VOL. 10, NO. 14, AUGUST 2015 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

REVERSIBLE WATERMARKING TECHNIQUE USING TIME-STAMPING FOR RELATIONAL DATA

Malathi K. and Veeramuthu A.
Department of Information Technology, Sathyabama University, Chennai, India
E-Mail: aveeramuthu@gmail.com

ABSTRACT

Watermarking procedure is a conspicuous pattern used to recognize credibility. This procedure is elusive and harm against malicious attack. Watermarking has been utilized for ownership protection for a couple data organizations like pictures, video, sound, program, xml records, geographic information frameworks related data, content archives, relational databases that are utilized as a part of distinctive application domains. As of late, cunning mining systems have been utilized for data which is extracted from relational databases. This is utilized to identify captivating patterns that give critical backing to leaders in making compelling, right, and applicable choices. By and large, data imparted between its proprietors and true blue clients obliges data security. To be sure data protection and security, proprietor's database is outlined with watermarking data. The proprietor of the social database implants the watermark data. The bends in the first data are kept inside positive points of confinement, which are characterized by the ease of use limitations that save the learning contained in the data. The proposed method inserts each minor bit of a multi bit watermark in every chose column with the point of having greatest vigor. Guaranteeing the assailant is not able to degenerate the watermark of the dataset.

Keywords: reversible watermarking, relational data, malicious attack, security, ownership protection.

INTRODUCTION

Watermarking techniques are used to ensure security in terms of ownership protection and tamper proofing of a wide variety of data formats. This includes images, audio, video, natural language processing software, relational databases and more. Today, database relations are generally utilized and appropriated over the web. Since this information can be essentially intruded with, it is hard to verify the uprightness of these learning. Another developing ability advanced watermarking, supplements cryptography. This is finished by inserting an imperceptible flag straightforwardly into the learning, consequently it gives a beyond any doubt approach to shield advanced information from disallowed duplicating & adjustment. In the wake of implanting, the watermark & the information cannot be separated. Reversible watermarking techniques can ensure the data recovery along with ownership protection. Watermarking has the property that it can provide ownership protection over the digital content by marking the data with a watermark unique to the owner. The embedded watermark can consequently be used for proving and claiming ownership. With the advent of modern copyright protection and information hiding techniques, database watermarking can be used to enforce ownership rights of relational data. However a major drawback of these techniques is that they modify the data to a very large extent which often results in the loss of data quality. There is a strong need to preserve the data quality in watermarked data so that it is of sufficiently high quality and helps to fit for use in decision making as well as in planning processes in different application domains. Data quality can be defined as the appropriateness of data for its intended applications. Achieving robustness (attack resilience) in the presence of reversibility (ability to recover the watermark and the original data) is a challenging task. The knowledge of mutual information for every candidate feature is also employed to compute the watermark information. Digital watermarks can be ordered into classifications in light of their application: delicate watermarks for alter location & vigorous watermarks for ownership confirmation. As of late, a few scientists started to perceive the significance of watermarking the databases and proposed some strong watermarking plans for the database relations. Notwithstanding, these plans are intended to ensure the copyright of a database connection. In spite of the fact that it is essential to affirm the source or proprietor of a database connection, sometimes, it is hard to affirm the credibility of database relations. This is of expanding enthusiasm for a lot of utilizations where the database relations are freely accessible on the Web. For instance, in the utilization of the database outsourcing, proprietors of databases, who don't have sufficient assets to keep up the applications, store their databases on servers gave by outside application administration suppliers so that the proprietor can check and concentrate all alone center errands. The application administration suppliers give learning handling administration to customers for the proprietors. Since administration wholesalers may not be believed, it is the database proprietor's obligation to verify the uprightness of outsourced databases. Comparable applications incorporate edge processing and learning dispersal and so forth. A watermarking technique can be delegated either vigorous or delicate.

Powerful watermarks are normally utilized for copyright and ownership confirmation. In examination,

delicate watermarks are valuable for purposes of confirmation and uprightness authentication. A delicate watermark gives on ensure that the photo has not been messed with and originated from the right source. The late surge in the development of the Net finishes in offering of an assortment of online administrations, for example, database as an administration, computerized vaults and libraries, e business, online choice bolster strategy and so forth. These applications make the computerized resources, for example, advanced pictures, video, sound, database substance are fundamentally accessible by standard individuals around the globe for offering, buying, conveying, or a lot of different purposes. Because of this, such advanced items are confronting genuine difficulties like theft, unlawful redistribution, ownership asserting, falsification, robbery and so forth. Advanced watermarking skill is a compelling answer for meeting such difficulties. A watermark is contemplated to be information that is installed into basic data for alter location, confinement, ownership verification, backstabber following and so forth. Reversible watermarking systems can verify data recuperation alongside ownership insurance. For various types of utilizations, advanced watermarking should fulfill distinctive properties. The watermarking can be processed by adjusting or embeddings learning at a bit level or larger amount. For this sort of utilization, advanced watermarking should have properties like delicacy, imperceptibility, high recognition dependability etc. Accordingly, it is guaranteed that the data quality won't be influenced. Hence, it gives an intense answer for data recuperation that is reversible and strong against overwhelming assaults.

