

Enhanced Watermarking Using Secure Reversible Algorithm

Kavisankar Leelasankar¹ and Devika C²

¹Department of CSE, Hindustan Institute of Technology & Science, Chennai, Tamil Nadu, India.

kavisankar@gmail.com

²Department of CSE, SRM Institute of Science and Technology, Chennai, Tamil Nadu, India.

Abstract

Information security is the need of the hour. Most of the information are now stored in the large database of social engineering. The data retrieved from these social databases are to be extracted in a secure manner. There are more security dangers with respect to access and modification rights of these data. It is even more dangerous when the ownership of the data is modified. Watermarking technique comes in handy for the protection of the ownership. So, that the modification of the data is averted. But while performing the watermarking technique the quality of the information is disturbed. There is a need that the quality of the information is not affected for that the reversible watermarking technique is used. But they are prone to attacks. A robust and semi-blind reversible watermarking technique is proposed. The proposed enhanced watermarking technique using secure reversible algorithm preserves the quality of data and it provides the robustness against attack and selective watermarking improves performance of the system. Reversible watermarking technique based on Time-Stamping allows recovery of original data. The distortions are minimized in the watermarked content and the ownership rights are protected for the database owner.

Key Words and Phrases: Information security, watermarking, robustness, reversible watermarking, selective watermarking, secure reversible algorithm, semi-blind reversible watermarking technique.

1 Introduction

Watermarking procedures have verifiably been utilized to guarantee security as far as proprietorship insurance and sealing for a wide assortment of information organizations. This incorporates pictures, sound, video regular dialect preparing programming, social databases and that's only the tip of the iceberg. Reversible watermarking methods can guarantee information recuperation alongside proprietorship insurance. Fingerprinting, information hashing, serial codes are some different strategies utilized for proprietorship insurance. Fingerprints moreover called value-based watermarks, are utilized to screen and recognize advanced possession by watermarking every one of the duplicates of substance with various watermarks for various beneficiaries. Basically this sort of computerized watermarking tries to distinguish the wellspring of information spillage by following a blameworthy specialist. In hashing, advanced substance can be spared by performing a restricted hash capacity whereby the information substance doesn't change. On the off chance that the hash of the first and altered information is the same, information validness can be confirmed yet possession can't be demonstrated effectively. Serial or order codes are utilized for separating of wrong substance over the Internet and are principally material to pictures, sound and video. Watermarking has the property that it can give possession security over the advanced substance by denoting the information with a watermark one of a kind to the proprietor.

The installed watermark [1] can accordingly be utilized for demonstrating and asserting possession. Advanced watermarking is the critical strategy to secure the copyright of computerized pictures. In Intellectual Property Right (IPR), a trademark or logo of the proprietor can be chosen as a watermark. This watermark is implanted into the first picture to secure that picture.

The first picture subsequent to installing the watermark is known as watermarked picture. The watermarked picture can be distributed and proprietor can demonstrate the responsibility for the picture by recovering the watermark from the watermarked picture. In doctor's facilities and human services frameworks there is tremendous measure of information stockpiling. It likewise transmits that information to different frameworks for finding. It incorporates restorative pictures, tolerant records and some authoritative reports. Among every one of these information, medicinal pictures and patient records are the critical information that should be secured against unapproved access and vindictive assaults. To give the security to this data uprightness, classification and legitimacy are the three essential prerequisites.

Privacy can be kept up by implanting the patient data into the therapeutic pictures. In the wake of performing the implanting operation the watermarked picture and unique picture ought to be like perform the finding with the shrouded data. To keep up the trustworthiness of therapeutic pictures is another essential issue. Confirmation ought to be given to the therapeutic pictures. What's more, for this there is the prerequisite of watermarking. Computerized watermarking is a procedure that implants the data into the host media to give the security reason. Security includes duplicate control confirmation, copyright protection. Computerized watermarking is utilized so that right data is gotten and appropriate treatment is given to the patient. It is critical to extricate the picture and data as the first picture with no bending in picture. In restorative pictures, after transmission, it is important to have both, unique picture and data to be lossless. Our primary point is to insert and concentrate the watermark with least misfortune. Reversible watermarking recuperates the first picture subsequent to separating the watermark. The reversible watermarking gives the confirmation furthermore recoups the first picture.

A general watermarking plan needs to meet the taking after necessities. Reversible watermarking tries to beat the issue of information quality debasement by permitting recuperation of unique information alongside the installed watermark data.

