ISSN: 0975-766X
CODEN: IJPTFI
Available Online through
www.ijptonline.com
Research Article

A NEW WATERMARKING APPROACH FOR RELATIONAL DATABASE WITH ONTOLOGY

G.Balaji[1], Dr.B.Muthu Kumar[2]
[1]Final year MCA Student, Sathyabama University, Chennai - 600119, Tamilnadu, India.
[2]Professor, Department-MCA, Faculty of Computing, Sathyabama University, Chennai - 600119, Tamilnadu, India.
Email: infoofbalaji@gmail.com

Received on 18-02-2016 *Accepted on 20-03-2016*

Abstract

The relation of watermarking database has been expressed for identifying the privacy of data, relational data character identification which posing the unique challenges with watermarking technique, and the popular properties of watermarking system to the relational data. It is presenting the enhanced technique of watermarking for geared relational data for determination of piracy, which proposing the scheme of watermarking for relational database that contains data in category for solving the ownership problems. This paper is proposing the novel scheme for robust watermarking database; the original database is standing for data distortion semantic control and for QIM (Quantization Index Modulation) extension to numerical attributes of circular histogram.

The semantic control of distortion over the process of embedding system is proposing the detection of existing link of semantic attribute's value in tuple with ontology. This technique could avoid the rare and incoherent record which is occurring for the interpretation of data or betrayal of the watermark presence. The embedding of watermark is being conducted within relative modulation of the angular position with center of mass for circular histogram for numerical attribute.

Theoretically, this technique has demonstrated robust performance for the scheme against of general attacks. The technique is capable for protection of copyright, tracing of traitor and identification of owner purposes. The proposed technique is producing the better result for watermarking over the relational database.

Keyword*:*

Robust watermarking database, Quantization Index Modulation.

1. Introduction

The duplication of the images, software, audio, text and video is being a big concern for digital assets owners. The schemes are generally based on the digital watermark insertion in the data [1]. The watermark technique is introducing the enhancement over watermarked objects with some intentional errors. The proposed intentional errors are calling the marks and each mark constituting the watermark [2]. The widespread use of internet and computers, exchanging and accessing the digital content has been become a common task. The digital content could be easily modified and duplicated; there could be big deal for the concern of intellectual property and integrity for the protection of data property. In short, the digital watermarking technology is referring the secret of imperceptible embedded signal over original data [3]. The proposed work is concerning over the scheme of digital watermarking for the integrity of database. There are many fragile schemes for watermark technique has been proposed in recent years, which were about to watermarked the multimedia content. Most of the watermark technique is focusing on the digital images. In recent days, some of the researchers have introduced the value of watermark technique database and has proposed several schemes for protecting the relational database [4]. However these proposed techniques are robust in scheme and being designed for the protection of copyright. So, it is important for protecting the database ownership, the database copies may not be in consideration. The considerations over the relational database to modified and authenticate the content for recovery and detection [5]. The previous researchers have assumed the things generally for the data interpretation which could be perturbed for the alteration being carried out within the message insertion in database. The data's are in the database is not secured, because it will not be protecting the existing user from any malicious or unwanted users. The operations like update, delete and insert could be done within every particular users. To overcome on these issues, the proposed technique is better within the watermarking and perturbation by ontologies [6]. There is no more time is being taken for identification of the malicious or attacker issues in the large database. The proposed ontologies are capturing the related field's knowledge [7].

2. Related Work

The network over internet diversifying and proliferating around the globe, digital media accessibility is containing contents like videos, images and audios are more frequent [8]. The approaches of digital watermarking are ensuring the protection of ownership, digital data security and authentication of data. The author has presented a technique for extracting and embedding the watermark, which being applied in the spatial-domain/time-domain for transforming the

transmission signal domain. This absorbs the digital watermarking ideas by starting the possible attacks, classification, overview, performance analysis, comparative study, and limitation within several techniques of watermark [9]. The author of [10] has proposed the genetic algorithm as a primary concern for reaching at the every ameliorate fidelity and multimedia data robustness.

The watermarking of audio is a major research area. There is a general problem occurring in the methods of embedding data which affects the original data distortion inevitably over the embedding itself. The typical distortion couldn't be removed fully because of bit-replacement, truncation, and quantization in grayscale limit 0 to 255. So, the distortion is little perceptual and small models for minimizing the visibility, the distortion might be not acceptable for medical image or any sensitive information. Recently, the author of [11] has proposed a view over the developments in watermarking and data embedding algorithms with text embedding, image, video, or binary streams or host audio for video, video or image signal.

The data embedding is perceptually invisible or inaudible for the maintenance of source data quality. The data embedding could be adding the features for hosting the multimedia signal such as multilingual or dual language in the movie soundtrack for providing the protection over copyright. The discussion over the embedding procedure of data and the reliability and capability for delivering are the novel services. The author [1] has presented the technique for significance of semantic web over a day, proposing the main concern over the technique for semantic web to database web work. The ontology is playing a crucial role and acting crucially over the foundation creation in web semantic process.

