 attributes having datatypes such as numeric, non-numeric and date.

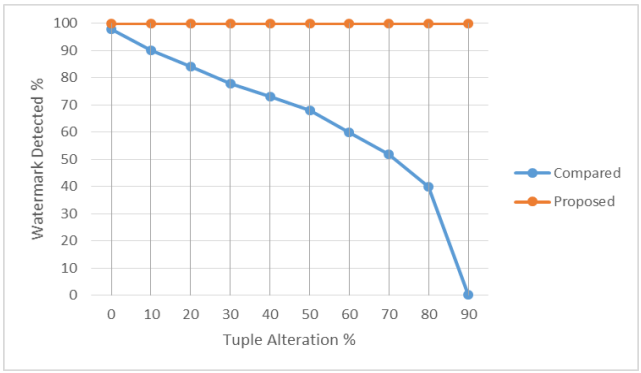

Fig.3 Robustness results due to the Value Modification Attack

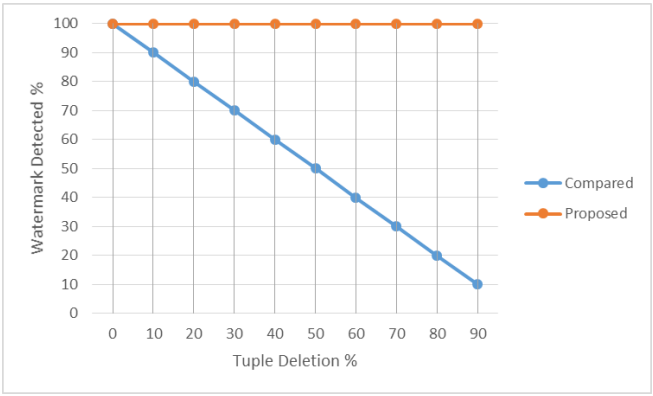

Fig. 4. Robustness results due to the Subset Attack

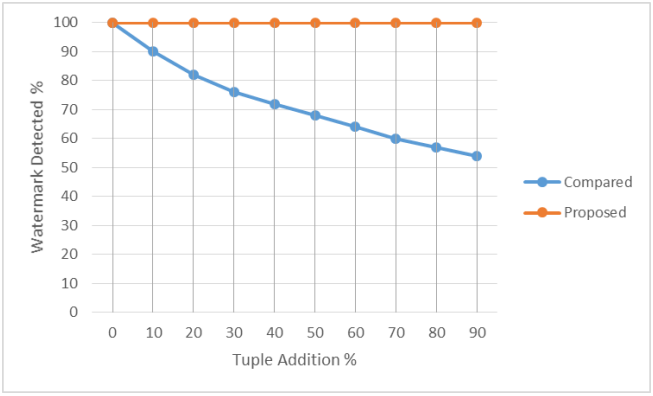

Fig. 5. Robustness results due to the Superset Attack

In this paper an analysis of the capacity of the algorithm has been done with Ali Al-Haj and Ashraf Odeh [30] to check the robustness of the watermark against various types of attacks.

Figures 3, 4 and 5 show the performance of the scheme presented in this chapter. In all the types of attacks the detection rate of the new scheme is 100%.

The research work verified to ensure that the proposed algorithm is Robust for innocent attacks, attribute value modification attacks, subset and superset attacks. SHA256 hashing method is used throughout the process and the Watermark generated for registration is of 64 characters in length.

VI. CONCLUSION

In this paper, the research proposed a Robust Watermarking Scheme to protect the Copyright Information for Relational Databases. The proposed scheme is based on the zero-watermarking approach that uses an image as secret key for generating Watermark. The embedding algorithm does not insert any information into the cover data. Instead, the watermark key constructed using the proposed technique, is registered with a Certification Authority which acts as the decision authority in case of any dispute with the publicly available data. The quality and usefulness of the protected data are preserved since no marks are inserted into the host data. Another meaningful advantage of our proposed method is that it is suitable for watermarking database attributes of any type. In other words, there is no constraint on the data types of attributes selected for watermark insertion. Based on both theoretical analysis and experiments, the research demonstrated that the proposed scheme is Robust and is effective in detecting the Copyright Information for malicious as well as innocent alterations in the data.

