Journal of Modern Computing and Engineering Research
JMCER
Volume 2022, p. 49-54
https://jmcer.org

Reversible Watermarking Approach for Ensuring the Integrity of Private Databases Against Attacks

Asmaa Alqassab[1], Mafaz Alanezi[2]

[1, 2] *Department of Computer Science, College of Computer Science and Mathematics, University of Mosul, Iraq*

[1] *asmaa_mow@uomosul.edu.iq,* [2] *mafazmhalanezi@uomosul.edu.iq*

Received: August 9, 2022 Revised: September 9, 2022 Accepted: September 10, 2022

Abstract

Database watermarking is considered one of the active research fields, where best trade-off between: robustness, reversibility, and capacity, to protect sensitive data's: integrity, ownership, and copyright, is needed in any watermarking scheme. As for database security, developing a persistent and robust watermarking system, is the ultimate objective for securing the databases. Accordingly, in our suggested method, we have studied various works suggested by other authors with a focus on determining their strengths and weaknesses. Eventually, we came with a new idea for protecting RDB by means of reversible watermarking, where better results in comparison with previous researchers' methods are gained.

Keywords: *Relational Database, Reversible Watermarking, RRW, Attacks on Relational Database, Relational Database Protection*

1 Introduction

In information hiding field, digital watermarking technique is a significant area of research. It is the process of concealing some data within a multimedia data, to meet the needs of authentication or content protection. In ordinary such technique enables hiding data, such as copyright information or any other identification and verification data, known as a "watermark", within a multimedia data as a carrier which can be a host image called "original image" or "cover image", in such a manner as to enable detection and extraction of the concealed watermark which may be done later to confirm the data validity, without causing perceptible changes to the host cover image, and is hard to be modified or detected too.

Thus, Watermarking is considered an effective technique for data security protection, like copyright protection and counterfeit tracing (Hemani and Mandoria, 2017) (Duan et al., 2020) (Al-Qassab and Nori, 2014).

Watermarking technology is utilized for embedding some information into multimedia data. This information is not usually visible, only dedicated detector or extractor can see and extracts that information. The framework in figure 1 depicts digital watermark life cycle which basically comprises three obvious phases: the first one is the embedding phase, then followed by the attack phase and finally the detection phase (Gaur and Manglani, 2015), (Kumar, 2016), (Singh et al., 2016), (Alqassab and Alanezi, 2021).

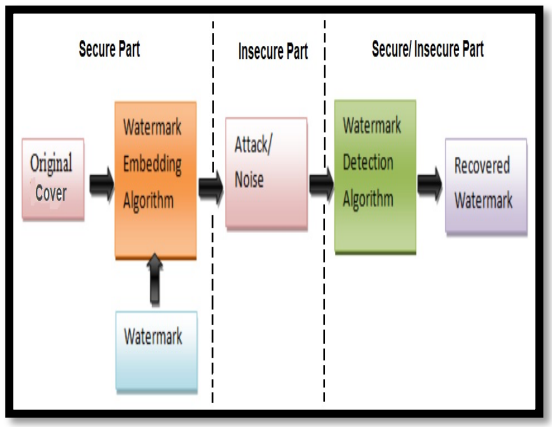


Figure 1: Digital Watermarking Life Cycle

Across the network and during data transmission, watermarked data may experience various sorts of attacks or noise that may be added to

Corresponding author: Asmaa Alqassab, asmaa_mow@uomosul.edu.iq

it. So, the attack phase encompasses any of such potential attacks. For example, malicious attacks can be launched by the attacker on watermarked data, through manipulating some data contents with the intention of embedded watermark disturbing. Thereby, our watermarked data bits are either modified or destroyed (Gaur and Manglani, 2015) (Kumar, 2016) (Singh et al., 2016) (Kamran and Farooq, 2018) (Alqassab and Alanezi, 2022).