3. Proposed Work

3.1 Overview

In this system we propose new control method of semantic distortion which takes ontology advantage over the database strategy. Ontology gives common vocabulary of a region and explanation, with various formality levels, the terms meaning and the link between them. Ontology has been applied successfully in various domains from extraction of data to annotation of image and retrieval.

In our knowledge, it has not yet been used to control distortion of watermarking. As we will manifest, one ontology gives semantic knowledge or database description that can allows us to recognize the permissible distortion of attribute in a tuple.

Overall Architecture

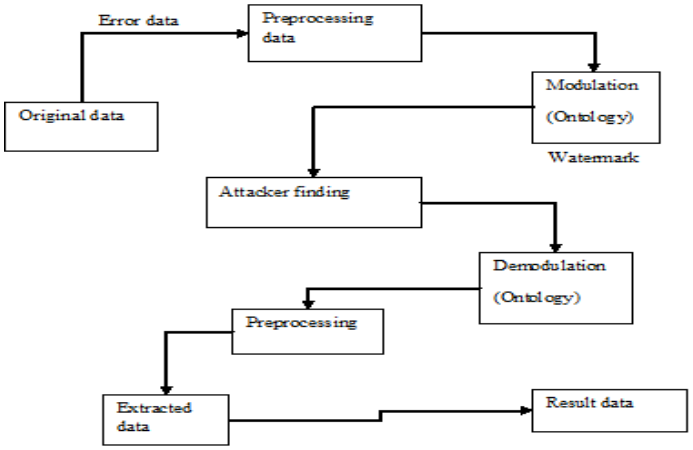

Figure 1: Overall Architecture.

3.2 Proposed Work Method

3.2.1 Defense Register and Verification: In this system the first process is users have to register for this application then only user can able to login. After that in the admin module first we will create Registration form. In this Data's are inserting at the same time data perturbation and watermarking the database are achieved.

3.2.2 Datapeturbation and Watermarking: In this system we use water mark technique, here admin only update the details and data's are updated in database (watermarking and data perturbation). Admin is authority person for add, delete, edit for any on of the data. After that all files can be seen in another page.

3.2.3 Attack Detection via Distortion Control: In this process, the registered users can login and view the defense information. But if any attacks happen in data (original data's are deleted or changed by attacker). The data will be changed in temporally. After that admin can view the files and detect the attack. If any attack happens in the data, it could not affect the original data.

4. **Result and Discussion:** In order to measure the performance of our proposed approach, a sequence of experiments on extracted dataset were conducted. Based on the following configuration our proposed method should be implemented

1) Intel Pentium(R),
2) Processor: Pentium IV,
3) Processer speed 2.90 GHz,
4) Clock speed: 550MHz,
5) Hard Disk: 20GB,
6) RAM: 128MB,
7) Cache Memory: 512KB

4.1 Cloud Tech Home

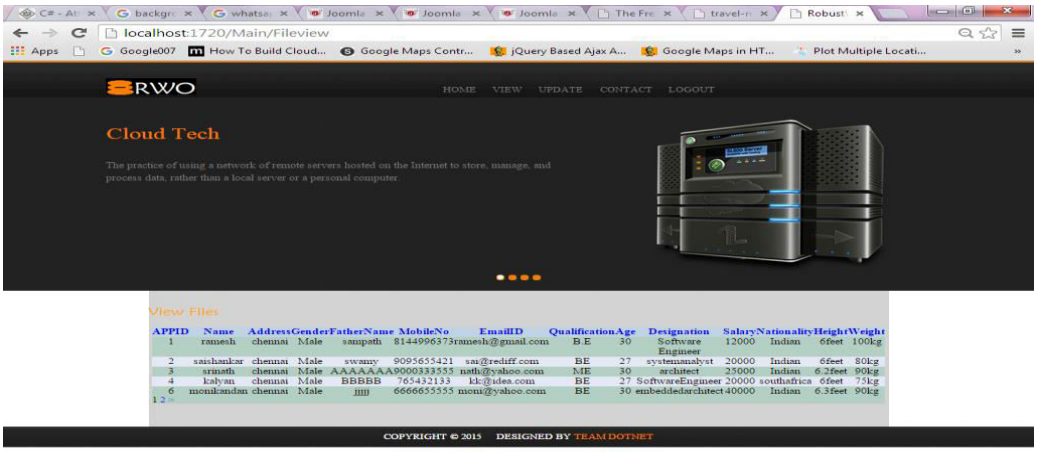

Figure-4.1: Cloud Tech Home.

The above mentioned figure 4.1 is presenting the view files scenario within the user's details such as name, address, mail, contact and other related details are being updated in the database.