REFERENCES

1. Raju Halder, Shantanu Pal and Agostino Cortesi.(2010). Watermarking Techniques for Relational Databases: Survey, Classification and Comparison. In Journal of Universal Computer Science, vol. 16, no.21 (2010), 3164-3190.
2. Z. Jalil, A. M. Mirza, “A Review of Digital Watermarking Techniques for Text Documents”, IEEE, 2009.
3. Sion, R., Atallah, M., and Prabhakar, S. (2005). Rights protection for categorical data. IEEE Transactions on Knowledge and Data Engineering, 17:912–926.
4. Agrawal, R. and Kiernan, J. (2002). Watermarking relational databases. In Proceedings of the 28th international conference on Very Large Data Bases (VLDB ’02), pages 155–166, Hong Kong, China. VLDB Endowment.
5. N. Chotikakamthorn. Electronic Document Data Hiding Technique using Inter-character Space. In Proceedings of the 1998 IEEE Asia-Pacific Conference on Circuits and Systems (IEEE APCCAS). 1998, 419~422.
6. R. Yao, Q. Zhao, and H. Lu. A Novel Watermarking Algorithm for Integrity Protection of XML Documents. International Journal of Computer Science and Network Security. February 2006, 6(2): 202~207.
7. J.R.N. Baweu and H. Guo. Integrity Verification for XML Data. In Proceedings of the World Congress on Engineering and Computer Science (WCECS’07). San Francisco. 2007, 633~638.
8. R. Liu and H. Wang. Integrity Verification of Outsourced XML Databases. In Proceedings of the International Conference on Computational Science and Engineering (CSE '09). 2009, 207~212
9. R.C. Merkle. A Certified Digital Signature. In Proceedings of Advances in Cryptology (CRYPTO). 1989, 218~238.
10. S.A. Shah, X. Sun, A. Hamadou, and X. Wang. Combined Watermarking Solution for XML Documents. International Journal of Digital Contents Technology and its Applications (JDCTA). November 2011, 5(11): 69~78.
11. J. Guo, Y. Li, R. H. Deng, and K. Chen. Rights protection for Data Cubes. In Proceedings of Information Security Conference (ISC). 2006, 359~372.
12. J. Guo and W.-D. Qiu. Watermarking Data Cubes. Journal of Shanghai Jiaotong University (Sci.). 2009, 14(1): 117~121.
13. R. Sion, M. Atallah, and S. Prabhakar. Resilient Rights Protection for Sensor Streams. In Proceedings of the Very Large Databases Conference. 2004, 732~743.
14. R. Sion, M. Atallah, and S. Prabhakar. Rights Protection for Discrete Numeric Streams. IEEE Transactions on Knowledge and Data Engineering. 2006, 18(5): 699~714.
15. H. Guo, Y. Li, and S. Jajodia. Chaining Watermarks for Detecting Malicious Modifications to Streaming Data. Information Sciences. 2007, 177(1): 281~298.
16. H. Xian and D. Feng. Leakage Identification for Secret Relational Data Using Shadowed Watermarks. In Proceedings of the 2009 International Conference on Communication Software and Networks (ICCSN’09). 2009, 473~478.
17. R. Sion and Mikhail Atallah. Attacking Digital Watermarks. In Proceedings of Security, Steganography, and Watermarking of Multimedia Contents. San Jose, CA, USA. 2004, 848~858.
18. Y. Li, V. Swarup, and S. Jajodia. Defending Against Additive Attacks with Maximal Errors in Watermarking Relational Databases. In Proceedings of the IFIP WG 11.3 Working Conference on Data and Application Security. 2004, 81~94.
19. G. Gupta. Robust Digital Watermarking on Multimedia Objects. Ph.D dissertation. Computer Science. Macquarie University. August 2008 [149] R. Sion. Database Watermarking for Copyright Protection. In Handbook of Database Security. Springer Verlag. 2008, 297~328.
20. S. A. Shah, X. Sun, A. Hamadou, and A. Majid. Semi-Fragile Watermarking Scheme for Relational Database Tamper Detection. In Proceedings of the 2011 3rd International Conference on Future Networks (ICFN’11). 2011.
21. Li, Y., Guo, H., and Jajodia, S. (2004). Tamper detection and localization for categorical data using fragile watermarks. In Proceedings of the 4th ACM workshop on Digital rights management (DRM ’04), pages 73–82, Washington, DC, USA. ACM Press.
22. Hazem M. El-Bakry and Nikos Mastorakis.(2009). A New Watermark Approach for Protection of Databases. In Proceedings of the 9th WSEAS International Conference on APPLIED INFORMATICS AND COMMUNICATIONS (AIC ’09).
23. Y. H. Ali and B. S. Mahdi. Watermarking for Relational Database by using Threshold Generator. Engineering & Technology Journal. 2011, 29(1): 33~43.
24. Y. Fu, C. Jin and M. Chuanxiang. A Novel Relational Database Watermarking Algorithm. Pacific Asia Workshop on Intelligence and Security Informatics. LNCS. 2007, 4430: 208~219.
25. C. Jin, Y. Fu, and F. Tao. The Watermarking Model for Relational Database Based on Watermarking Sharing. In Proceedings of the International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP’06). 2006, 677~680.
26. Y. Fu, T. Ye, X. Niu, and Y. Yang. A Novel Relational Database Watermarking Algorithm for Joint Ownership. In Proceedings of the International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP’08). 2008, 985~988.
27. B.V.S. Rao and M.V.N.K. Prasad. Digital watermarking for relational databases using traceability parameter. International Journal of Computer Applications in Technology. 2009, 35(2-4): 113~121.
28. Y. Zhang, X. Niu, D. Zhao, J. Li, and S. Liu. Relational Databases Watermark Technique based on Content Characteristic. In Proceedings of the 1st International Conference on Innovative Computing, Information and Control (ICICIC ’06). Beijing, China. IEEE Computer Society. 2006, 677~680.
29. J.R.N. Baweu and H. Guo. Integrity Verification for XML Data. In Proceedings of the World Congress on Engineering and Computer Science (WCECS’07). San Francisco. 2007, 633~638.
30. A. Odeh and A. Al-Haj. Watermarking of Relational Database Systems. In Proceedings of the First International Conference on the Applications of Digital Information and Web Technologies (ICADIWT’08). 2008, 270~274.