Known attacks on image watermarking can be categorized as: (Singh and Chadha, 2013) (Fazli and Moeini, 2016) (Begum and Uddin, 2020):

- Removal Attacks: aim to eliminate the watermark data embedded within a watermarked image. These attacks take advantage of the fact that this embedded watermark is nothing but an "additive noise" inserted within the host image. So, on this basis, they try to harm the watermark to a large extent rather than eliminate the watermark data entirely, and this can be done through disturbing the watermarked image with noise signal insertion that results in confusing the data sender. The whole noise forms, including: salt-and-pepper, additive, gaussian noise, etc., belong to this category.
- Geometric Attack: Any manipulation which influences the image geometry including: image rotating, scaling, flipping, etc.
- Image Enhancement: works on the chosen features by heightening their dynamic range in an image. Such attacks include contrast enhancement, sharpening, histogram equalization, etc.

2 Related Works

Applying digital watermarking for the database security started to attract the attention of the researchers, various watermarking methods have been suggested so far:

Ali and Mahdi (2011) suggested a watermarking approach on the basis of a private-key for protecting the copyright of the numerical database attributes. In this approach the (hash-based message authentication code) was employed in tandem with a threshold generator used for identifying whether the marking bit locations' values, were "1" or "0".

Tzouramanis (2011) presented a watermarking approach with the aim of database' legal ownership identifying in addition to elasticity to multifarious forms of attacks proving. This approach was applied on numeric tuples of the relational database through reordering every bit in each tuple in a secret manner. Afterwards, a number of its data bits could be picked so that the tuple could be routed to a certain watermark bit besides picking a single data bit that was assigned with the value of the allotted watermark bit.

Chang and Wu (2012) introduced a fragile reversible watermark approach for attaining database contents verification and tamper detection by means of SVR prediction (support vector regression) in which important original database properties were embedded. FP-tree (frequent pattern tree) procedure for data mining was used along with the associated rules as a means to identify the significant characteristics of every single chosen data used for the SVR prediction process. Yet, this approach hadn't enough robustness to cope with serious attacks.

Ramani (2013) suggested an approach that had the ability to verify the database ownership and at the same time ensured robustness as well as security versus the attempts to eliminate the mark. This could be done by an imperceptive mark inserting. In this approach, an image was used in the watermarking process to prove the database ownership through converting that image into row bits which were encrypted by applying the (MD5) security algorithm. Eventually, these encrypted row bits were considered a watermark that was embedded within the database attributes.

Shyamala et al. (2015) provided an approach with a security mechanism that enabled handling of the proprietary disputes about the watermarked datasets when additive attacks took place. This approach provided utmost accuracy and less distortion in decoding phase.

Murugan et al. (2017) suggested a new invisible watermarking approach which suited any sort of the data attributes, aiming to attain relational databases' right protection as well as authentication. The approach comprised of logical embedding of the database' copyrights owner as a watermark and a watermarking key creating, which are kept together within the CA (Certification Authority) where the true owner already had registered. Thereafter, the

procedure of the watermark extraction could be implemented using the created watermarking key. Finally, as a way for proving database integrity along with the real owner authenticity, both of the original watermark and the extracted one were compared for the watermark accuracy calculation.

Unnikrishnan and Pramod (2017) provided a reversible watermarking approach for original database reclaiming and tamper detecting within the relational database. For the mark embedding and for the purpose of specifying the database' optimal regions, the optimization algorithms including: the FA algorithm (firefly) and the OLPSO algorithm (orthogonal learning particle swarm optimization), were applied. When tampering occurred, the suggested approach had the power to restore the tampered database back to its original status.

Mukherjee and Jana (2019) suggested a Reversible Data Hiding (RDH) on the basis of the DE with higher payload in which, in order to enhance the visual quality, 3 thresholds were used. The image was broken up into (3 × 3) blocks then pixels inside each block are classified as "Type-1" and "Type-2" pixels according to their locations (odd or even). Next, the standard deviation values and the correlation among pixels are used for watermark bits embedding. Results were assessed using (512×512) images.

