



iJRASET

International Journal For Research in
Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 Issue: VII Month of publication: July 2022

DOI: <https://doi.org/10.22214/ijraset.2022.45769>

www.ijraset.com

Call:  08813907089

E-mail ID: ijraset@gmail.com

Database Security with Fingerprint Masking

Deepa RM¹, Deepika S², Sriram Lakumarapu³

¹LG Soft India Pvt Ltd, ²TCS, ³Vasavi College of Engineerings

Abstract: Information in numerous areas including medication, business, and science was so crucial, in which directories are utilized efficiently for information sharing. Nevertheless, the directories confront the danger to be pirated, taken or even misused, which might lead to many of protection risks regarding ownership rights, information tampering as well as secrecy safeguards. Watermarking is the technology which is used to secure the database from the various attacks. It is also used to hide the content from the unauthorized users. The majority of state-of-the-art techniques alter the initial information to a big level, lead to information quality wreckage, and then can't attain balance that is good between robustness from malicious strikes as well as information restoration. We suggest a reversible and robust watermarking method with Genetic Algorithm and Histogram Shifting Watermarking (GAHSW) to relation the numerical data. This algorithm used to get the unique key for the database as well as the watermarked place. Experimental evaluation show the usefulness and methods within the terminology of robustness from malicious strikes as well as upkeep of information quality. We have achieved the security level on comparing with existing system.

Keywords: Information Security, Watermark, Reversible, Right

I. INTRODUCTION

Presently, relational directories are utilized as well as discussed thoroughly as a result of the growing usage on the Internet and also cloud computing. Nevertheless, the amazing rise in the development, sharing and transfer of directories at the same time incurs protection consequences, like information theft, unlawful copying as well as copyright violation. Thus information protection difficulties are becoming more and more visible. In fact, outsourced information may be redistributed or even customized with no authorization at proprietors. Mishaps of database leakage were found often within the past few years, even during domains including health care whereby information are delicate. Historically, watermarking methods are already used to make sure ownership safeguards as well as tamper proofing for different details platforms

II. RELATED WORK

Database watermarking was first of all released in 2002 [1]. Since then, several techniques are recommended. When it comes to, a delicate as well as strong chronic watermarking technique which embeds both public and private watermarks is suggested [2]. Depending on if the watermarking presents some alterations towards the information on the database, the watermark engineering could be classified into 2 parts: Primarily bring in robust and distortion-based watermarking strategies. The majority of the distortion based watermarking systems have been suggested to deal with distortion restrictions. For example, [3] [4] within the embedding procedure doesn't alter numerical characteristics when the accessibility problems for particular details aren't satisfied [5], focus on protecting the database stats, as well as requires into bank account the total database semantics that will additionally be preserved. [6] [7] However, these techniques change the information to a big level, which might lead to the loss in information quality. In order to conquer the issues of these distortion based techniques, reversible database watermarking continues to be brought to recoup the initial information completely soon after removing lodged watermarks through the watermarked directories [8]. Relational directories are utilized as well as discussed thoroughly as a result of the growing usage on the Internet and also cloud computing. Nevertheless, the amazing rise in the development, sharing and transfer of directories at the same time incurs protection consequences, like information theft, unlawful copying as well as copyright violation [9]. Thus information protection difficulties are becoming more and more visible. In fact, outsourced information may be redistributed or even modified with no authorization at proprietors. Mishaps of database leakage were found often within the past few years, even during domains including health care whereby information are sensitive [10].

III. PROPOSED WORK

Database entry is going to be supplied when the person provides a proper password and username. The risk that is high of database information usually tampers and tough stolen. In case another pc user wish to examine and / or alter information within the database after that without disclose watermarking the person wasn't in a position to have information that is correct, to obtain the actual information the old have to supply the reverse watermarking next just he is able to in a position to see the appropriate information.

A. Feature Analysis and Selection

This particular component consists of the information partitioning.. It is encoded by the watermark techniques that continues to be carried out by manager of the Admin. This algorithm partitions the information established directly to rational organizations through making use of information partitioning algorithm.