RELATED WORK

In [1], suggest a change over the Agrawal and Kiernans method, in lieu of utilizing hash capacity, they utilize disorderly arbitrary arrangement taking into account the Logistic disarray mathematical statement which has properties: the non-dull iterative operation and the affectability to preparatory worth. It keeps away from the innate shortcoming of crash of Hash capacity. The decision of bits of LSB for implanting watermark meets the prerequisites of both learning reach and information exactness of every characteristic, than fundamentally to make utilization of a same methodology for all traits. So, the mistake brought about by watermark is diminished altogether, not exceptionally influences the accessibility of the database.

In [2], depict a picture based watermarking plan where as opposed to implanting unique picture as watermark, a mixed picture taking into account Arnold change with scrambling number is utilized. Since Arnold change of a picture has the periodicity P, the outcome which is gotten in the extraction stage can be recouped from the mixed structure to the first after emphases. In the installing stage, the first picture of size is initially changed over into mixed picture which is then spoken to by a twofold string of length. Furthermore, all tuples in the connection are gathered into L bunches. The hash quality is registered utilizing tuple's essential key, mystery key and request of the picture. The gathering of the tuple is resolved utilizing the figured hash value.

In [3], installs important watermark data by first changing over it into a bit stream. The plan registers exceptional ID for all tuples in the connection and sorts them in rising request as indicated by their ID values. The tuples are then divided into gatherings every containing tuples. The bit stream is implanted into the chose tuples in gathering by taking after same choice criteria as in AHK calculation with special case that it considers just single ascribe to check. Before conferring the change, a limitation capacity is utilized to check whether the change surpasses the information ease of use limits. The imperative capacity incorporates the fundamental information measurable estimation, semantics and auxiliary imperatives.

In [4], displays an alternate way to deal with powerful watermarking plan for databases. Not at all like Agrawal's tuple based watermarking plan, Sion's plan is subset based where all tuples are safely partitioned into non-converging subsets. A solitary watermark bit is inserted into tuples of a subset by changing the dispersion of tuple qualities. The same watermark bit is implanted more than once over a few subsets and the lion's share voting strategy is utilized to recoup the inserted bits. Notwithstanding the subset assault, this plan is asserted to be strong against different assaults, for example, information turning and information change. Notwithstanding, the plan is not suitable for database relations that need continuous overhauls, since it is extremely lavish to re-watermark the overhauled database relations.

In [5], the author declared the first reversible watermarking scheme for relational databases. In this technique, histogram expansion is used for reversible watermarking of relational database. The histogram expansion technique helps to reversibly watermark the selected nonzero initial digits of errors. This technique keeps track of overhead information to authenticate data quality. However, this technique is not robust against heavy attacks (attacks that may target large number of tuples).

In [6], proposed vigorous, visually impaired, strong and reversible, picture based watermarking plan for huge scale databases. The bit string of a picture is utilized as a watermark where one bit from the bit string is inserted in all tuples of a solitary part and the same methodology is rehashed for whatever is left of the parcels. This strategy exhibits a striking reduction in watermark location rate amid different sorts of overwhelming assaults, and the database tuples get exceptionally contorted.

In [7], proposed a reversible watermarking technique introduces distortions as a result of the embedding process. Changes in the data are controlled by placing certain bounds on LSB. On the contrary, to limit the distortions, the data outside the limited bounds is left un-watermarked. As a result, the watermark robustness gets compromised.

In [8], proposed the reversible watermarking by the forecast mistake developer. The Prediction-lapse development watermarking strategies like join indicator rather than a distinction administrator to choose applicant pixels or highlights for installing of watermark data. The proposed strategy is delicate against noxious assaults as the watermark data is inserted in the fragmentary piece of numeric highlights just. In this specific situation, the plan lives up to expectations on the grounds that the aim of the assailant is to protect the convenience of the information.

PROPOSED WORK

Problem description

The diverse watermarking strategies that exhibit the surprising diminishing in watermark recognition rate, database tuples get profoundly twisted, not strong against overwhelming assaults and misfortune in information quality. Therefore improves the reversible watermarking method for social information that guarantees information recuperation without bargaining information quality and most extreme strength.

System architecture

System Architecture presents a high level overview of how the functions and responsibilities of the system were partitioned or components which, are shown in Figure-1. The owner or an admin of the database is one who creates the record to generate the multi bit from UTC (Universal Time Coordination) which is to be secured. The authorized user can get the permission from the admin to share the data from a database. Then the admin has to partition the data and selection of particular tuples for embedding the watermarked content. At that point the edge calculation is processed for every attribute. In the event that the estimation of any credit of a tuple is over its particular processed edge, it is chosen for encoding procedure. During registration phase admin has to provide some images to the user. The legitimate user is supposed to choose the image for the verification phase. That image is to be stored in the server for the specific user. During login phase admin has to convert the raw image to gray scale followed by the edge detection image. The idea here is the user will have a challenge set which contains decoy and selected images of the user. The decoy images are randomly generated by the scheme during the verification process. Basically the authentication is simply a legitimate user needs to correctly identify the selected images from the challenge set and he/she will be authenticated. The watermarked content has to be extracted only by the legitimate user to give the proper ownership. If the user ownership content is matched by the admin generated content, the decoding process has to be done.

