Secure Spread, Robustic and Reversible Watermarking Techniques for Relational Databases

G.Nithyavani[*1], P.Rajesh[2]
ME-CSE[*1], Assistant Professor –Department of CSE[2]
Kingston Engineering College[*1, 2]
Vellore, India[*1, 2]

***Abstract* - Watermarking is advocated to enforce ownership rights over shared relational data and for providing a means for tackling data tampering. When ownership rights are enforced using watermarking, the underlying data undergoes certain modifications; as a result of which, the data quality gets compromised. Reversible watermarking is employed to ensure data quality along-with data recovery. However, such techniques are usually not robust against malicious attacks and do not provide any mechanism to selectively watermark a particular attribute by taking into account its role in knowledge discovery. Therefore, reversible watermarking is required that ensures; (i) watermark encoding and decoding by accounting for the role of all the features in knowledge discovery; and, (ii) original data recovery in the presence of active malicious attacks. In this paper, a robust and semi-blind reversible watermarking (RRW) technique for numerical relational data has been proposed that addresses the above objectives.**

***Key Words* - Reversible watermarking, SVM, KNN, CSR Modeling.**

I.INTRODUCTION

In the digital world of today, data is excessively being generated due to the increasing use of the Internet and cloud computing. Data is stored in different digital formats such as images, audio, video, natural language texts and relational data. Relational data in particular is shared extensively by the owners with research communities and in virtual data storage locations in the cloud. The purpose is to work in a collaborative environment and make data openly available so that it is useful for knowledge extraction and decision making. Take the case of Wal-Mart—a large multinational retail corporation that has made its sales database available openly over the Internet so that it may be used for the purposes of identifying market trends through data mining.

II.PROBLEM DOMAIN

Data mining is the process of analyzing data from different perspectives and summarizing it into useful information-information that can be used to increase revenue, cuts costs, or both. Data mining software is one of a number of analytical tools for analyzing data. It allows users to analyze data from many different dimensions or angles, categorize it, and summarize the relationships identified.

III.OBJECTIVE AND SCOPE OF THE PAPER

Digital watermarking of multimedia content is more commonly known. Particularly image watermarking—a derivative of Steganography is an age-old practice allowing covert transmission of messages from one party to another by exploiting redundancy in common image formats. Our focus is to develop an information model through a statistical measure that identifies such features that do not have a significant effect on the decision making process. The goal is to make the data item must be secured from vulnerabilities and threats and to provide data quality and data recovery from malicious attacks.

IV.PROBLEM CHARACTERIZATION

Our focus is to develop an information model through a statistical measure that identifies such features that do not have a significant effect on the decision making process. Reversible watermarking techniques can ensure data recovery along with ownership protection. Fingerprinting, data hashing, serial codes are some other techniques used for ownership protection. Experimental studies prove the effectiveness of RRW against malicious attacks and show that the proposed technique outperforms existing ones. While the real extent and economic impact is hard to quantify, scientists and officials agree that cybercrime is a huge and still growing problem. According to literature, existing reversible watermarking techniques, do not take into account the mutual information measure for determining relative importance of features.

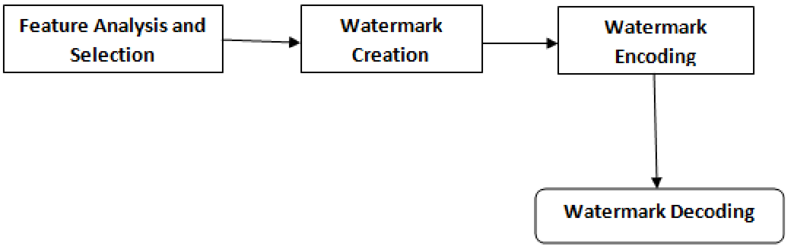

Fig. 1

V.FEATURES OF WATERMWRKING

The watermarking has a rich set of features. It includes;

1. The feature of my project is watermarking (hiding) the content in the video which will acquire more security than the existing one.
2. The another feature of this project is that we synthesize well-established research on technology acceptance models and criminology in the context of consumer-oriented cybercrime

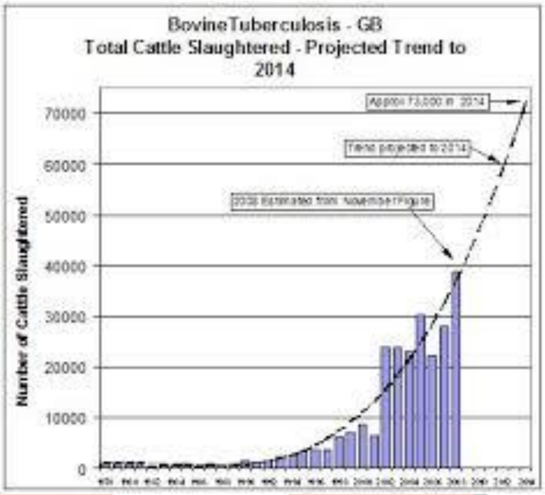

Fig. 2

VI.LITERATURE SURVEY

A body of literature has been conducted by several authors and a list of them is given below; A method for trust management in cloud computing: Data coloring by cloud watermarking.