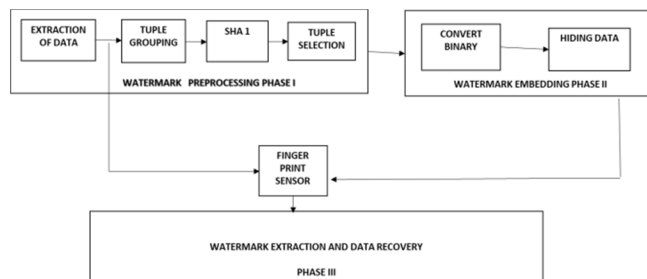


Fig . 2 Architecture Diagram Watermarking by Tuples Selection

It is a single shoot and even one specific row within a Relational Database. With this particular phase to select the specific tuples for embedding Watermarked Content. Computation is means computed for each characteristic. If the valuation of any kind of feature type of a tuple is above the respective computed threshold of its, it is selected for Encoding Process. The info option threshold for an attribute is believed.

B. Watermark Encoding

Watermark bits are lodged during the first information established by making use of watermark embedding algorithm. The suggested algorithm embeds every bit a multibit watermark made of day period for each and every selected row. The watermark bits are lodged in the selected tuples by installing a good watermarking goal. Our technique embeds each share on the watermark at every single selected tuple of each and every partition.

C. Watermark Decoding and Edge detection Authentication

Authentication is recommended as being an alternative therapy for textual material reliant. It is mainly depends on customer fingerprint rather than alphanumeric. The main argument here is that pass-user's finger print documents electronic documents immediately after what he/she is gonna be authenticated users are far of higher quality during understanding. The finger print documents written documents has to be saved with Server For that Specific User. All through Login phase Admin must find out the point with the fingerprint of his. Basically authentication is simple; a real computer person needs to correctly provide the fingerprint of his after that he/she is gonna be authenticated.

Watermark Extraction process in the Decoding point. The Watermarked Content has to be extracted exclusively by legitimate computer pc user to create the correct ownership. If the User ownership created written content is matched up in place by content material was produced through the Admin, Decoding treatment has to achieve. Otherwise it is not achieved.

D. Proposed Algorithm

- 1) Step 1: The user need to register with their details and finger print.
- 2) Step 2: Extract the required data from the database.
- 3) Step 3: The data selected will be viewed.
- 4) Step 4: The tuple will be grouped using the primary key.
- 5) Step 5: Divide the dataset into four partitions.
- 6) Step 6: Using sha-1 algorithm the hashing will be done on the dataset.
- 7) Step 7: Selection and rejection of tuples using primary key.
- 8) Step 8: Convert the selected data into binary.
- 9) Step 9: Hide the data using watermark embeddings so the data will be hidden securely.
- 10) Step 10: To recover the data user need to login using the registered information. Authentication will be done using finger print.
- 11) Step 11: The original data will be shown to the authorized user.

IV. RESULT AND DISCUSSIONS

The experiments are performed using the TOMCAT 7.0 and MYSQL 5.0 version. The computations are performed using Toolbox that is readily available in TOMCAT. Connecting local server to improve the testing of each connection and redirect the pages and links.

A. Registration through Fingerprints

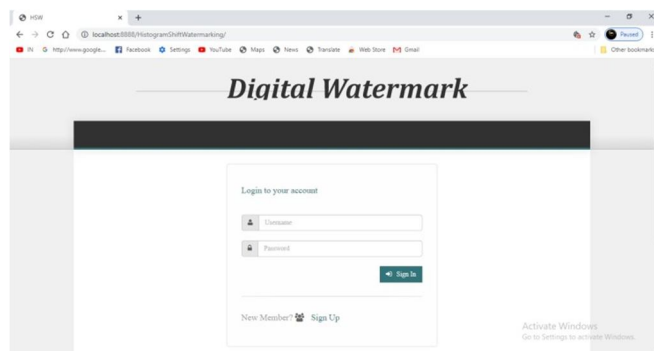


Fig . 3 User Registration Portal

User needs to sign up with their fingerprint and personal details . The system register the user account provided by the user . After sign up you need to login with the user detailed as provided before.

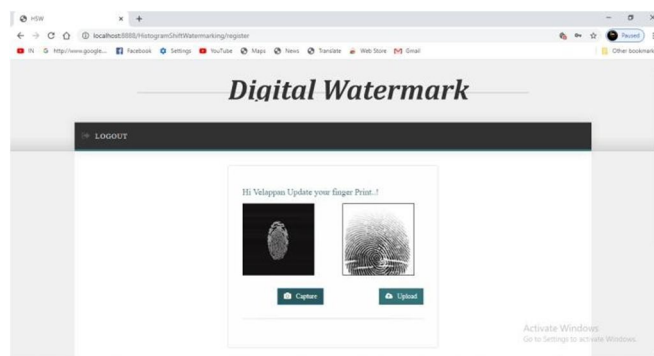


Fig . 4 Register the fingerprint of user

Register the fingerprint . It also register with the user details . Biometric scanner used in this Digital Watermarking for the Security purposes.