Data group partitioning

In this part, the data is partitioned with the help of a data partitioning algorithm. Partitioning the data is done by the admin. The proprietor of the social database inserts the watermark information; the twists in the first information are kept inside specific cutoff points, which are characterized by the ease of use limitations, to save the learning contained in the information. The proposed calculation implants all of a multi bit watermark (produced from date-time) in every chose line (in a numeric quality) with the target of having most extreme power regardless of the possibility that an aggressor is by one means or another ready to effectively degenerate the watermark in some chose a piece of the information set. The proposed framework executes another way to deal with creating the watermark bits from UTC date-time, which is the essential time standard used to synchronize the time everywhere throughout the world. A hearty watermark calculation is utilized to implant watermark bits into the information set of database proprietor. Admin or owner of a database is responsible for creating the records which are to be more secure. The admin has to partition the dataset which is already present in the records. Data partitioning comes under watermark encoding phase, which has been done by the owner of the database. The data partitioning method partitions the data set into a logical set of groups, which is shown in equation (1) and refer the algorithm 1 for data partitioning.

$$Par(t) = H(S_k||H\left(t{:}\ K_p\middle||S_k\right))\ mod\ \ N \qquad (1)$$

Where t: K_p is the primary key of the given tuple t, H () is a cryptographic hash function message digest, || is the operator for concatenation, and S_k is a secret key. The petition is based on the data partitioning algorithm where the partitions have a primary key which is not redundant. Logical groups or partitions have been achieved using this algorithm. The group's length is decided by the owner of a database. Therefore the admin plays a vital role and give a clear vision to share the data to their legitimate users for the purpose of ownership protection.

Tuple selection

A tuple is one record or one row in a relational database. The data partitions or data groups are the input of the tuple selection. From the data partitions, the threshold calculation is applied for the each row using the defined formula. Threshold computation is a strategy figured for every quality. In the event that the estimation of any characteristic of a tuple is over its separate figured

edge, it is chosen for encoding procedure. The information choice edge for a trait is computed by utilizing the accompanying mathematical statement, shown in equation (2) and sees the algorithm 2 for tuple selection:

$$T = C * M + SD \quad (2)$$

Where, C is the confidence factor with a quality somewhere around 0 and 1. The confidence factor, c is kept mystery to make it exceptionally troublesome for an aggressor to figure the chose tuples in which the watermark is embedded. The administrator needs to choose just those tuples, amid the encoding process, whose qualities are above T. At that point the utilization of a hash value processing for the chose tuples. In this step, a cryptographic hash function is connected to the course information set to, choose just those tuples which have an even hash value.

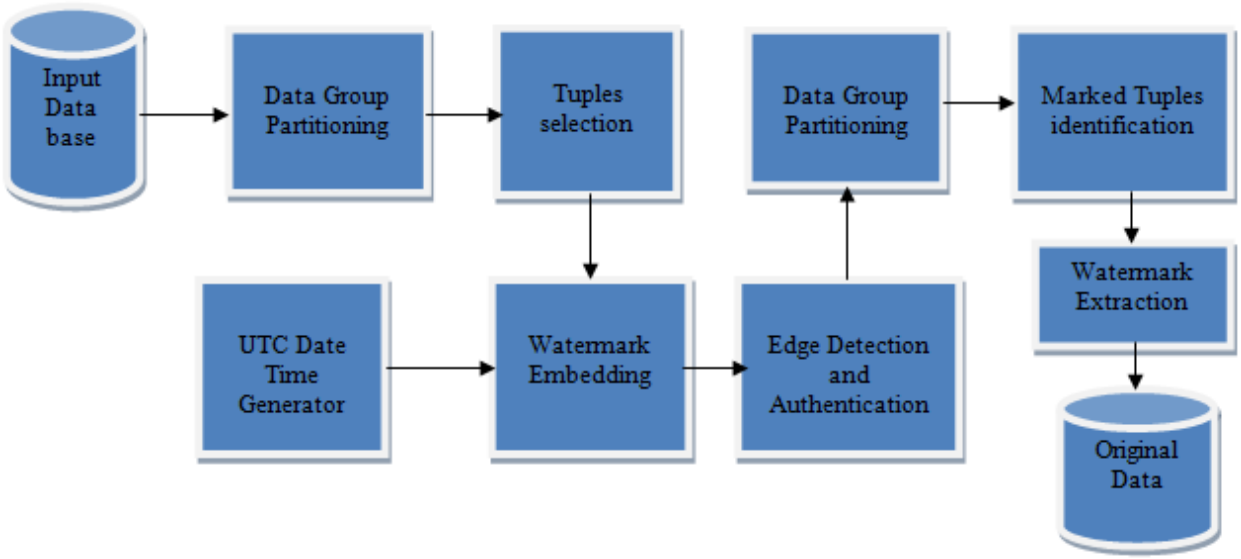


Figure-1. System architecture.