1. Y.-C. Liu, Y.-T. Ma, H.-S. Zhang, D.-Y. Li, and G.-S. Chen.
   Data coloring method based on cloud watermarking to recognize and ensure mutual reputations. The experimental results show that the robustness of reverse cloud generator can guarantee users' embedded social reputation identifications. Hence, work provides a reference solution to the critical problem of cloud security.
2. D. M. Thodi and J. J. Rodriguez.
   The algorithm exploits the correlation inherent among the neighboring pixels in an image region using a predictor. The prediction-error at each location is calculated and, depending on the amount of information to be embedded, locations are selected for embedding. Data embedding is done by expanding the prediction-error values. A compressed location map of the embedded locations is also embedded along with the information bits. Our algorithm exploits the redundancy in the image to achieve very high data embedding rates while keeping the resulting distortion low.
3. M. E. Farfoura, S.-J. Horng, J.-L. Lai, R.-S. Run, R.-J. Chen, M. K. Khan.
   The authentication protocol based on an efficient time-stamp protocol, and we propose a blind reversible watermarking method that ensures ownership protection in the field of relational database watermarking. Whereas previous techniques have been mainly concerned with introducing permanent errors into the original data, our approach ensures one hundred percent recovery of the original database relation after the owner-specific watermark has been detected and authenticated.
4. E. Sonnleitner
   Watermarking databases is an emerging technological interest, especially within the frame of a vastly growing number of publicly available web-databases. In order to ensure integrity, detect malicious modification and protect ownership rights,
5. M. Kamran and M. Farooq, 2012.
   The major contribution of this paper is an information-preserving watermarking scheme to address the above-mentioned challenges. We model the watermarking process as a constrained optimization problem. Here demonstrated, through experiments, that our scheme not only preserves the diagnosis accuracy but is also resilient to well- known attacks for corrupting the watermark.
6. A.M. Alattar, 2003.

A spatial triplet is any three pixel values selected from the same spectral component, while a spectral triplet is any three pixel values selected from different spectral components. The algorithm is recursively applied to the rows and columns of the spectral components of the image and across all spectral components to maximize the hiding capacity. Simulation results show that the hiding capacity of the algorithm is very high and the resulting distortion is low.

7. M.Mitchell, 1996.
   GAs are applied to problems in statistical estimation and the results are compared to the output of standard software. It is argued that many statistical and mathematical restrictions that usually restrict modeling and analysis can be dispensed with by employing the GA as an optimization technique.
8. J. Cox, j. Kiliaa, j. Bloom, and T.shamoon, 2001.
   A new digital watermarking method through bit replacement technology, which stores mul-tiple copies of the same data that is to be hidden in a scrambled form in the cover image. An indigenous approach is described for recovering the data from the damaged copies of the data under attack by applying a majority algorithm to find the closest twin of the embedded information.
9. X. Li, B. Yang and T. zeng, 2012.
   Prediction-error expansion (PEE) is an important technique of reversible watermarking which can embed large payloads into digital images with low distortion. In this paper, the PEE technique is further investigated and an efficient reversible watermarking scheme is proposed, by incorporating in PEE two new strategies, namely, adaptive embedding and pixel selection. Unlike conventional PEE which embeds data uniformly, to adaptively embed 1 or 2 bits into expandable pixel according to the local complexity. This avoids expanding pixels with large prediction-errors, and thus, it reduces embedding impact by decreasing the maximum modification to pixel values. Meanwhile, adaptive PEE allows very large payload in a single embedding pass, and it improves the capacity limit of conventional PEE.
10. P.W. Wong and N.Memon, 2001.
    Describes a watermarking scheme for ownership verification and authentication. Depending on the desire of the user, the watermark can be either visible or invisible. The scheme can detect any modification made to the image and indicate the specific locations that have been modified. If the correct key is specified in the watermark extraction procedure, then an output image is returned showing a proper watermark, indicating the image is authentic and has not been changed since the insertion of the watermark. Any modification would be reflected in a corresponding error in the watermark. If the key is incorrect, or if the image was not watermarked, or if the watermarked image is cropped, the watermark extraction algorithm will return an image that resembles random noise. Since it requires a user key during both the insertion and the extraction procedures, it is not possible for an unauthorized user to insert a new watermark or alter the existing watermark so that the resulting image will pass the test. Here present secret key and public key versions of the technique

