International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

A Survey Paper on Right Protected with Provable Distance based Mining

Snehalata S. Thorat[1], R. P. Kulkarni[2]

[1]ME Student, Department of Computer Engineering, Sinhagad Institute of technology, University of Pune, Maharashtra, India

[2]Department of Computer Engineering, Sinhagad Institute of Technology, University of Pune, Maharashtra, India

Abstract: ***This paper exhibits a survey on diverse advanced watermarking strategies and their properties. The primary explanation behind advancement of watermarking exploration is to secure scholarly properties of the computerized world. Since the recent innovation makes it simple copying the content without any limitations and altering without any restrictive expert deliberations. Without protecting the systems, it is hard to depend on storage and communication frameworks for secure medicinal, business, and military applications. Watermarking is a stand out amongst the most basic solution for make the information exchanging secure from the unlawful interference. In this paper we have survey literature related to watermarking, right protection through watermarking,***

Keywords: watermarking, mining, right protected, privacy preservation, distortion.

1. Introduction

Data exchange and information sharing have turned into an inherent part of business and academics. Both practices energize logical enquiry, ease approval of effort and augment transparency. Accordingly, information sharing what more information has distributed is perceived as vital productivity impetuses in various research efforts. This work presents a protection mechanism system that can convey noticeable confirm on the legal responsibility for shared dataset, without compromising its ease of use for a class of mining operations. To accomplish this, we promise that distance based relation between the dataset articles remain unaltered.

We implant ownership confirmation utilizing watermarking techniques. Watermarking has developed throughout the years as a successful technique for building information progeny. It has been utilized broadly as a part of numerous media applications, on image, feature, and sound information. Traditional watermarking techniques concentrate on a single object data and are not custom-made for protecting distance between various objects. In that sense, some technique increases and fortifies existing watermarking procedures. Our objective is two-fold: to ensure right-protection and, in the meantime, protect the original relationship between the dataset objects. Having finished this, any learning or retrieval task that relies on upon the preserved structural properties will remain undistorted much after the watermark application.

Watermarking is the methodology of machine helped data hiding in a carrier signal; the hidden data should, [1] however does not have to contain a connection to the carrier signal. Watermarks may be utilized to confirm the credibility or trustworthiness of the signal or to demonstrate the character of its owners. It is unmistakably utilized for following copyright encroachments and for banknote validation. Like customary watermarks, computerized watermarks are just noticeable under specific conditions, i.e. in the wake of utilizing some calculation, and subtle at whatever time else [2] If a watermark distorts the signal in a manner that it gets noticeable, it is of no use. Our paper is structured as follows: First, we describe how right-protection can be materialized via watermarking approach. We also show how to detect the watermark. Subsequently, we study the related work on watermarking.

2. Literature Survey

Traditional Watermarks may be connected to media (like pictures or feature), while in watermarking; the sign may be sound, pictures, and feature, writings or 3d models. A signal may convey a few diverse watermarks at the same time. Dissimilar to metadata that is added to the carrier signal, a watermark does not change the extent of the carrier signal [2].The required properties of a digital watermark rely on upon the use case in which it is connected. For stamping media records with copyright data, a watermark must be noticeably robust against changes that can be connected to the carrier signal. Rather, if integrity must be guaranteed, fragile watermark would be applied. Both steganography and watermarking utilize steganography methods to install information secretly in noisy signal. Be that as it may while steganography goes for subtlety to human faculties, digital watermarking tries to control the strength as top priority. Since a copy of information is the same as the first, watermarking is an inactive assurance tool. It simply stamps information, yet does not debase it nor controls access to the information.

One application of digital watermarking is source tracking. A watermark is inserted into a signal at each one purpose of distribution. In the event that a duplicate of the work is discovered later, then the watermark may be recovered from the duplicate and the source of the distribution is known. This system apparently has been used to locate the source of illegally replicated films.