Watermark encoding

The watermark creating capacity takes date-time stamp as information and afterward produces watermark bits b1b2 . . . bn from this date-time stamp. Watermark bits are given as data to the watermark encoding capacity. The date-time stamp "may" additionally help to distinguish added substance assaults in which an aggressor needs to re-watermark the data set.

Edge detection authentication and watermark decoding

Edge detection Authenticator is proposed as an alternative solution to text based. It is mainly depends on images rather than alphanumerical. The main argument here is that the pass-images from the challenge set and then he/she will be authenticated users are better at recognizing and memorizing pictures.

During Registration phase Admin has to provide some images to the user. In the registration phase the user is supposed to choose the pass-images for the verification phase. That image has to be Stored on Server For that Specific User. During Login phase Admin has to convert the raw image to a gray scale followed by Edge detection image. The idea here is the user will have a challenge set which contains decoy and pass-images. The decoy images are randomly generated by the scheme during the verification process.

On the other hand, pass-image will be the users selected images. Basically authentication is simple; a legitimate user needs to correctly identify pass-images from the challenge set and then he/she will be authenticated.

Watermark Extraction process in the Decoding phase. The Watermarked Content has to be extracted only by the legitimate user to give the proper ownership. If the User ownership content is matched by the Admin generated content, Decoding process has to do. Otherwise, it's not done.

Algorithms

Input: Data Set D_s, Secret Key S_k,
Number of partitions N
Output: Data partitions $q_0,.....,q_{n-1}$
Begin
For each tuple t € D_s do
Par(t)←$H(S_k \| H(t:K_p \| S_k))$ mod N
Insert t into $q_{Par(t)}$
End for
Return $q_{0,....,}q_{n-1}$
End

Algorithm 1: Data Partitioning

Input: Data partitions $q_0,.....,q_{n-1}$,C
Output: Data set Ds'_T
Begin
For each attribute A€q;do
Compute M and SD on A
Calculate T=C*M+SD
End for
Return Ds'_T←T
End

Algorithm 2: Tuple Selection

Input: Data set Ds'_T, S_k
Output: Ds''_T
Begin
For each t € $D_s{}'_T$ do
Even value (t) = H ($S_k \| t: K_P$) mod 2
If even value==0
Then
Insert t into $D_s{}''_T$
Else
Not refer this tuple for watermarking
Endif
Endfor
Return $D_s{}''_T$
End

Algorithm 3: Selection of Tuple for Watermarking

EXPERIMENTAL RESULTS AND DISCUSSIONS

Figure-2 shows the data partitioning, which comes under watermark encoding phase which has been done by owner of the database (i.e.) admin. The group's length is decided by the admin. The partitioning process of data is based on the data partitioning algorithm.

The data selection threshold for an attribute is calculated by using the equation T=C* M+ SD Where, C is the confidence factor with a value between 0 and 1. The confidence factor c is kept secret to make it very difficult for an attacker to guess the selected tuples in which the watermark is inserted.

A tuple is one record or one row in a relational database. In this phase the selection of the particular tuples based on the threshold computation. If the tuple's value is above than the computed threshold value it is selected for watermark embedding which, is shown in Figure-3.

The watermark encoding with the selected tuples are shown in Figure-4 and algorithm 3.

Edge detection, authentication is method as an alternative solution for text based. It is mainly depends on images rather than alphanumerical. The main argument here is that pass-images from the challenge set and then he/she will be authenticated users are better at recognizing and remembering pictures.

PERFORMANCE ANALYSIS

As per our experiments when more than 80% of the data was deleted, the DPA watermark was detected with 100% accuracy. We compared DPA with well known reversible watermarking techniques for detecting the watermark information after such attacks.

Table-1. Performance comparison.

Methods	Accuracy (%)
GADEW	80.0
DEW	90.0
PEEW	97.0
DPA	97.7

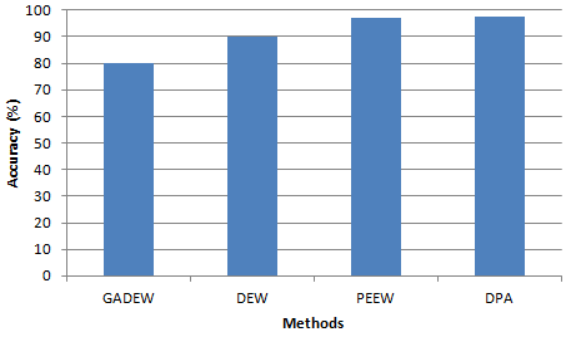


Figure-6. Performance comparison graph.

DPA (Data Partitioning Algorithm) is highly robust as compared to GADEW(Genetic Algorithm based on difference Expansion watermarking), PEEW(Prediction-error expansion watermarking) and DEW (Difference Expansion watermarking) techniques is the analysis of the three methods. DPA 100% accuracy compares to GADEW, PEEW and DEW gave less accuracy which is shown in Table-1 and Figure-6.