VII.CONCLUSION AND FUTURE ENHANCEMENT

The proposed approach is to secure the video data hiding based using Bit stream level data hiding and selective embedding. The is divided into frames and the secret data is embedded within the video frames that will provide a secure location for data hiding. Secret data embedding is performed using DWT and the data is hidden in one of the high frequency sub band of DWT by tracing pixels in that sub band. The embedding is done by entropy encoder using Huffman encoding that has unique prefix code. Use of ABE algorithm the security is enhanced that is secure data is converted to cipher text and then it will hidden in the frames embed the data into the video. Video and data are separated using decoding technique.

VIII.ACKNOWLEDGEMENT

I would like to take this opportunity to express my profound gratitude and deep regard to my guide, *Prof.N.Rajesh CSE, Kingston Engineering College*, for his exemplary guidance, valuable feedback and constant encouragement in completing this paper. His valuable suggestions were of immense help in getting this work done. Working under him, was an extremely knowledgeable experience. Also, I would like to extend my sincere gratitude to my parents and my brother for their constant support and encouragement in completing this paper.

IX.REFERENCE

[1] Y.-C. Liu, Y.-T. Ma, H.-S. Zhang, D.-Y. Li, and G.-S. Chen, “A method for trust management in cloud computing: Data coloring by cloud watermarking,” Int. J. Autom. Comput., vol. 8, no. 3, pp. 280–285, 2011.
[2] (2012, Feb. 4).Walmart to start sharing its sales data. [Online]. Available: http://nypost.com/p/news/business/walmart-opens-up
[3] (2013, Apr. 11). Identity theft watch. [Online]. Available: http:// scambook.com/blog/2013/ 04/identity-theft-watch-customerpasswords- stolen-from-walmart-vudu-video-service/
[4] (2013, Feb. 26). Securing outsourced consumer data. [Online]. Available: http://databreaches.net/securing-outsourced-consumer-data/
[5] (2012, Jun. 3). As patients’ records go digital, theft and hacking problems grow. [Online]. Available: http://kaiserhealthnews. org/Stories/2012/June/04/ electronic-health-records-theft-hacking.aspx
[6] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, “Secure spread spectrum watermarking for multimedia,” IEEE Trans. Image Process., vol. 6, no. 12, pp. 1673–1687, Dec. 1997.
[7] I. Cox, M. Miller, J. Bloom, and M. Miller, Digital Watermarking. Burlington, MA, USA: Morgan Kaufmann, 2001.
[8] P. W. Wong, “A public key watermark for image verification and authentication,” in Proc. IEEE Int. Conf. Image Process., 1998, vol. 1, pp. 455–459.

[9] 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. 1593– 1601, Oct. 2001.
[10] F. A. Petitcolas, “Watermarking schemes evaluation,” IEEE Signal Process. Mag., vol. 17, no. 5, pp. 58–64, Sep. 2000.
[11] J. T. Brassil, S. Low, and N. F. Maxemchuk, “Copyright protection for the electronic distribution of text documents,” Proc. IEEE, vol. 87, no. 7, pp. 1181–1196, Jul. 1999.
[12] R. Agrawal and J. Kiernan, “Watermarking relational databases,” in Proc. 28th Int. Conf. Very Large Data Bases, 2002, pp. 155–166.
[13] R. Sion, M. Atallah, and S. Prabhakar, “Rights protection for categorical data,” IEEE Trans. Knowl. Data Eng., vol. 17, no. 7, pp. 912– 926, Jul. 2005.
[14] S. Subramanya and B. K. Yi, “Digital rights management,” IEEE Potentials, vol. 25, no. 2, pp. 31–34, Mar.-Apr. 2006.
[15] P. E. Gill, W. Murray, and M. A. Saunders, “Snopt: An sqp algorithm for large-scale constrained optimization,” SIAM Rev., vol. 47, no. 1, pp. 99–131, 2005.
[16] K. E. Parsopoulos and M. N. Vrahatis, “Particle swarm optimization method for constrained optimization problems,” Intel. Technol.–Theory Appl. New Trends Intell. Technol., vol. 76, pp. 214– 220, 2002.
[17] R. Hassan, B. Cohanim, O. De Weck, and G. Venter, “A comparison of particle swarm optimization and the genetic algorithm,” in Proc. 46th AIAA/ASME/ASCE/AHS/ASC Struct., Struct. Dyn. Mater. Conf., 2005, pp. 1–13.