2 Existing System

The existing very relevant method involves watermarking

electronic text documents that contain justified paragraphs and irregular line spacing. This method uses a spread-spectrum technique to combat the effects of irregular word or line spacing. It also uses a BCH (Bose-Chaudhuri-Hocquenghem) [2] error coding technique to protect the payload from the noise resulting from the printing and scanning process. Watermark embedding in a justified paragraph is achieved by slightly increasing or decreasing the spaces between words according to the value of the corresponding watermark bit. Similarly, watermark embedding in a text document with variable line spacing is achieved by slightly increasing or decreasing the distance between any two adjacent lines according to the value of the watermark bit. Detecting the watermark is achieved by measuring the spaces between the words or the lines and correlating them with the spreading sequence.

3 Proposed System

In this method, an optimal value is embedded in the selected features of dataset with the objective of preserving data quality and minimizing data distortions. This embedding is done in numerical values of the datasets to make the scheme resilient against attacks. Taking in to account the disadvantages of existing system, the proposed work has a one such reversible watermarking method that keeps the information helpful for learning disclosure. Information alterations are permitted to such degree that the quality of the information before inserting watermark data also, subsequent to separating, is worthy for learning extraction process. Hence, learning disclosure gets to be fruitful in choice emotionally supportive networks where great information recuperation [3] is basic. Reversible watermarking methods are as of now accessible in writing; be that as it may, to the best of our insight, no work has been led on overcoming the issues of reversible watermarking methods in the nearness of malevolent assaults. Accomplishing heartiness in the nearness of reversibility is a testing assignment. These two elements might be possibly clashing since a reversible watermark string additionally makes it a less demanding focus for assault. In this manner, we attempt to locate the most suitable watermark data transfer capacity that guarantees most extreme watermark vigor without critical loss of data that may come about by watermarking. To this end, we model the transfer speed enhancement as an imperatives improvement issue.

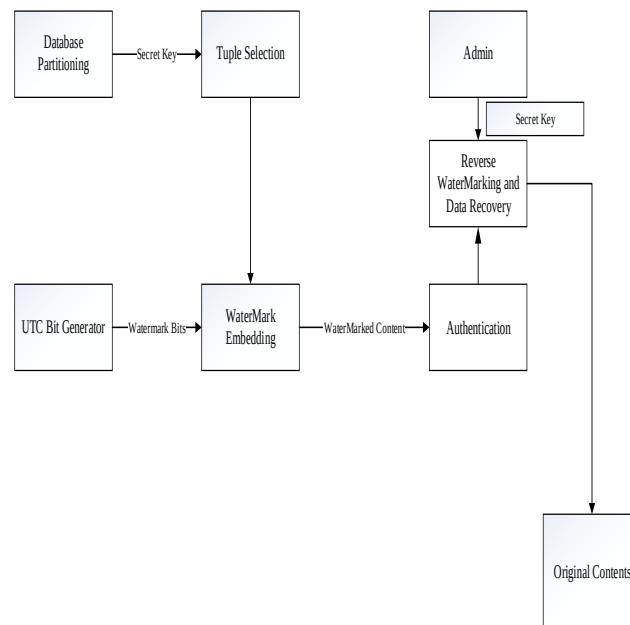


Figure 1: Architecture Diagram

Figure 1. Shows the Architecture Diagram of the proposed Enhanced Watermarking Using Secure Reversible Algorithm.

Depending on the needs and the workflow that has been done, the modules used are as follows:

- Database partitioning
- Tuple selection
- Watermark embedding
- Authentication
- Reverse watermarking and data recovery

The effect of this is the reduction of copper losses found in the windings of transformer and thus finally leads to increased power transfer and low leakage inductance.

A. Database partitioning

Partitions the dataset into logical groups.

Input: Dataset D, secret key Ks, No: of partitions m

Output: Data partitions

For each tuple r in D do

$Par(r) = H(ks || H(r.Pk || ks)) \bmod m$

r: primary key of tuple r

H(): cryptographic hash function

ks: secret key

m: partition length

B. Tuple selection

Threshold value is calculated for each attributes.

INPUT: Data partitions and C

OUTPUT: DT()

For each attribute A, calculate T

$T = c * \text{mean} + \text{standard deviation}$

C: confidence factor

If attribute value > threshold value, then

Select that tuple for watermarking

C. Watermark Embedding

From date-time stamp, watermark bits are generated the selected tuples are encoded using watermark bits [4].

D. Authentication

Based on images, legitimate user should register them using a username and pass-image. At the time of login, a challenge set containing gray scale images will provide for authentication.

E. Reverse watermarking and Data recovery

Reverse watermarking & Data recovery will be done only by the legitimate user. If the user ownership content is matched with the admin generated content, then decoding of watermark bits and original data is done.