PARTITION GROUP HAS BEEN ALLOCATED

FIRST PARTITION PRIMAYKEYS	SECOND PARTITION PRIMAYKEYS	THIRD PARTITION PRIMAYKEYS	FOURTH PARTITION PRIMAYKEYS
4, 9, 21, 35, 38, 45, 56, 60, 65, 67, 68, 69, 75, 85, 86, 99, 105, 107, 112, 114, 123, 140, 143, 144, 145, 150, 153, 159, 160, 166, 169, 170, 171, 174, 180, 181, 208, 212, 216, 217, 218, 224, 229, 238, 239, 244, 249, 250, 251, 254, 255, 259, 265, 269, 273, 274, 275, 281, 282, 284, 292, 299, 300, 301, 311, 314, 315, 320, 324, 326, 327, 329, 345, 350, 357, 358, 361, 362, 366, 368, 371, 374, 378, 379, 385, 386, 387, 392, 395, 401	1, 2, 5, 6, 25, 27, 32, 36, 41, 43, 47, 48, 50, 57, 62, 64, 66, 74, 78, 83, 84, 98, 100, 103, 108, 110, 111, 119, 127, 128, 129, 131, 132, 134, 137, 148, 156, 172, 173, 176, 189, 194, 195, 198, 203, 205, 206, 215, 220, 221, 225, 226, 230, 232, 236, 237, 245, 246, 247, 252, 253, 272, 290, 303, 319, 325, 330, 336, 339, 341, 349, 353, 354, 355, 356, 360, 369, 372, 376, 377, 393, 394, 398	7, 8, 14, 15, 20, 22, 26, 29, 31, 33, 34, 42, 46, 58, 73, 77, 87, 88, 89, 90, 92, 93, 94, 95, 96, 101, 102, 109, 113, 115, 117, 120, 122, 125, 133, 135, 139, 141, 142, 146, 147, 151, 152, 154, 155, 158, 162, 163, 165, 167, 175, 177, 183, 184, 185, 187, 188, 193, 199, 200, 207, 209, 210, 211, 213, 222, 223, 227, 240, 243, 248, 256, 257, 258, 260, 262, 263, 267, 270, 271, 276, 277, 283, 287, 289, 294, 296, 297, 302, 304, 305, 308, 309, 310, 312, 316, 318, 321, 334, 335, 340, 342, 343, 344, 348, 352, 359, 363, 364, 365, 367, 373, 375, 380, 388, 390, 396, 399, 400	3, 10, 11, 12, 13, 16, 17, 18, 19, 23, 24, 28, 30, 37, 39, 40, 44, 49, 51, 52, 53, 54, 55, 59, 61, 63, 70, 71, 72, 76, 79, 80, 81, 82, 91, 97, 104, 106, 116, 118, 121, 124, 126, 130, 136, 138, 149, 157, 161, 164, 168, 178, 179, 182, 186, 190, 191, 192, 196, 197, 201, 202, 204, 214, 219, 228, 231, 233, 234, 235, 241, 242, 261, 264, 266, 268, 278, 279, 280, 285, 286, 288, 291, 293, 295, 298, 306, 307, 313, 317, 322, 323, 328, 331, 332, 333, 337, 338, 346, 347, 351, 370, 381, 382, 383, 384, 389, 391, 397

Figure-2. Data partitioning.

TUPLE SELECTION PRIMARY KEYS

FIRST PARTITION PRIMAYKEYS	SECOND PARTITION PRIMAYKEYS	THIRD PARTITION PRIMAYKEYS	FOURTH PARTITION PRIMAYKEYS
4, 9, 21, 35, 38, 45, 56, 60, 65, 67, 68, 69, 75, 85, 86, 99, 105, 107, 112, 114, 123, 140, 143, 144, 145, 150, 153, 159, 160, 166, 169, 170, 171, 174, 180, 181, 208, 212, 216, 217, 218, 224, 229, 238, 239, 244, 249, 250, 251, 254, 255, 259, 265, 269, 273, 274, 275, 281, 282, 284, 292, 299, 300, 301, 311, 314, 315, 320, 324, 326, 327, 329, 345, 350, 357, 358, 361, 362, 366, 368, 371, 374, 378, 379, 385, 386, 387, 392, 395, 401	1, 2, 5, 6, 25, 27, 32, 36, 41, 43, 47, 48, 50, 57, 62, 64, 66, 74, 78, 83, 84, 98, 100, 103, 108, 110, 111, 119, 127, 128, 129, 131, 132, 134, 137, 148, 156, 172, 173, 176, 189, 194, 195, 198, 203, 205, 206, 215, 220, 221, 225, 226, 230, 232, 236, 237, 245, 246, 247, 252, 253, 272, 290, 303, 319, 325, 330, 336, 339, 341, 349, 353, 354, 355, 356, 360, 369, 372, 376, 377, 393, 394, 398	7, 8, 14, 15, 20, 22, 26, 29, 31, 33, 34, 42, 46, 58, 73, 77, 87, 88, 89, 90, 92, 93, 94, 95, 96, 101, 102, 109, 113, 115, 117, 120, 122, 125, 133, 135, 139, 141, 142, 146, 147, 151, 152, 154, 155, 158, 162, 163, 165, 167, 175, 177, 183, 184, 185, 187, 188, 193, 199, 200, 207, 209, 210, 211, 213, 222, 223, 227, 240, 243, 248, 256, 257, 258, 260, 262, 263, 267, 270, 271, 276, 277, 283, 287, 289, 294, 296, 297, 302, 304, 305, 308, 309, 310, 312, 316, 318, 321, 334, 335, 340, 342, 343, 344, 348, 352, 359, 363, 364, 365, 367, 373, 375, 380, 388, 390, 396, 399, 400	3, 10, 11, 13, 16, 17, 18, 19, 23, 24, 28, 30, 39, 40, 44, 49, 54, 55, 59, 61, 63, 71, 72, 76, 79, 80, 81, 82, 91, 104, 106, 118, 121, 124, 126, 136, 138, 157, 161, 164, 168, 179, 182, 186, 190, 191, 192, 196, 197, 201, 202, 214, 219, 228, 233, 235, 241, 242, 261, 266, 278, 280, 285, 286, 291, 293, 295, 298, 306, 307, 313, 317, 322, 323, 331, 332, 337, 338, 346, 351, 370, 381, 382, 383, 384, 389, 397