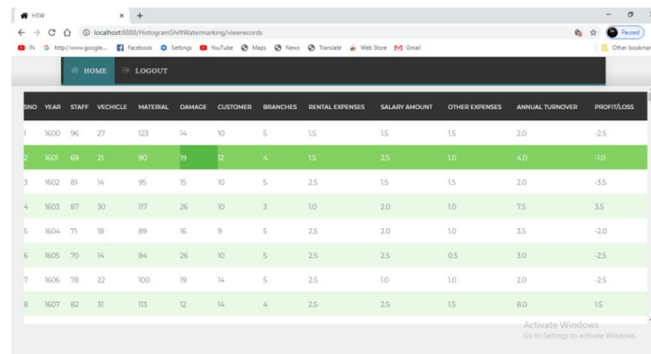
B. Structure of the Data Set

Fig . 5 Generate Report



Extract the data set from the databases . The extracted data will be Reported as a summary.

To view the data sets of a certain organization or other commercial industries.

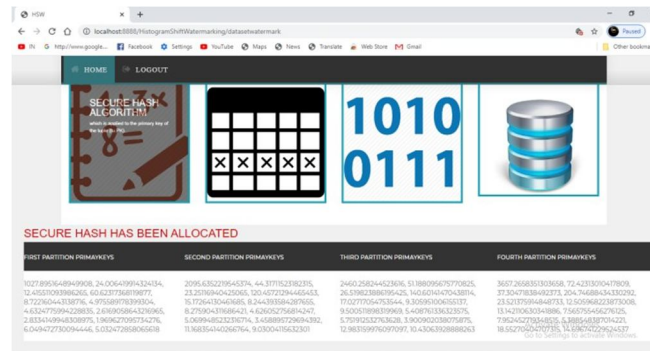


ID	YEAR	STAFF	VEHICLE	MATERIAL	DAMAGE	CUSTOMER	BRANCHES	RENTAL EXPENSES	SALARY AMOUNT	OTHER EXPENSES	ANNUAL TURNOVER	PROFIT/LOSS
1	1600	96	27	123	14	10	5	15	15	15	2.0	-2.5
2	1601	69	31	90	19	12	4	15	2.5	10	4.0	-1.0
3	1602	81	14	95	15	10	5	2.5	15	15	2.0	-3.5
4	1603	87	30	177	26	10	3	10	2.0	10	7.5	3.5
5	1604	71	18	89	16	9	5	2.5	2.0	10	3.5	-2.0
6	1605	70	14	84	26	10	5	2.5	2.5	0.5	3.0	-2.5
7	1606	78	22	100	19	14	5	2.5	10	10	2.0	-2.5
8	1607	82	31	113	12	14	4	2.5	2.5	15	8.0	1.5

Fig . 6 Database from the data sets

The primary keys were used to divided the data into four partitioning data sets . Each group will be partitioned as tuples using primary keys . Tuples Grouping will be done on the above data set provided .