In this way the proposed method using the Reversible watermarking technique based on Time-Stamping allows recovery of original data. It also minimizes the distortions in the watermarked content. It also protects the ownership rights for the database owner.

4 Experimental Results Conclusion

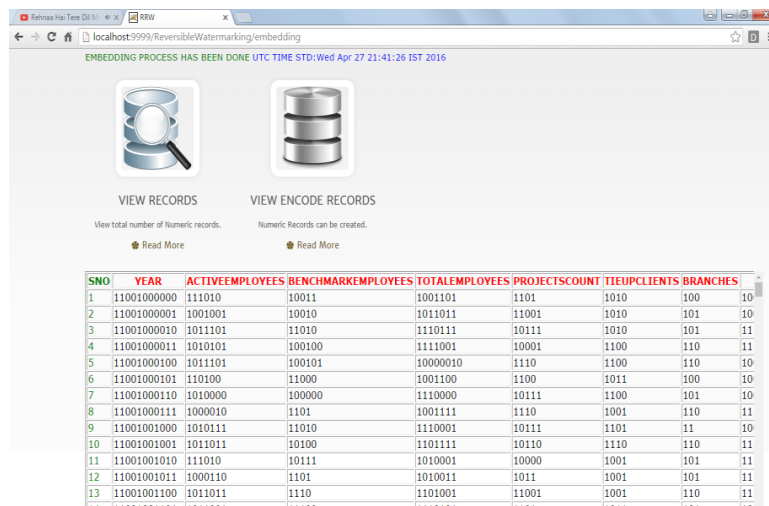


Figure 2: Watermark Embedding

Figure 2. Shows how the watermark embedding with the help of UTC time standard. The Reversible watermarking technique based on this UTC time-Stamping allows recovery of original data.

Table 1. Experimental Setup

Serial No	Experimental Setup	
	Support Needed	Specification
1	Number of system	5
2	Accessing Time	30 minutes
3	Protocol Needed	IPv4
4	Total RAM size	1024MB
5	Software Tools	JDK 1.6, Tomcat(JSP, Servlet)
6	Database	Mysql 6.0, Oracle10G

Table 1: Experimental Setup need and the required specification are given in the above table.

5 Conclusion

An optimal value is embedded in the selected features of dataset with the objective of preserving data quality and minimizing data distortions. This embedding is done in numerical values of the datasets to make the scheme resilient against attacks. Distortions in data are minimized using parameter generation. The selective watermarking is used such that when the attacker tries to corrupt the watermark data. He has to attacks all tuples in-order to corrupt the watermark, which makes the proposed method even stronger. Moreover the robustness against heavy attacks and recovery of original data is ensured.

Reversible watermarking technique based on Time-Stamping allows recovery of original data. The distortions are minimized in the watermarked content and the ownership rights are protected for the database owner. In future the approach shall be extending to non-numeric domains. The Watermark bits can be generated from biological methods and the security can be enhanced by deploying the hash value computations.

References

- [1] Alattar, Adnan M, *Reversible watermark using difference expansion of triplets*, IEEE **1**, (2003), 1-501.
- [2] Thodi, M. Diljith, Jeffrey J. Rodríguez, *Reversible watermarking by prediction-error expansion*, IEEE, (2004), 21-25.
- [3] Thodi, M. Diljith, and Jeffrey J. Rodriguez, *Prediction-error based reversible watermarking*, IEEE **3**, (2004), 1549-1552.
- [4] Sonnleitner, Erik, *A robust watermarking approach for large databases*, IEEE, (2012), 1-6.
- [5] Loganayaki A, *Robust Watermarking For Relational Database*, International Journal of Communication and Computer Technologies **1(41)**, (2013).

- [6] Iftikhar, Saman, M. Kamran, and Zahid Anwar, *RRW—A Robust and Reversible Watermarking Technique for relational data*, IEEE **27(4)**, (2015), 1132-1145.
- [7] H. Divecha, Nidhi, N. N. Jani, *Reversible watermarking technique for medical images using fixed point pixel*, IEEE, (2015), 725-730.
- [8] Naseem, Muhammad Tahir, Ijaz Mansoor Qureshi, Muhammad Zeeshan Muzaffar, *Chaos based invertible authentication of medical images*, IEEE, (2013), 1-5.
- [9] Braci, Sofiane, Remy Boyer, Claude Delpha, *Security evaluation of informed watermarking schemes*, IEEE, (2009), 117-120.
- [10] Lafaye, Julien, *An analysis of database watermarking security*, IEEE, (2007), 462-467.
- [11] Cayre, Francois, Caroline Fontaine, Teddy Furon, *Watermarking security: theory and practice*, IEEE **53(10)** (2005), 3976-3987.