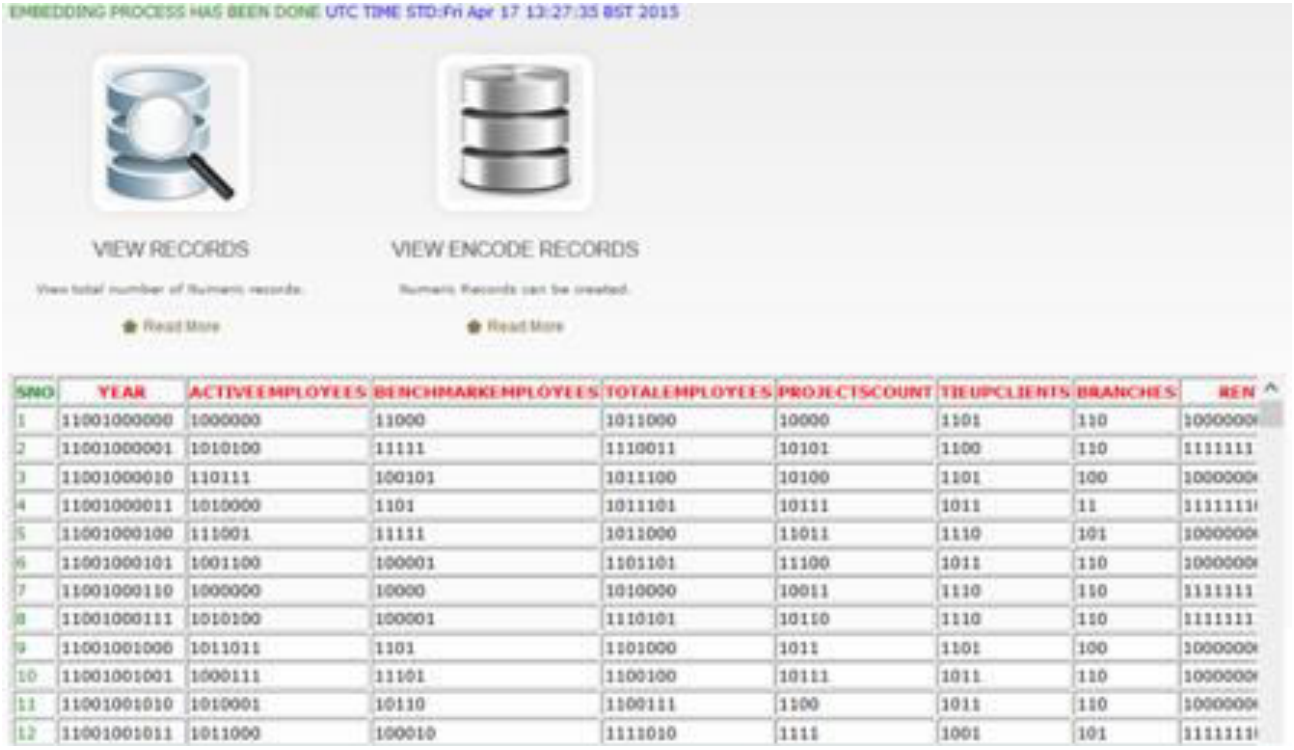
TUPLE REJECTION PRIMARY KEYS

FIRST PARTITION PRIMAYKEYS	SECOND PARTITION PRIMAYKEYS	THIRD PARTITION PRIMAYKEYS	FOURTH PARTITION PRIMAYKEYS
			12, 37, 51, 52, 53, 70, 97, 116, 130, 149, 178, 204, 231, 234, 264, 268, 279, 288, 328, 333, 347, 391