C. Encrypted Data Set



SECURE HASH ALGORITHM

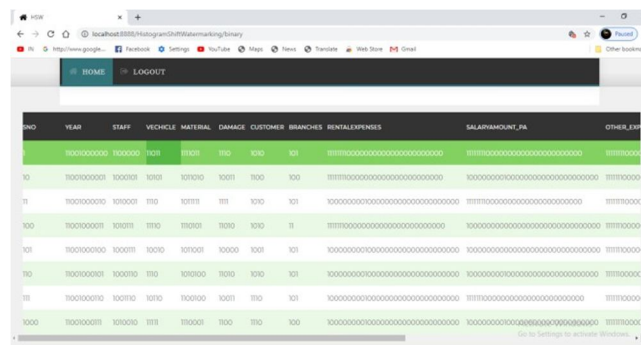
SECURE HASH HAS BEEN ALLOCATED

FIRST PARTITION PRIMARYKEYS	SECOND PARTITION PRIMARYKEYS	THIRD PARTITION PRIMARYKEYS	FOURTH PARTITION PRIMARYKEYS
1027.89564894908, 24.0064991424354, 12.465093898262, 63.62377697977, 8.7226204438786, 4.9758978393004, 4.632475994228835, 2.61695984321096, 2.83343964630897, 1.960627099734276, 6.04947273009446, 5.032472858060618	2095.638229545374, 44.37115218235, 22.578840420306, 100.4772394464543, 15.1726413040486, 8.244393894287655, 8.2739437868421, 4.62632758842407, 6.08994462323674, 6.448897226949362, 11.56835444264764, 9.0300475632301	2462.25624432896, 51.98899567770825, 26.53982388978425, 140.604047043854, 17.0277705473544, 9.3069500405037, 9.500518881879948, 5.40876133623075, 5.7091623763628, 5.90092023867875, 12.98319976097097, 15.43063928888263	3697.265835303658, 72.423300477805, 27.3047838492373, 204.74688454332082, 23.5217591484873, 12.50196822873008, 13.14219363044896, 7.66575946276125, 7.96244273556555, 6.3885483704323, 18.5527050477715, 14.39676227962437

Fig . 7 Secure Hash Algorithm

The Tuples which are grouped in the above step will be Hashed using SHA-1 Algorithm for Security purposes . The tuple selection and rejection of data will be done so that the unauthorized user will not able to access it.

D. Binary Format Data Set



COVERT BINARY

ID	YEAR	STAFF	VEHICLE	MATERIAL	DAMAGE	CUSTOMER	BRANCHES	RENTAL EXPENSES	SALARY AMOUNT_PA	OTHER_EXP
1	1600	96	27	123	14	10	5	15	15	15
2	1601	69	31	90	19	12	4	15	2.5	10
3	1602	81	14	95	15	10	5	2.5	15	15
4	1603	87	30	177	26	10	3	10	2.0	10
5	1604	71	18	89	16	9	5	2.5	2.0	10
6	1605	70	14	84	26	10	5	2.5	2.5	0.5
7	1606	78	22	100	19	14	5	2.5	10	10
8	1607	82	31	113	12	14	4	2.5	2.5	15

Fig . 8 Covert Binary

The Selected tuples will be converted to binary and the data will be distorted again the whole data set will be distorted for added security.

E. Hiding the data set using Watermarking

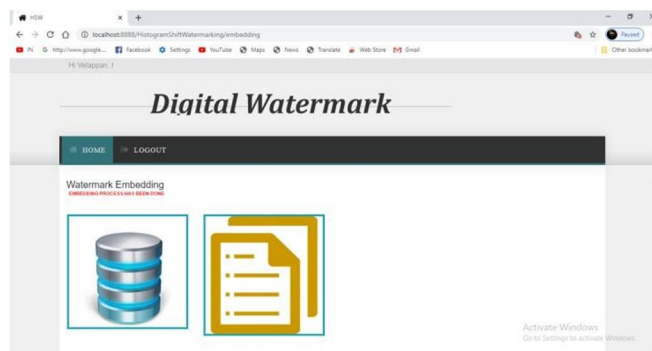


Fig . 9 Watermarking embedding

Hiding the data set watermark technique by embedding fake data again it was crosschecked whether the data was hidden and fake data was watermarked.

F. Database Retrieval Through Fingerprint

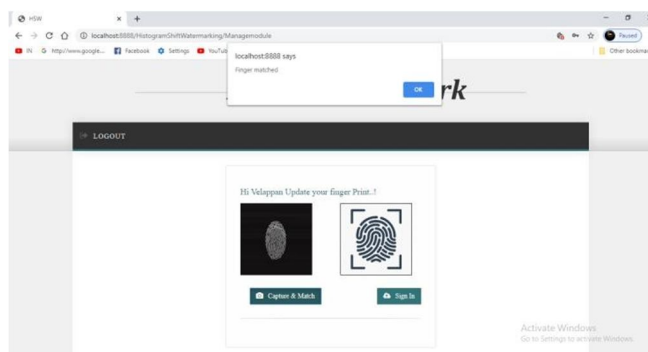
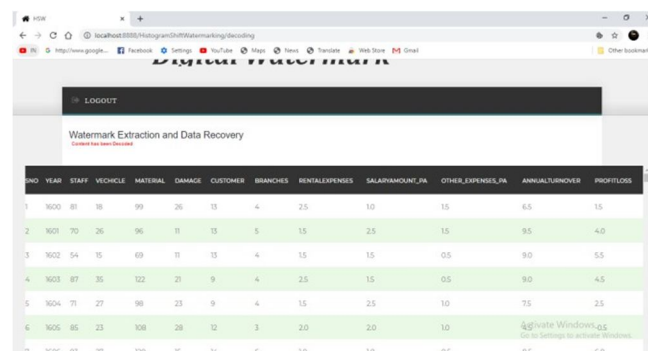


Fig . 10 Fingerprint Authentication

Retrieving the data using fingerprint provided during the sign up phase . Once the fingerprint matches hidden data will be revealed for security purposes.

