ISSN: 0975-8585

Research Journal of Pharmaceutical, Biological and Chemical Sciences

A Robust and Reversible Watermarking (RRW) Technique Based on a Time-Stamp in Relational Data.

Sibyl Ann Jacob*, Vaishnoodevi Ramdas, and Mohana Prasad K.

Department of CSE, Sathyabama University, Chennai, Tamil Nadu, India.

ABSTRACT

Watermarking method is to recognizable pattern used to identify authenticity. Intentionally introduced pattern in the data is hard to find and destroy, robust against malicious attack. Watermarking, with no exemption, has been utilized for possession protection of various data formats—pictures, video, sound, programming, XML archives, geographic related information, content records, some legacy databases etc—that are utilized as a part of various application areas. As of late, intelligent mining strategies are being utilized on information, separated from social databases, to recognize intriguing examples (by and large covered up in the information) that give huge backing to leaders in making viable, precise, and important choices; thus, sharing of information between its proprietors and honest to goodness clients. The proprietor of the Relational Database installs the watermark information, the bends in the first information are kept inside of specific points of confinement, which are characterized by the ease of use requirements, to safeguard the learning contained in the information. The proposed calculation inserts all of a multi-bit watermark in each chose line with the goal of having greatest power regardless of the possibility that an assailant is some way or another ready to effectively degenerate the watermark in some chose part of the information set. The main aim of this paper is to maintain the ownership of Relational Database and also minimizing distortion in the watermarked content and prove the effectiveness of Robust and Reversible Watermarking (RRW) against malicious attacks.

Keywords: Watermarking, Relational database, Multi-bit watermark, Information.

Corresponding author

ISSN: 0975-8585

INTRODUCTION

Headway in information technology is assuming an expanding part in the utilization of data frameworks involving relational databases. These databases are utilized adequately as a part of shared situations for data extraction; subsequently, they are powerless against security dangers concerning proprietorship rights and information altering. As of late, computerized media is exceeded expectations because of the flourishing improvement of software engineering and the Internet innovation. By and by, free proliferation and advantageous control of computerized media source to the extensive business harms to the information proprietors and the suppliers. Consequently, computerized watermarking is acquainted with obstruct the aforementioned repudiation [1]. Computerized watermarking is a methodology of introducing information into cutting edge blended media. Computerized watermarking has come to the greater part of information proprietors and turns into a dynamic zone of examination [2]. Numerous specialists have displayed different watermarking techniques to install discharge information, copyright data, into advanced pictures keeping in mind the end goal to secure the mystery data. Furthermore, this process only allows an insignificant modification to the original data [3-6]. Generally, digital watermarking can be classified as visible and invisible watermarking. Invisible digital watermarking is a process of permanently embedding a secret data into digital image carrying information. Therefore, the presence of the watermark is virtually imperceptible by human sensory system [7]. Among visible watermarking, it is difficult to remove unless exhaustive and expensive human interventions are involved. One of the most important encounter problems in watermarking is that as the quality of image increases the robustness of the watermarking decreases and vice versa. An efficient and robustness watermarking method is that which conquer this most encountered problem professionally [8]. On the other hand, restoration of the original contents after extraction of the hidden data is crucial task in watermarking and known as reversible watermarking. A different reversible watermarking systems have been presented in the past composed works; as requirements be they can be generally portrayed into three sorts: lossless pressure based procedures, distinction extension (DE) methodologies, and histogram change HM) strategies [9].

In this paper, we execute another approach to manage make the watermark bits from Universal date and time. The Watermarking process includes Encoding and Decoding Phase. The Encoding phase consist of Data partitioning, Selection of data set for watermarking, Watermark embedding process. Decoding phase consist also these process to extract the Watermarked content.

LITERATURE SURVEY

Chip-Hong Chang et.al [7] proposed a transform domain watermarking scheme using Fuzzy-ART in binary image watermarking for image authentication. Their proposed Fuzzy- ART was utilized to locate the spectral positions and the modulating factors according to the perceptibility of the image. As they have embedded the cryptographically randomized watermark Information into the image, the embedding strength was efficient. Liu Jinhu et.al, [11] proposed a “quantization-based image watermarking in the dual tree complex wavelet domain”. They embedded each watermark bits by modulating a set of dual tree complex wavelet coefficients using quantization approach. When this method was applied, the effect of geometric distortion on the watermarked image has been reduced. Hong Peng et.al have proposed a blind image watermarking approach [12], which has combined the multi wavelet and support vector machine to effectively capture line-like, curvelike and wedge-like, contour-like features of image. They have used the mean value modulation technique to modulate a set of multi wavelet coefficients in approximation sub-bands, hence effects of the image distortion has been reduced when it was suffering from different attacks. SVMs classifier was proposed “to learn mean value relationship between watermark and coefficients in multi wavelet sub-bands”.