TUPLE SELECTION FOR WATERMARKING PRIMARY KEYS

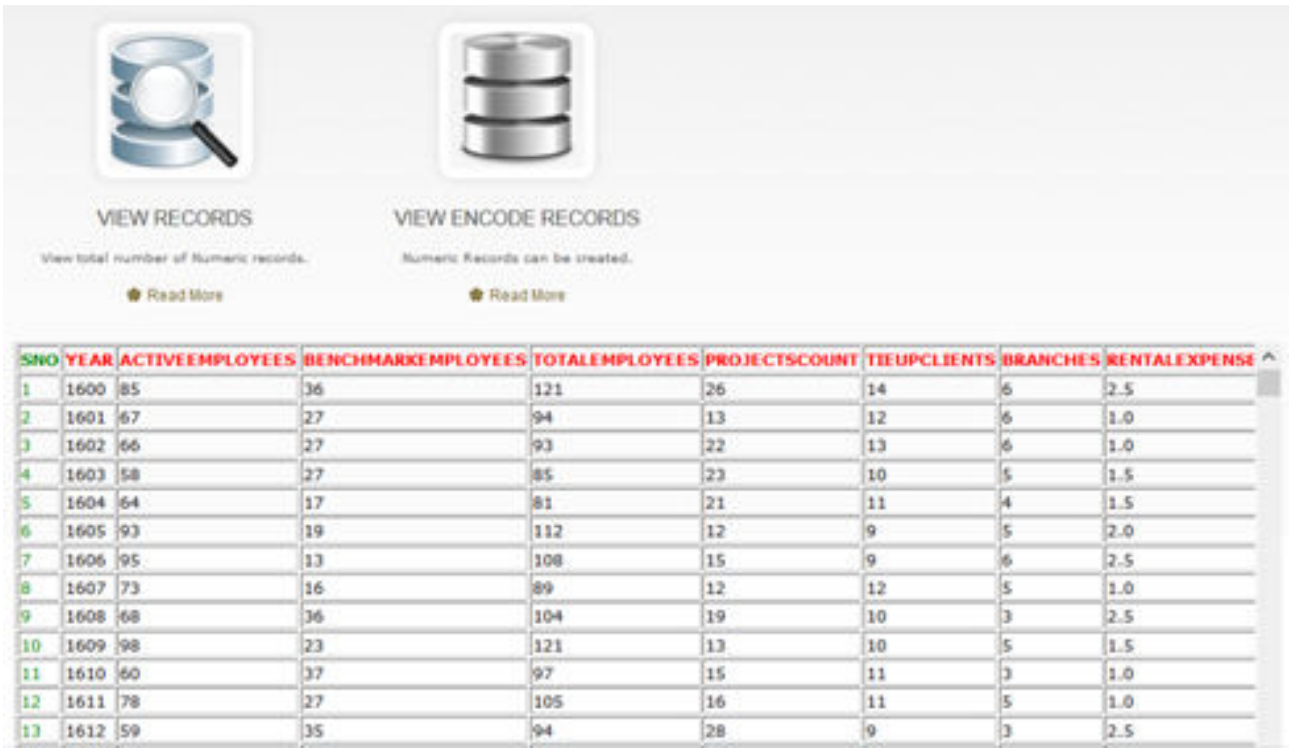
FIRST PARTITION PRIMAYKEYS	SECOND PARTITION PRIMAYKEYS	THIRD PARTITION PRIMAYKEYS	FOURTH PARTITION PRIMAYKEYS
21, 35, 38, 45, 60, 65, 68, 69, 85, 86, 105, 107, 112, 145, 153, 159, 166, 169, 171, 174, 180, 208, 212, 217, 224, 239, 244, 255, 259, 265, 273, 281, 282, 292, 300, 301, 314, 326, 327, 345, 350, 362, 366, 378, 385, 386, 392, 395	1, 6, 41, 57, 66, 78, 83, 84, 98, 110, 127, 129, 131, 132, 134, 148, 156, 173, 176, 195, 198, 203, 205, 220, 221, 225, 230, 236, 246, 252, 272, 303, 325, 336, 353, 369, 376, 393, 394, 398	7, 14, 22, 26, 29, 31, 42, 46, 73, 77, 88, 90, 94, 95, 101, 109, 113, 115, 125, 133, 135, 139, 141, 152, 167, 183, 184, 188, 207, 209, 211, 213, 222, 240, 243, 258, 260, 263, 270, 276, 287, 289, 294, 304, 305, 312, 316, 335, 342, 348, 352, 359, 363, 367, 373, 375, 396	13, 16, 23, 24, 30, 39, 40, 44, 54, 59, 61, 63, 71, 72, 76, 79, 82, 91, 104, 118, 136, 138, 182, 186, 190, 191, 214, 228, 233, 235, 278, 280, 286, 291, 295, 306, 307, 313, 332, 338, 346, 370, 381, 383, 384, 389, 397

Figure-3. Tuple selection.