AUTHORS PROFILE

Dr. Murugan R received his PhD in Computer Science from Bharathiar University, Coimbatore. His other qualifications include MCA, MPhil (Computer Science), DRDBMS. He has 21 years of experience in teaching and currently works as an Associate Professor and HEAD of the Department of Computer Applications at MES College Marampally (NAAC reaccredited with A+ in 2019), Aluva, Kochi, Kerala. His research interests include Information Security, Database Management System and Data Mining and has published 11 research articles in International and National levels. He served the Department of Vocational Studies as a Nodal Officer for more than 6 years. He guides and mentors aspirants in research projects and software application developments with his academic and IT industrial experiences. He has achieved the Best Performing Teacher Award twice. He is also a member of various professional bodies.

Dr. John T Abraham received his PhD in Computer Science in 2001. His other qualifications include MCA, MSc(Information Systems and Management), MPhil, MTech(IT), DDBM, DAS400, DMF, DST. Till 2012 he worked in various colleges like Vaishnav College, Chennai, S A Engineering College Chennai, Vel Tech Engineering College Chennai, Saintgits College of Engineering Kottayam, KVM College of Engineering and Technology Cherthala, Mount Zion Engineering College Kadammanitta in various positions like Academic Director, Head of the Department etc. Two years he worked in the Faculty of Information Technology, Misurata University, Libya. From 2012 onwards he is working in Bharata Mata College, Kochi, Kerala. His research interests include Data Base Management Systems, Management Information Systems, Software Engineering etc. and published around 100 research articles in International and National level. He has also received many International and National level awards and is a member of various professional bodies.

Ibrahim Salim M was born in Kothamangalam in 1977. He is an assistant professor in the Computer Applications at MES College Marampally, Aluva, Kochi, Kerala. Currently he is doing his PhD in Data Mining at Bharathiar University, Coimbatore. His qualification includes MPhil (Computer Science) and MCA. His research and publication interests include Data Mining and Computer Networks. He has presented papers at various conferences. His teaching areas are Computer Networks, Operating Systems and various programming papers. He is the NCC officer of his college from 2010 onwards. He was the member of Board of studies of Computer Applications at Mahathma Gandhi University, Kottayam, Kerala. He conducted various seminars and conferences.