Yih-Chuan Lin et.al [10], proposes a quadtree segmentation based reversible watermarking. They have utilized the histogram shifting method to embed the data into the gray image. As this technique presented with block-by block embedding, quad tree segmentation methods has estimated the embedding capacity of each blocks. Xinpeng Zhang [9] has achieved the “good payload distortion performance of reversible data hiding by the proposed practical reversible data hiding scheme”. A content reconstruction problem in self-embedding systems has been stated in [13]. They have analyzed about the of the inherent restoration trade-offs. Based on this analysis, they have proposed the image authentication and reconstruction scheme. Huawei Ti et.al [2] proposed an efficient resynchronization.

ISSN: 0975-8585

PROPOSED SYSTEM MODEL

The proposed system architecture is shown in the figure 3.1. It has the following parts: Data Group Partitioning, Tuple selection for watermarking, watermark embedding, Edge detection Authentication and Watermark Extraction.

Data Group Partitioning

In this module includes the Data partitioning Relational Numerical Database Watermarking. Data Partitioning comes under Watermark Encoding Phase which has been done by owner of the Data Base (ie) Admin. The data partitioning algorithm parcels the information set into legitimate gatherings by utilizing data partitioning algorithm.

$$P(r) = H(K_s \,||\, H(rP_k \,||\, K_s)) \bmod m$$

Here,

rP_k - primary key of the tuple r,

H - cryptographic hash function Message Digest,

|| is the concatenation,

K_s - secret key.

Logical groups or Partitions has been arrived after applied this algorithm. Admin has to decide the groups' length that is m.

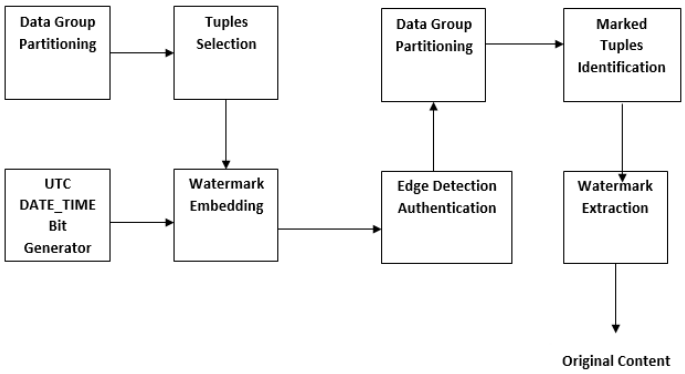

Fig 3.1: Proposed System Architecture

Tuples Selection for Watermarking

A Tuple is one record or one row in a Relational Database. In this phase, we select the particular tuples for embedding watermarked content. Threshold Computation is a strategy handled for each trademark. If the estimation of any property of a tuple is over its specific registered limit, it is decided for Encoding Process. The information choice edge for a trait is registered by using the going with scientific proclamation:

$$T = c^* \text{ Mean} + \text{Standard Deviation}$$

Here, c - confidence factor and a value should be 0 to 1.

In this walk, a cryptographic hash limit MD5 is related on the picked information set to pick just those tuples which have an even hash respect. This stride performs two destinations: 1) it further upgrades the watermark security by covering the character of the watermarked tuples from an interloper; and 2) it further reductions the measure of to-be-watermarked tuples to reason for limitation mutilations in the information set. On the off chance that the Hash Value Computation is Satisfied Select the tuples for Watermarking bits from chose tuples for Encoding process.

ISSN: 0975-8585

Watermark Embedding

The watermark creating limit takes date-time stamp as a data and after that makes watermark bits b1, b2 . . . bn from this date-time stamp. These bits are given as data to the watermark encoding limit. The date-time stamp "may" in like way see included substance assaults in which an aggressor needs to re-watermark the information set. To add to a watermarked information set, these watermark bits are installed in the essential information set by utilizing watermark implanting estimation. The proposed estimation embeds the greater part of a multibit watermark made from date-time in each picked segment. The watermark bits are embedded in the picked tuples using a solid watermarking limit. Our procedure implants every piece of the watermark in each chose tuple of every allotment.

