Bibliotheque de Humanisme et Renaissance | ISSN : 0006-1999
Volume 80, Issue 1, 2020

Securitized watermarking: Watermarking of a dataset using usability constraints

Amritha B & Linu A Thomas

P.G. Students, Dept. of Computer science and Engg, Lourdes Matha College of Science & Tech., Kerala, India

Abstract

In this present world security becomes a major concern and as a result protecting ownership on dataset is becoming a challenge. So to mitigate these threats, watermarking is a commonly used mechanism to prove the ownership of these databases. Therefore, a new watermark embedding algorithm is implemented which enhances security of the inserted watermark. One of the major issue in watermarking is that it does not preserve the information in the dataset, so to meet this requirement watermark is being inserted in the dataset using usability constraints. Usability constraints are used to preserve the data during the insertion of watermark in the dataset.

Index Terms –watermarking, watermark embedding, usability constraints

I. INTRODUCTION

In this world there are so many applications so many datas will be generated and these datas that are being generated should be safe and it should not be taken by an unauthorized user .So here watermarking technique is used for each of the datasets. Watermarking is a prospective weapon against piracy, embeds ownership information without degrading the quality of the host contents. The most important challenge in watermarking dataset is how to preserve the information in dataset, so to meet this requirement usability constraints are being enforced while inserting watermark in the dataset..This inserted watermark is imperceptible and robust against any type of attacks. So far no technique has been proposed to model the usability constraints . Usability constraints are used to preserve data during the process of watermark insertion in the dataset. So this watermark technique should not result in the distortion of data and the dataset information should be preserved i.e, dataset information should not change after the watermark embedding process. In this paper a model is proposed for identifying usability constraints which must be enforced while insertion of watermark in the dataset.

- Improves the security of the inserted watermark because the attacker will not be able to remove the watermark
- Usability constraints are enforced while embedding watermark in the dataset which not only preserves dataset information but also ensures robustness of the inserted watermark.
- The proposed technique is independent of the type of data i.e, numeric and nonnumeric data

II. PROBLEM DEFINITION

The problem is to develop the usability constraints to protect the information in the dataset and to ensure robustness of the inserted watermark.

III. RELATED WORK

R.Sion and Atallah [1]introduced a watermarking technique for the relational databases but they are useful for preserving the information present in the dataset.
R. Agarwal and J. Kiernan[2]introduced MAC i.e, message auntentication code with the help of secret key to identify the candidate tupules.
M. Shehab and E.Bertino [3] defined optimization based watermarking technique to define pattern search and genetic algorithm optimizers.
M. Kamran and Muddassar Farooq[4] introduced an information preserving watermarking scheme to enforce usability constraints by using electronic medical record(EMR) systems.
M. Kamran and Muddassar Farooq [5]introduced a formal model to define usability constraints which preserves dataset information.
So the current work is based on developing usability constraints which must be inserted while embedding watermark in the dataset.

IV. PROPOSED SYSTEM

The proposed system aims at identifying the usability constraints and to enforce the usability constraints while embedding the watermark in the dataset. Watermarking process should be robust against different types of malicious attacks. A new watermark embedding algorithm is developed in such a way that it should be difficult for an attacker to delete or alter the watermark and this is done using encryption and decryption techniques.

❖ Usability constraints

Usability constraints are enforced to preserve the dataset information. It preserves the data during the process of inserting watermark in the dataset. When a watermark is inserted in the dataset the data will change slightly resulting in the distortion of data. So to avoid the changes in data we use usability constraints

The usability constraints used are:

- Global Usability constraints
- Local Usability constraints

- **Global Usability constraints**

Global Usability constraints are used for the whole dataset

- **Local usability constraints**

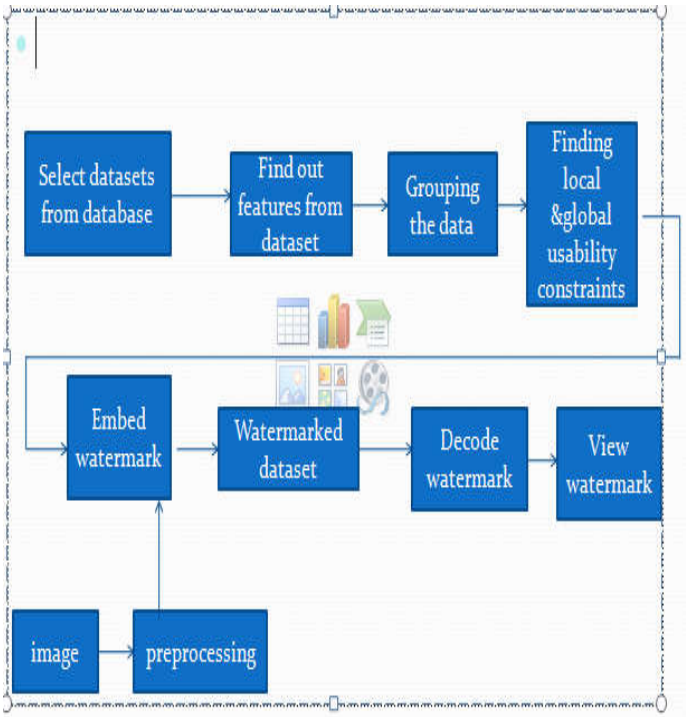
Local usability constraints are used for certain groups of data.
So this usability constraints have been derived for both the types of datasets

- **Numeric datasets**
- **Nonnumeric datasets**

This new proposed technique models the usability constraints to preserve the dataset information and it also ensures the robustness of the inserted watermark. Security of the inserted watermark is implemented using encryption and decryption techniques. Here a new watermark embedding technique is used for ensuring security. So this technique improves the security of the inserted watermark so that the attacker will not be able to remove the watermark by launching malicious codes.

ARCHITECTURE FOR PROPOSED SYSTEM

The architecture diagram shows the flow of whole process.



The proposed system has the following functionalities. First and foremost, the datasets are being selected from the database. Here iris dataset is used and the next step is to find out the different features of this dataset and this features are based on the particular dataset. Next step is Data grouping ,Data grouping is used to find out the usability constraints and it is done using different class functions.

After that local and global usability constraints are found out for each of the features. Local usability constraints means splitting the whole data to different group according to the features or classes and then finding the factors which affect each group .Global usability constraints studies about the whole dataset.

Next step is watermark embedding, which is used to embed a watermark into the dataset. It ensures that whether the inserted watermark is robust against any type of attacks. So, now the watermarked dataset can be viewed but any unauthorized person cannot make any changes to the watermarked data. The security of the watermarked data is ensured using encryption and decryption techniques. Similarly an image is also been watermarked. Firstly an image is being preprocessed .Preprocessing is a technique of resizing an image to make it fit into the dataset. So after preprocessing the image is embedded into the dataset and the same procedure continues. Finally the dataset and the images are watermarked .

V. ADVANTAGES OF PROPOSED SYSTEM

- The proposed technique is independent of the type of dataset .It works for both numeric and nonnumeric datasets.
- Usability constraints are enforced which not only ensures the robustness of the inserted watermark but also preserves the information contained in the dataset.
- Usability constraints avoids the changing of data during the insertion of watermark in the dataset.
- Proposed system improves the security in terms of deleting or changing the watermark. The security is implemented using encryption and decryption techniques.
- Unauthorized user cannot view the watermarked data even if they access it they cannot make any changes in the data.
- Images are watermarked with more security.

VI. CONCLUSION

The information contained in the dataset is preserved using usability constraints. Usability constraints also ensures the robustness of the inserted watermark. This enhanced watermarking technique works for both numeric and nonnumeric data .It ensures security of the inserted watermark .Last but not the least images are also watermarked with more security.

REFERENCES

[1]R Agrawal and J Kiernan," Watermarking relational databases", in proc.28th Int. conf. Very Large Databases, 2002, pp. 155-166.
[2] M. Shehab, E. Bertino, and A. Ghafoor, "Watermarking relational databases using optimization-based techniques," IEEE Trans. Knowl. Data Eng., vol. 20, no. 1, pp. 116–129, Jan. 2008
[3] M.Kamran and M .Farooq," An information-preserving watermarking scheme for right protection of EMR systems," IEEE Trans. Knowl. Data Eng., vol. 24, no. 11, pp. 1950–1962, Nov. 2012.
[4]R.Sion ,M. Atallah ,and S. Prabhakar," Rights protection for relational data,"IEEETrans.Knowl.DataEng.,vol.16,no.12,pp.1509–1525, Dec. 2004.
[5]M.Kamran and M.Farooq,"A formal usability constraints model for watermarking of outsourced datasets," IEEETrans.on information forensics and security,Vol.8,no.6,June2013