G. Extracted Original Data



ID	YEAR	STAFF	VEHICLE	MATERIAL	DAMAGE	CUSTOMER	BRANCHES	RENTAL EXPENSES	SALARY AMOUNT, PA	OTHER EXPENSES, PA	ANNUAL TURNOVER	PROFIT/LOSS
1	1600	81	18	99	26	13	4	2.5	1.0	15	6.5	15
2	1601	70	26	96	11	13	5	1.5	2.5	15	9.5	4.0
3	1602	54	15	69	11	13	4	1.5	1.5	0.5	9.0	5.5
4	1603	87	35	122	21	9	4	2.5	1.5	0.5	9.0	4.5
5	1604	71	27	98	23	9	4	1.5	2.5	1.0	7.5	2.5
6	1605	85	23	108	28	12	3	2.0	2.0	1.0	8.5	6.0
7	1606	93	27	120	15	14	6	1.0	1.0	0.5	8.5	6.0

Fig . 11 Data Recovery

The original data which is recovered from the hidden data will be showed to the authorized person so that the security will be maintained.

V. CONCLUSION

Watermarking has turned into a great exploration because the growing need of ownership safeguards when discussing repository information. Transformations inside the database that significantly compromise the information quality are made by conventional watermarking methods. Reversible watermarking methods are accustomed to fix the dilemma since they are able to recoup authentic details through the watermarked database as well as make sure information quality. Although the strategies aren't strong sufficiently from malicious episodes, a lot of reversible watermarking methods are recommended.

REFERENCES

- [1] Chai, H., Yang, S., Jiang, Z. L., Wang, X., Chen, Y., & Luo, H. (2019, December). A New Robust and Reversible Watermarking Technique Based on Erasure Code. In *International Conference on Algorithms and Architectures for Parallel Processing* (pp. 153-168). Springer, Cham.
- [2] Li, Y., Wang, J., Ge, S., Luo, X., & Wang, B. (2019). A reversible database watermarking method with low distortion. *Mathematical biosciences and engineering: MBE*, 16(5), 4053-4068.
- [3] Zhao, M., Jiang, C., & Duan, J. (2019, October). Reversible Database Watermarking Based on Differential Evolution Algorithm. In *2019 International Conference on Artificial Intelligence and Advanced Manufacturing (AIAM)* (pp. 120-124). IEEE.
- [4] Kamble, P., Raut, N., Raut, A., & Naik, S. (2019, April). An Innovative Approach for Data Recovery Using Robust Reversible Watermarking. In *2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI)* (pp. 1401-1404). IEEE.
- [5] Agarwal, N., Singh, A. K., & Singh, P. K. (2019). Survey of robust and imperceptible watermarking. *Multimedia Tools and Applications*, 78(7), 8603-8633.
- [6] Sabbane, F., Aherrahrou, N., & Tairi, H. (2019, March). A new region based watermarking scheme for medical images. In *Proceedings of the New Challenges in Data Sciences: Acts of the Second Conference of the Moroccan Classification Society* (pp. 1-6).
- [7] Hurrah, N. N., Parah, S. A., & Sheikh, J. A. (2019). A Secure Medical Image Watermarking Technique for E-Healthcare Applications. In *Handbook of Multimedia Information Security: Techniques and Applications* (pp. 119-141). Springer, Cham.
- [8] Khan, M. A., Khan, U. A., Ali, A., Hussain, F., & Nisar, W. (2019). A Robust Color Image Watermarking Scheme using Chaos for Copyright Protection. *Mehran University Research Journal of Engineering and Technology*, 38(2), 361-378.
- [9] Chang, T. J., Pan, I. H., Huang, P. S., & Hu, C. H. (2019). A robust DCT-2DLDA watermark for color images. *Multimedia Tools and Applications*, 78(7), 9169-9191.
- [10] Kumar, C. V., Natarajan, V., Nirmala, K., Balasubramanian, T., Rao, K. R., & Krishnan, S. (2019). Encrypted separable reversible watermarking with authentication and error correction. *Multimedia Tools and Applications*, 78(6), 7005-7027.



10.22214/IJRASET



45.98



IMPACT FACTOR:
7.129



IMPACT FACTOR:
7.429



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089  (24*7 Support on Whatsapp)