Edge detection Authentication

Edge detection Authentication is proposed as an option answer for content based. It is fundamentally relies on upon pictures as opposed to alphanumerical. The fundamental contention here is that pass-pictures from the test set and after that he/she will be confirmed clients are better at perceiving and retaining pictures. Amid Registration stage Admin needs to give a few pictures to the client. In the enrollment stage the client should pick the pass-pictures for the confirmation stage. That picture must be Stored in Server For that Specific User. Amid Login stage Admin needs to change over the crude picture to a dim scale took after by Edge discovery picture. The thought here is the client will have a test set which contains bait and pass-pictures. The distraction pictures are haphazardly created by the plan amid the confirmation process. Then again, pass-picture will be the clients chose pictures. Essentially verification is basic; a honest to goodness client needs to accurately distinguish pass-pictures from the test set and after that he/she will be confirmed.

Watermark Extraction

Watermark Extraction process in the Decoding phase. The Watermarked Content has to be extracted only by legitimate user to give the proper ownership. If the User ownership content is matched by the Admin generated content, Decoding process has to done. Otherwise it’s not done.

EXPERIMENTAL RESULTS

Analyses are directed on Intel Core i3 with CPU of 2.40 GHz and RAM of 2 GB. For Company Employee dataset, containing more than 300 tuples is chosen. RRW was assessed for: (1) researching impact on the information nature of the basic information; (2) heartiness against pernicious assaults; and (3) reclamation of the first information. The information recuperation, watermark identification exactness and impact of RRW on information quality are assessed utilizing the contextual analysis of an organization worker dataset. A little arrangement of tuples from the same dataset are additionally utilized as a case to delineate the whole technique orderly in the accompanying figures. Vigor of RRW is exhibited through a broad assault examination. Our outcomes have demonstrated 100 percent precision in both watermark recognition and information recuperation. The trials performed, exhibit information recuperation in best case and also in most pessimistic scenario situations where Mallory tries to embed, modify and erase 10, 20, 30, 40, 50 percent and up-to 100 percent of the information.

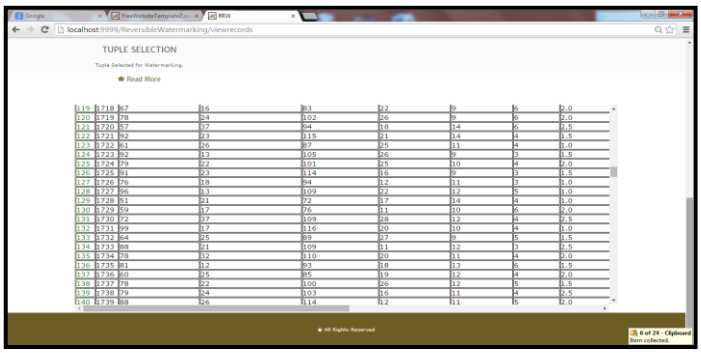

Fig 4.1: Tuple selection

ISSN: 0975-8585

The following screenshot shows the allocated partition group,

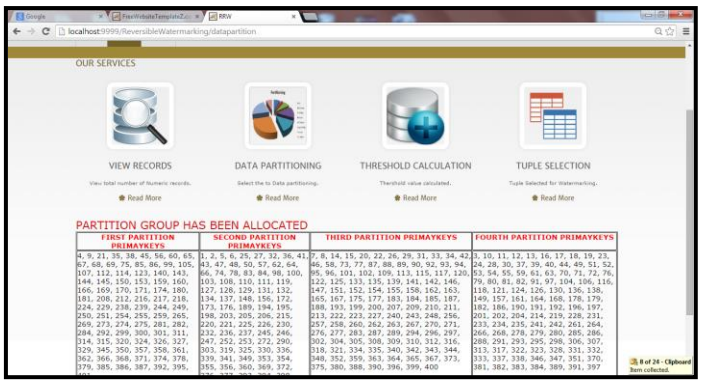

Fig 4.2

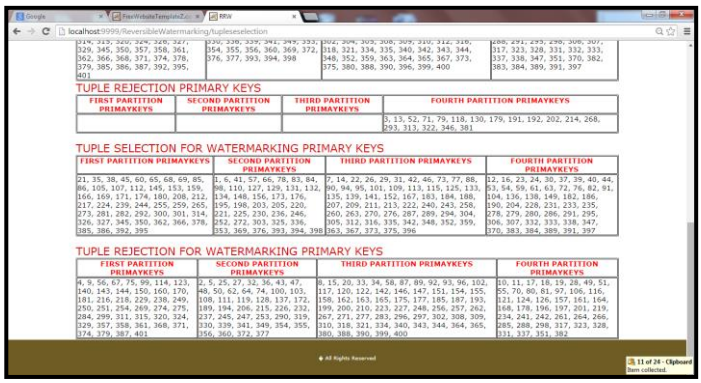

Fig: 4.3

The following screenshot shows the tuple rejection primary keys, tuple selection for watermarking primary keys and tuple rejection for watermarking primary keys.