4.2 Attacker Detection

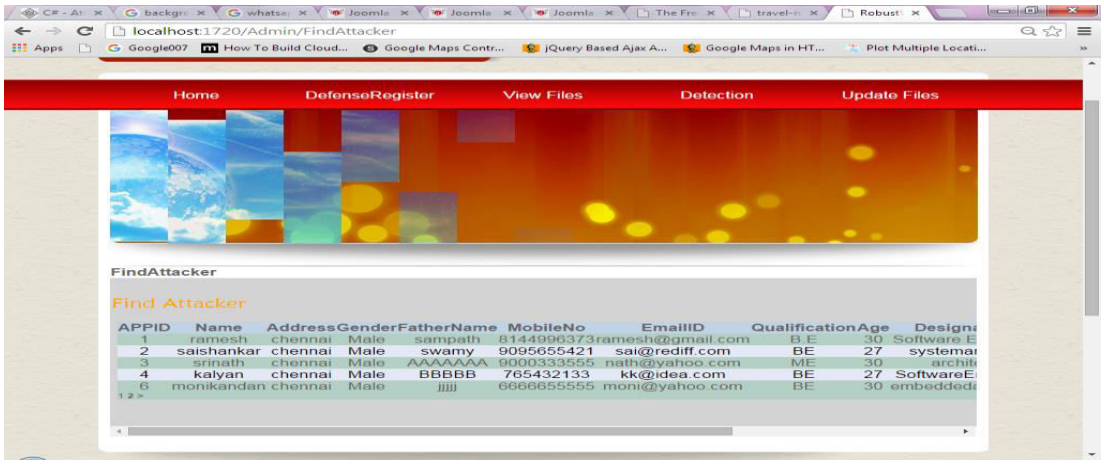

Figure-4.2: Attacker Detection.

The above mentioned figure 4.2 is presenting the attacker identification by the malicious activity and displaying the detail information of the every malicious user.

4.3 Attack Identification

Figure-4.3: Attack Identification.

The above mentioned figure 4.3 is presenting the attack identification over the system attack. The attackers are being classified within the proposed technique.

5. Conclusion With Enhancement

In this paper proposed to watermarking and perturbation with ontology for detect attackers in database management. The existing system problem is unauthorized user access database and change database information because modification delete insert etc. we solve the existing issue and propose watermark algorithm with ontology technique, it purpose to identity modify data base information and detect attacker with recovery the original data value information. Future enhance, improve the watermark technique and additional technique use to can't access unwanted users in database with securely.

6. Reference

1. Johnson NF, Duric Z, Jajodia S (2000) Information hiding: steganography and watermarking – attacks and countermeasures. Kluwer , Amsterdam.
2. Hamed khataeimaragheh1 and Hassan Rashidi, "A Novel Watermarking Scheme For Detecting And Recovering Distortions In Database Tables" International Journal of Database Management Systems (IJDMS) Vol.2, No.3, August 2010
3. Fridrich.J, Goljan.M, Du.M., (January 2001). Invertible authentication, in: Proc. of SPIE, Security and Watermarking of Multimedia Contents.
4. Agrawal.R, Kiernan.J., (2002). Watermark relational databases of the 28th Int Conference on Very Large Data Bases.
5. Guo.H, Li.Y, Liu.A, Jajodia.S., (2006). A fragile watermarking scheme for detecting malicious modifications of database relations. Information Sciences 176, pp 1350–1378.
6. Hamna k., Munira I. and NarmeenS..B., Web Accessibility Evaluation of News Websites Using WCAG 2.0, *Research Journal of Recent Science,* 3(1), 7-
7. Humaira, Naz Tabbasum and Sadiq Ayesha, "A Survey on Automatic Mapping of Ontology to Relational Database Schema" Research Journal of Recent Sciences ISSN 2277-2502 Vol. 4(4), 66-70, April (2015)
8. Siddarth Gupta1, Vagesh Porwal, "Recent Digital Watermarking Approaches, Protecting Multimedia Data Ownership" an International Journal, Vol. 4, Issue 2, No.14 , March 201513 (2014)

9. Jessica Fridrich Miroslav Goljan Rui Du, “Lossless Data Embedding—New Paradigm in Digital Watermarking” Received 20 May 2001 and in revised form 29 October 2001

10. Mitchell D. Swanson, Member, Ieee, Mei Kobayashi, And Ahmed H. Tewfik, “Multimedia Data-Embedding and Watermarking Technologies”, FELLOW, IEEE.

11. afzal humaira, naz tabbasum and sadiq Ayesha, “a survey on automatic mapping of ontology to relational database schema” Received 30th November 2014, revised 26th January 2015, accepted 12th December 2015.

Corresponding Author:

G.Balaji,

Email: *infoofbalaji@gmail.com*