Murugan et al. (2019) suggested a zero-watermarking approach for the purpose of securing the copyright information of the relational database in which in watermark generating phase an image was utilized as a private key. In this approach, the cover data had no inserted information. As an alternative, the watermarking key that had been created was used for the registration process within the Certification Authority. Furthermore, this approach could be utilized for watermarking various sorts of the database attributes.

Wang (2019) suggested a "2-directional" DE based RDH technique, in which embedding process is performed within dual directions. At the beginning, scanning of the image in a unique manner is done such that a pixel values collection of 1-D is obtained. After that, embedding of the difference is done within two directions and a 2-D image is regenerated again. In order to control both of the capacity and the quality, a threshold value has been utilized. Grayscale (512 × 512) images were used.

3 Suggested Approach

A blind robust, invisible and reversible watermarking scheme on the basis of the DE is suggested for embedding of the metadata related to people's personal information within a coloured cover image to verify integrity and authenticity. A proposed system flowchart can be seen in Figure 2.

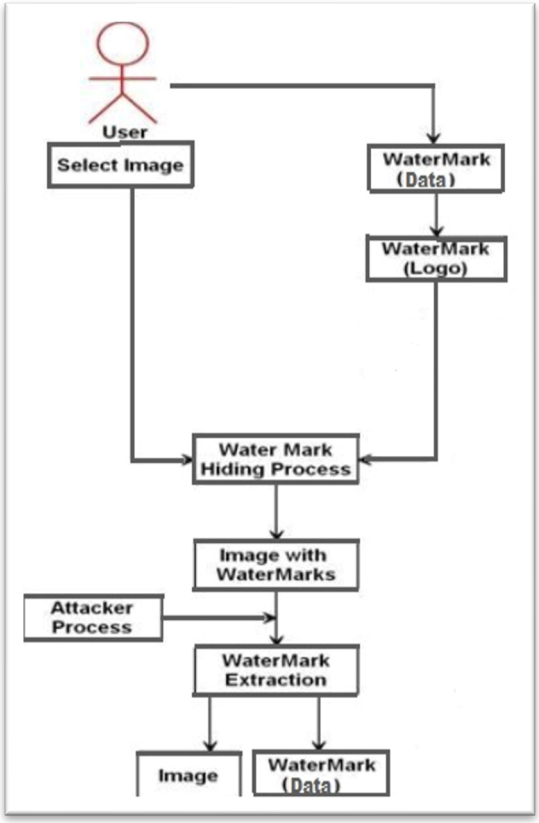


Figure 2: The proposed system flowchart.

4 Experimental Results

To demonstrate the suggested scheme robustness, different image watermarking attacks including: bilateral filtering, gaussian noise, histogram equalization, intensity adjustment, LSB invert, salt and pepper noise and sharpening, were applied on the watermarked image. Table 1 shows how the watermarked image looks like before and after attacks along with Table 2 which reveals the results obtained utilizing SSIM, PSNR, MSE, IF, AR

and BER metrics (original sample images were taken from google). Imperceptibility between watermarked and original images utilizing PSNR, MSE, SSIM and IF metrics achieved by the suggested watermarking scheme can be seen in Table 3.

Table 1: Watermarked images before and after various attacks.

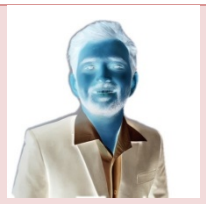
Original Image	
	
Bilateral Filtering (Level 1)	**Gaussian Noise (Level 3)**
	
Histogram Equalization	**Intensity Adjustment (Level 0.4)**
	
LSB Invert	**Salt and Pepper (Level 520)**
	
Sharpening	
	

Table 2: Robustness under various attacks utilizing SSIM, PSNR, MSE, IF, AR and BER metrics.