CONCLUSION

In this paper, a novel robust and reversible method for watermarking numerical information of social databases is introduced. We accomplished to keep up the responsibility for Database furthermore minimizing contortion in the watermarked content demonstrates the viability of RRW against malevolent assaults. The fundamental commitment of this work is that it permits recuperation of a vast part of the information even in the wake of being subjected to pernicious assaults. RRW is additionally assessed through assault investigation where the watermark is identified with most extreme deciphering exactness in various situations.

REFERENCES

1. Wu Y.T, Shih F.Y Man, Cybern. B, Cybern, "Genetic algorithm based methodology for breaking the steganalytic systems," IEEE Trans. Syst, 2006, Vol. 36, no. 1, pp. 24–31.
2. Huawei Tian, Yao Zhao, Rongrong Ni, "LDFT-Based Watermarking Resilient to Local Desynchronization Attacks", IEEE Transactions on Cybernetics, 2013 ,Vol. 43, pp. 2190- 2201.
3. Zeng W, "Digital watermarking and data hiding: technologies and applications," in Proc. Int. Conf. Inf. Syst. Anal. Synth, 1998, vol. 3, pp.223-229.
4. Honsinger C. W, Jones P, Rabbani M, Stoffel J C, "Reversible recovery of an original image containing embedded data", 2001, U.S. patent: 6,278,791.
5. Fridrich J, Goljan M, Du R, "Invertible authentication," in Proc. Security Watermarking Multimedia Contents, 2001, pp. 197-208.

6. Caldelli R, Filippini F, Becarelli R, "Reversible watermarking techniques: an overview and a classification," EURASIP Journal on Information Security, 2010, vol. 2010, Article ID 134546, 19 pages.
7. Chip-Hong Chang, Zhi Ye, Mingyan Zhang, "FuzzyART Based Adaptive Digital Watermarking Scheme", IEEE Transactions on Circuits and Systems for Video Technology, 2005, Vol. 15, pp. 65-81.
8. Neethu V. Gopal and Madhu S. Nair, "Fuzzy-ART Based Geometrically Invariant Robust Watermarking Scheme", Engineering Letters, 2014, Vol. 22.
9. Xinpeng Zhang, "Reversible Data Hiding with Optimal Value Transfer", IEEE Transactions on Multimedia, 2013, Vol. 15, pp.316-325.
10. Yih-Chuan Lin, Tzung-Shian Li, "Reversible Image Data Hiding Using Quad-tree Segmentation and Histogram Shifting", Journal of Multimedia, 2011, Vol. 6, pp.349-358.
11. LIU Jinhua, SHE Kun, "Quantization-Based Robust Image Watermarking Using the Dual Tree Complex Wavelet Transform", China Communications, 2010, pp.1-6.
12. Hong Peng, Jun Wang, Weixing Wang, "Image watermarking method in multiwavelet domain based on support vector machines", The Journal of Systems and Software,2010, Vol. 83, pp. 1470–1477.
13. Paweł Korus, AndrzejDziech, "Efficient Method for Content Reconstruction with Self-Embedding", IEEE Transactions on Image Processing, 2013,Vol. 22, pp. 1134- 1147.
14. K. Mohana Prasad, Dr. R. Sabitha "Meta Physical Algorithmic Representation for Flawless Clustering**"** Journal of Theoretical and Applied Information Technology *(JATIT)*, ISSN : 1992-8645, Volume 76, NO 1,PP 82-87.
15. K.Mohana Prasad, Dr. R. Sabitha "Evolution Of An Algorithm For Formulating Efficient Clusters To Eliminate Limitations**"** *International* ournal of Applied Engineering J Research (IJAER*)*, ISSN 0973 – 4562, Volume 9, Issue 23, pp. 20111-20118.
16. K. Mohana Prasad, Dr. R. Sabitha," Yoking of Algorithms for Effective Clustering",Indian Journal of Science and Technology,ISSN: 0974-6846 Vol 8(22), IPL0269, September 2015,pp 1-4.