1) Right Protection through Watermarking

In this scheme, we have to survey how watermarking mechanisms can embed a secret key (watermark) on a collection of objects. We also survey the techniques for 2D

sequence data (image contours) and how to detect watermark.

a. Watermark Embedding

A spread-spectrum approach [7] is discovered. This embeds the watermark system across multiple frequencies of each and every object and across multiple objects of the dataset. So that, it has to be render the correction in watermarks by removing the watermark which is difficult without substantially compromising the data utility. Using complex Fourier descriptors which is represented by X = {X1, . . . ,Xn} the object x is mapped into frequency domain. The mapping of the space domain to the frequency domain is described by the normalized discrete Fourier transform, DFT(x), and its inverse, IDFT(X). The strength of the watermark installing relies on upon the decision of coefficients. We insert the watermark in the coefficients that display, as a rule over the dataset, the biggest Fourier sizes. This makes the removal of the watermark troublesome; covering it out would imply that critical frequencies of the dataset will be contorted. This would reduce the dataset utility. It is apparent that the high-energy coefficients catch critical attributes of the dataset. We embed the watermark in the sizes of the Fourier descriptors and leave the stages unaltered; watermarking is done using the Fourier descriptors with the biggest normal magnitude.

b. Watermark Detection

We measure the likelihood of presence of a watermark by assessing the relationship between a tested watermark and the right-protected dataset. Measuring straightforwardly the correlation between the watermark and the magnitude of Fourier descriptors may demonstrate ineffectual. The reason being that the original level of the normal of magnitude goes about as background noise, mask the inserted watermark which will try to distinguish. We address this issue by unequivocally recording the bias of normal extents before inserting the watermark and remove it before the recognition. We likewise record this bias vector alongside the watermark, and both are utilized together as the key.

2) Generic Watermarking System

Following Fig. 1 shows generic watermarking system which is structured in three parts: viz; watermarking embedding algorithm, extraction algorithm and detection [3][4]. During embedding process, algorithm acknowledges the host also the information to be implanted and produces a watermarked signal.

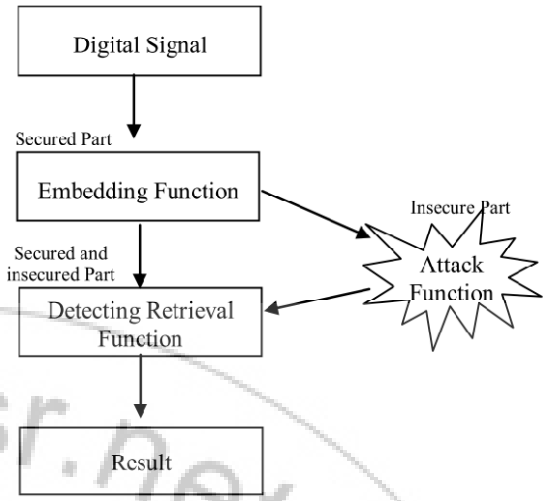

Figure 1: Watermark Lifecycle Phases [4]

The watermarked signal is then transmitted or put away. In the event that an individual makes an alteration, then the content is said to be attacked. A watermark attack is on information where the vicinity of a uniquely created bit of information can be recognized by an attacker without knowing the encryption key [4].

3) Related Work to Watermarking

Watermarking is a steganography method utilized for establishing the ownership, with numerous applications in multimedia datasets [5], for example, images [6], vector graphics [7], audio [8, 9] and video [10, 11]. Multimedia watermarking concentrates on the assurance of a single item whilst minimizing visual/audible distortion of the data. Privacy-preserving procedures are likewise identified with our work, since they additionally adjust information yet authorize diverse requirements. To attain privacy preservation two research ways are typically took after: an) assurance through information change or covering, and b) assurance through dataset partition. Information modification can be attained through noise addition [12, 13], condensation [14] or information change [15, 16]. Comparative notions have likewise been utilized for watermarking databases [17, 18]. Privacy-protection through dataset partition is attained utilizing horizontal or vertical information partitioning [19, 20, 21, 22]. Of importance is additionally the work on watermarking streaming time-series [23]. We give provable ensures on protection of separation properties. A right protection plan focused around watermarking standards that saved the Nearest Neighbor of items was introduced in [24].

References

[1] Ingemar J. Cox: Digital watermarking and steganography. Morgan Kaufmann, Burlington, MA, USA, 2008.
[2] Frank Y. Shih: Digital watermarking and steganography: fundamentals and techniques. Taylor & Francis, Boca Raton, FL, USA, 2008.
[3] Zhang, X. and Wang, S. “Fragile watermarking scheme using a hierarchical mechanism”, Signal Processing Vol. 89, Issue 4, Pp. 675-679. 2009.