SSIM	PSNR	MSE	IF	AR	BER
Attack: Bilateral Filtering (Level 1)					
0.999	88.48	9.21810	0.99	1	0
Attack: Gaussian Noise (Level 3)					
0.994	44.05	2.55646	0.94	0.901	0.098
Attack: Histogram Equalization					
0.942	31.59	45.0295	0.10	1	0
Attack: Intensity Adjustment (Level 0.4)					
0.857	30.91	52.7155	-0.04	1	0
Attack: LSB Invert					
-0.05	30.43	58.8477	-0.16	1	0
Attack: Salt and Pepper (Level 520)					
0.930	32.70	34.8703	0.30	1	0
Attack: Sharpening					
0.927	35.74	17.3101	0.65	0.970	0.029

Table 3: Imperceptibility between watermarked and original images utilizing PSNR, MSE, SSIM and IF metrics, L represents the length of the watermark in bytes.

L	PSNR	MSE	SSIM	IF
1056	77.54	0.0011	0.999	0.999
1072	77.77	0.0010	0.999	0.999
1008	78.01	0.0010	0.999	0.999
944	78.31	0.0009	0.999	0.999
976	78.25	0.0009	0.999	0.999
16880	65.95	0.0164	0.999	0.999
4976	70.82	0.0053	0.999	0.999
16400	65.29	0.0192	0.999	0.999
32624	62.31	0.0381	0.998	0.999
5328	70.29	0.006	0.999	0.999

Table 4 shows a comparison between the previous approaches and our proposed approach. Obvious enhancement can be noticed regarding the Embedding Capacity (EC), PSNR and Location Map (LM).

Table 4: Comparison between the proposed approach and existing approaches.

Approach	Image Type	EC (bytes)	PSNR	LM
(Tian, 2003)	Gray	4946	44	Yes
Proposed	Colored	4976	70	No
(Gujjunoori & Oruganti, 2019)	Gray	16,384	41	Yes
Proposed	Colored	16,400	65	No
(Mukherjee & Jana, 2019)	Gray	32,512	34	No
Proposed	Colored	32,624	63	No
(Wang, 2020)	Gray	5200	43	No
Proposed	Colored	5328	70	No
(El-sayed et al., 2016)	Colored	16,879	39	No
Proposed	Colored	16,880	65	No

5 Conclusions

To define vulnerabilities of the current RDBs watermarking methods and to guarantee the RDBs authenticity and integrity, we conducted a comprehensive survey on these methods, which aided in choosing the appropriate method utilized for watermarking in databases fields. This has been done through determining essential requirements needed for the RDBs.

A new scientific method has been designed, executed, assessed, validated and tested under various types of known attacks over large amount of imaging samples to present a robust technique that realizes its efficiency through achieving the best measurements results when compared to other equivalent previous techniques.

Acknowledgement

The researchers thank the Department of Computer Science, College of Computer Science and Mathematics, University of Mosul.

References

Ali, Y. H. and Mahdi, B. S., 2011. Watermarking for Relational Database by using Threshold Generator, *Eng. & Tech. Journal*, Vol. 29(1), (pp. 33-43).

Alqassab A. and Alanezi M., 2022. Reversible Watermarking Approach for Ensuring the Integrity of Private Databases, *Springer, Lecture Notes in Networks and System (LNNS)*, (pp. 1-8).

Alqassab, A. and Alanezi, M., 2021. Relational Database Watermarking Techniques: A Survey. *Journal of Physics: Conference Series*, (pp. 1-9).

Al-Qassab, A.M. and Nori, A.S., 2014. Steganographic Technique using Fractal Image. *JITBM & ARF International Journal of Information Technology and Business Management*, Vol. 23(1), (pp. 52-59).

Begum, M. and Uddin, M. S., 2020. Digital Image Watermarking Techniques: A Review, *MDPI, Information*, (pp. 1-38).

Chang, J. and Wu H., 2012. Reversible Fragile Database Watermarking Technology using Difference Expansion based on SVR Prediction, *IEEE, International Symposium on Computer, Consumer and Control*, (pp. 690-693).