SNO	YEAR	ACTIVEEMPLOYEES	BENCHMARKEMPLOYEES	TOTALEMPLOYEES	PROJECTSCOUNT	TIEUPCLIENTS	BRANCHES	REN
1	11001000000	1000000	11000	1011000	10000	1101	110	1000000
2	11001000001	1010100	11111	1110011	10101	1100	110	1111111
3	11001000010	110111	100101	1011100	10100	1101	100	1000000
4	11001000011	1010000	1101	1011101	10111	1011	11	1111111
5	11001000100	111001	11111	1011000	11011	1110	101	1000000
6	11001000101	1001100	100001	1101101	11100	1011	110	1000000
7	11001000110	1000000	10000	1010000	10011	1110	110	1111111
8	11001000111	1010100	100001	1110101	10110	1110	110	1111111
9	11001001000	1011011	1101	1101000	1011	1101	100	1000000
10	11001001001	1000111	11101	1100100	10111	1011	110	1000000
11	11001001010	1010001	10110	1100111	1100	1011	110	1000000
12	11001001011	1011000	100010	1111010	1111	1001	101	1111111

Figure-4. Watermark encoding.



SNO	YEAR	ACTIVEEMPLOYEES	BENCHMARKEMPLOYEES	TOTALEMPLOYEES	PROJECTSCOUNT	TIEUPCLIENTS	BRANCHES	RENTALEXPENSE
1	1600	85	36	121	26	14	6	2.5
2	1601	67	27	94	13	12	6	1.0
3	1602	66	27	93	22	13	6	1.0
4	1603	58	27	85	23	10	5	1.5
5	1604	64	17	81	21	11	4	1.5
6	1605	93	19	112	12	9	5	2.0
7	1606	95	13	108	15	9	6	2.5
8	1607	73	16	89	12	12	5	1.0
9	1608	68	36	104	19	10	3	2.5
10	1609	98	23	121	13	10	5	1.5
11	1610	60	37	97	15	11	3	1.0
12	1611	78	27	105	16	11	5	1.0
13	1612	59	35	94	28	9	3	2.5

Figure-5. Watermark decoding.

The watermark extraction process is given in the decoding phase. The watermarked content has to be extracted only by the legal user to give the proper ownership. If the user ownership content is matched by the admin generated content, decoding process has to do. Otherwise, it's not done which, is shown in Figure-5.

CONCLUSIONS

Thus, the proposed system is used to maintain maximum robustness for the relational data. Also, it is used to detect the watermark fully and recovers both the embedded watermark and the original data. The relational data is partitioned into logical values and selection of particular tuples for embedding in watermarked content is carried out. The selected tuples get transformed into the watermarked content during watermark embedding phase. Thusly, it gives a strong answer for information recuperation that is reversible and flexible against substantial assaults. The watermark producing capacity takes date-time stamp as a data and afterward creates watermark bits b1b2 . . . bn from this date-time stamp. Watermark bits are given as information to the watermark encoding capacity. The date-time stamp "may" likewise help to distinguish added substance assaults in which an assailant needs to re-watermark the information set. Edge detection Authenticator is proposed as an alternative solution to text based. It is mainly depends on images rather than alphanumerical. The main argument here is that the pass-images from the challenge set and then he/she will be authenticated users are better at recognizing and remembering pictures.

Watermark Extraction process in the Decoding phase. The Watermarked Content has to be extracted only by the legitimate user to give the proper ownership. If the User ownership content is matched by the Admin generated content, Decoding process has to do. Otherwise, it's not done.

REFERENCES

[1] Qin Z., Ying Y., Jia-jin L. and Yi-shu L. 2006. Watermark based copyright protection of outsourced database. Proceedings of the 10th International Database Engineering and Applications Symposium (IDEAS'06), IEEE Computer Society. 6: 301-308.

[2] P. W. Wong and N. Memon. 2001. Secret and public key image watermarking schemes for image authentication and ownership verification. Image Processing, IEEE Transactions on. 10(10): 1593-1601.

[3] Huang M., Cao J., Peng Z. and Fang Y. 2004. A new watermark mechanism for relational data. Proceedings of the 4th International Conference on Computer and Information Technology (CIT '04), IEEE. 84: 946-950.

[4] R. Sion, M. Atallah and S. Prabhakar. 2005. Rights protection for cat- egorical data, Knowledge and Data Engineering. IEEE Transactions on. 17(7): 912-926.

[5] Y. Zhang, B. Yang and X.-M. Niu. 2006. Reversible watermarking for relational database authentication. Journal of Computers, IEEE Computer Society. 17(2): 59-66.

[6] E. Sonnleitner. 2012. A robust watermarking approach for large databases. Satellite Telecommunications, IEEE First AESS European Conference. 21: 1-6.

[7] G. Gupta and J. Pieprzyk. 2008. Reversible and blind database watermarking using difference expansion, in Proceedings of the 1stinternational conference on Forensic applications and techniques in telecommunications, information, and multimedia and workshop, ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering). 8: 24-29.

[8] D. M. Thodi and J. J. Rodriguez. 2004. Prediction-error based reversible watermarking. In Image Processing, ICIP'04, International Conference on. IEEE. 3: 1549-1552.