[4] S. Radharani, M.L. Valarmathi, "A Study on Watermarking Schemes for Image Authentication" International Journal of Computer Applications (0975 – 8887) Volume 2 – No.4, June 2010.
[5] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon. Secure spread spectrum watermarking for multimedia. IEEE Transactions on Image Processing, 6(12):1673–1687, 1997.
[6] P. Moulin, M. E. Mihcak, and G.-I. Lin. An information-theoretic model for image watermarking and data hiding. In IEEE International Conference on Image Processing, pages 667–670, 2000.
[7] X. Niu, C. Shao, and X. Wang. A survey of digital vector map watermarking. International Journal of Innovative Computing, Information and Control, 2(6):1301–1316, 2006.
[8] P. Bassia and I. Pitas. Robust audio watermarking in the time domain. In 9th European Signal Processing Conference, pages 25–28, 1998.
[9] M. D. Swanson, B. Zhu, A. H. Tewfik, and L. Boney. Robust audio watermarking using perceptual masking. Signal Processing, 66(3):337–355, 1998.
[10] D. Simitopoulos, S. A. Tsaftaris, N. V. Boulgouris, and M. G. Strintzis. Compressed-domain video watermarking of MPEG streams. In IEEE International Conference on Multimedia and Expo, volume 1, pages 569–572, 2002.
[11] W. Zhu, Z. Xiong, and Y.-Q. Zhang. Multiresolution watermarking for images and video. IEEE Transactions on Circuits and Systems for Video Technology, 9(4):545–550, 1999.
[12] H. Kargupta, S. Datta, Q. Wang, and K. Sivakumar. On the privacy preserving properties of random data perturbation techniques. In 3rd IEEE International Conference on Data Mining, pages 99–106, 2003.
[13] L. Liu, M. Kantarcioglu, and B. Thuraisingham. The applicability of the perturbation model-based privacy preserving data mining for real-world data. In 6th IEEE International Conference on Data Mining, pages 507–512, 2006.
[14] C. C. Aggarwal and P. S. Yu. A condensation approach to privacy preserving data mining. In International Conference on Extending Database Technology, pages 183–199, 2004.
[15] K. Chen and L. Liu. Privacy preserving data classification with rotation perturbation. In International Conference on Data Mining, pages 589–592, 2005.
[16] S. Oliveira and O. Zaiane. Privacy preserving clustering by data transformation. In 18th Brazilian Symposium on Databases, pages 304–318, 2003.
[17] R. Agrawal and J. Kiernan. Watermarking relational databases. In 28th International Conference on Very Large Databases, pages 155–166, 2002.
[18] R. Sion, M. Atallah, and S. Prabhakar. Rights protection for relational data. IEEE Transactions on Knowledge and Data Engineering, 16(12):1509–1525, 2004.
[19] G. Jagannathan, K. Pillaipakkamnatt, and R. N. Wright. A new privacy-preserving distributed k-clustering algorithm. In SIAM International Conference on Data Mining, 2006.
[20] J. Vaidya and C. Clifton. Privacy-preserving k-means clustering over vertically partitioned data. In 9th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, pages 206–215, 2003.
[21] H. Yu, X. Jiang, and J. Vaidya. Privacy-preserving SVM using nonlinear kernels on horizontally partitioned data. In ACM Symposium on Applied Computing, pages 603–610, 2006.
[22] H. Yu, J. Vaidya, and X. Jiang. Privacy-preserving SVM classification on vertically partitioned data. In 10th Pacific-Asia Conference on Knowledge Discovery and Data Mining, pages 647–656, 2006.
[23] R. Sion, M. J. Atallah, and S. Prabhakar. Rights Protection for Discrete Numeric Streams. IEEE Transactions on Knowledge and Data Engineering, 18(5):699–714, 2006.
[24] C. Lucchese, M. Vlachos, D. Rajan, and P. S. Yu. Rights protection of trajectory datasets with nearest-neighbor preservation. The VLDB Journal, 19(4):531–556, 2010.