Duan, S., Wang, H., Liu, Y., Huang, L. and Zhou, X., 2020. A Novel Comprehensive Watermarking Scheme for Color Images, *WILEY/Hindawi, Security and Communication Networks*, (pp. 1-12).

Fazli, S. and Moeini, M., 2016). A Robust Image Watermarking Method based on DWT, DCT, and SVD using a New Technique for Correction of Main Geometric Attacks, *Elsevier GmbH*, Vol. 127(2), (pp. 964-972).

Gaur, P. and Manglani, N., 2015. Image Watermarking using LSB Technique, *International Journal of Engineering Research and General Science*, Vol. 3(3), (pp. 1424-1433).

Hemani and Mandoria, H. L., 2017. Digital Watermarking Approaches and its Applications: A Review, *International Journal of Control Theory and Applications*, Vol. 10(18), (pp. 343-350).

Kamran, M. and Farooq, M., 2018. A Comprehensive Survey of Watermarking Relational Databases Research, *Cornell University*, arXiv:1801.08271v1 [cs.CR], (pp. 1-20).

Kumar, H. B. B., 2016. Digital Image Watermarking: An Overview, *Oriental Journal of Computer Science & Technology*, Vol. 9(1), (pp. 7-11).

Mukherjee, S. and Jana, B., 2019. A Novel Method for High-Capacity Reversible Data Hiding Scheme using Difference Expansion, *International Journal of Natural Computing Research*, Vol. 8(4), (pp. 13-27).

Murugan, R., Abraham, J. T. and Salim, I., 2019. A Robust Watermarking Technique for Copyright Protection for Relational Databases, *International Journal of Recent Technology and Engineering (IJRTE)*, Vol. 8(3), (pp. 4040-4046).

Murugan, R., Jaseena, K. U. and Abraham, J. T., 2017. An Invisible Watermarking Technique for Integrity and Right Protection of Relational Databases, *International Journal of Applied Engineering Research*, Vol. 12(24), (pp. 15754-15758).

Ramani, S. V., 2013. Watermark Based Copyright Protection for Relational Database, *International Journal of Computer Applications*, Vol. 78(2), (pp. 22-28).

Shyamala, G., kanimozhi, C. and kavya, S. P., 2015. An Efficient Distortion Minimizing Technique for Watermarking Relational Databases, *International Journal of Scientific Engineering and Technology Research*, Vol. 4(11), (pp. 2050-2054).

Singh, N., Nagpal, B. and Kamal, P., 2016. Analysis between Various Digital Watermarking Tools and Techniques, *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol. 6(6), (pp. 364-370).

Singh, P. and Chadha, R. S., 2013. A Survey of Digital Watermarking Techniques, Applications and Attacks, *International Journal of Engineering and Innovative Technology (IJEIT)*, Vol. 2(9), (pp. 165-175).

Tzouramanis, T., 2011. A Robust Watermarking Scheme for Relational Databases, *IEEE, 6th International Conference on Internet Technology and Secured Transactions*, (pp. 783-790).

Unnikrishnan, K. and Pramod, K. V., 2017. Robust Optimal Position Detection Scheme for Relational Database Watermarking through HOLPSOFA Algorithm, *Elsevier, Journal of Information Security and Applications 35*, (pp. 1-12).

Wang, W., 2019. A Reversible Data Hiding Algorithm based on Bidirectional Difference Expansion, *Springer Science+Business Media, LLC, Multimedia Tools and Applications*, (pp. 5965-5988).

Asmaa Alqassab a lecturer at College of Education, University of Mosul, Iraq. Her M.Sc. degree was in Computer Science in the field of Computer Security from University of Mosul, Iraq in 2012.

Mafaz Alanezi is a faculty member at the Department of Computer Science, University of Mosul, Iraq. She obtained her Ph.D. degree in Computer Science in the field of Computer and Network Security from University of Mosul / Iraq in 2012. Her M.Sc. degree was also in Computer Science in the field of Image Processing from the University of Mosul/ Iraq in 2003. Her current scientific degree Prof. Dr in Cybersecurity and Information Security.