PUBLISHING PATIENT DATA SET SECURELY THROUGH DIFFERENTIAL PRIVACY VIA WAVELET TRANSFORMS

Mr. P.M.GAVALI
Computer Science and Technology, Shivaji University,
Kolhapur, Maharashtra, India
gavalipm87@gmail.com

Prof. P.C.BHASKAR
Computer Science and Technology, Shivaji University,
Kolhapur, Maharashtra, India
pxbhaskar@yahoo.co.in

Abstract

Every organization stores a required data in the digital form. This data needs to be published due to the mutual benefits or due to the government rule. This data also has significant research value. While publishing a data in its original form, there is loss of privacy of the individual record. To avoid this, we can use ε -differential privacy. Dwork provides a simplest way to achieve this. But it does not work well with range count query. In this paper we have used Privelet+ method using array based implementation for wavelet transforms. This method shows better result than the Dwork method for the range count queries.

1. Introduction

Today every organization stores a required data in the digital form. For example, hospital stores data related with patients in digital form. This data needs to be published either due to mutual benefits or due to the government rule. For example, every licensed hospital in California is required to submit data related with the patient when patient gets discharge from the hospital [Carlisle, *et al.* (2007)]. This data includes sensitive information related with individual. If we publish this data in its original form, it violets the privacy of individual. Methods that deal with this problem are known as Privacy Preserving Data Publishing Techniques [Fung B.C.M, *et al.* (2010)]. These techniques publish data in such a way that published data remains practically useful while individual privacy is preserved. One of the methods for privacy preserving data publishing technique is ε -differential privacy [Dwork C., *et. al.* (2006)]. This method says, a randomized algorithm G satisfies ε-differential privacy, if 1) for any two tables T_1 and T_2 that differ only in one tuple, and 2) for any output O of G, we have $Pr\{G(T_1) =O\} \leq e^{\varepsilon} Pr\{G(T_2)= O\}$

Simplest method to achieve a ε-differential privacy is provided by Dwork [Dwork C., *et. al.* (2006)]. This method first computes the frequency distribution of the tuples in the input data and then publish a noisy version of the distribution by adding the noise of θ(1) variance to each entry. The noisy frequency matrix preserves privacy, as it conceals the exact data distribution. In addition, the matrix can provide approximate results for all range queries. But this method fails to provide useful results. In particular, for a count query answered by taking the sum of a constant fraction of the entries in the noisy frequency matrix, the approximate query result has a θ(m) noise variance, where m denotes the total number of entries in the matrix and m is typically an enormous number, as practical data sets often contain multiple attributes with large domains.

To deal with this problem we have implemented Privelet+ method [Xiaokui Xiao, *et al.* (2011)]. But while implementation we have used array based implementation for wavelet transforms rather than tree based implementation. This method provides more accurate range count query answers than the Dwork's method.

2. Problem Statement

Suppose we want to publish a table that T with $A_1,A_2,..,A_n$ domains. In this, we try to optimize the range count query of the form

SELECT COUNT (*) FROM T

WHERE $A_1 \in S_1$ AND $A_2 \in S_2$ AND,..,$A_n \in S_n$

$S_1,S_2..S_n$ are intervals defined on domain $A_1,A_2...A_n$

3. Proposed Structure

Privelet+ technique takes three inputs from the user. First input is table that we want to publish. Second is error magnitude that we want to add in published data and third is attribute list for further processing. This algorithm works in following different steps:

Step 1: Calculating frequency matrix

For the input table, we need to calculate the frequency matrix on one of the attribute. It computes the frequency distribution of the tuples in the input data. For example, suppose we want to publish following patient table having attributes as Patient Name, Patient Address, Patient Occupation, Patient Status and Patient Age. Patient Status specifies whether the person is suffering from diabetes or not.

Table 1 Medical Data

Patient Name	Patient Address	Patient Occupation	Patient Status	Patient Age
Yogesh A. Bhagwat	A/P Shiroli.	Farmer	Yes	41
Arnika P. Shetti	Ichalkaranji	Engineer	Yes	42
Dhiraj N. Kumar	Bihar	Doctor	No	43
Amol I. Magdum	Solapur	Teacher	No	41
Sandip D. Todakar	Kolhapur	Farmer	No	44
Ashvini A. Prasoon	Kolhapur	Doctor	No	43

The frequency matrix on Patient age for the above table can be given as,

Table 2 Frequency Matrix

Age	Yes	No
41	1	1
42	1	0
43	0	2
44	0	1

This can be calculated in java with following sudocode

```
ArrayList frequencyage=new ArrayList();
while (for each record){
    if(!frequencyage.contains(age)){
        frequencyage.add(age);
        // update fredata, Yfredata and Nfredata with count as one
    }
    if(frequencyage.contains(age)){
        //get the current count
        // increment count by one
        // update fredata, Yfredata or Nfredata
}
```

Step 2: Generating Submtrices

In this step, the frequency matrix is divided into the number of submatrix based on the user's input. Each submatrix must have the same number of coordinates calculated based on attribute list input.

For example given the frequency matrix in Table 2, if attribute list contains only the "Has Diabetes?" dimension, then the matrix would be split into two submatrices, one of which contains a column age and yes as attributes and other contains age and no.

Step 3: Calculate the wavelet coefficient

In this step, wavelets are calculated for each submatrix. For calculating wavelets, HAAR wavelet (HW) technique is used. These wavelets are generated by using an array. First all the elements of submatrix are placed into the array. Number of the elements must be equal to power of two. If this condition is not satisfied, we have to add dummy values. This array is copied into another array say copiedarray. The first wavelet coefficient is generated by taking the average of all the values known as base wavelet coefficient. The procedure to calculate remaining HAAR wavelet coefficients of an array of n samples is as follows

(1) Find the average of each pair of samples.(n/2)

(2) Find the difference between each average and the samples it was calculated form.(n/2)

(3) Fill the first half of the array with averages

(4) Fill the second half of the array with differences.

(5) Repeat the process on the first half of the array until n=1.

(6) Finally append the contents of copiedarray array to the newly created array.

Step 4: Calculating error and adding error in wavelet coefficient.

In this step we calculate the error for each wavelet coefficient based on its position in the array and then we add this calculated error in original wavelet coefficient to generate erroneous wavelet coefficients. Amount of error added in wavelet coefficient is given by (error magnitude)/ (weight of wavelet coefficient). Error magnitude is input taken from the user and the weight of wavelet coefficient can be calculated as follows.

For the base coefficient the weight is equal to the number of rows in the frequency matrix. For the other wavelet coefficient weight is 2^{l-i+1}, where l is log(size of the array+1)/ log(2) and i is the position of the node in the array. This position can be calculated for every element of array except contents of appended copiedarray by following sudocode.

```
int p=0;
int y=1;
for(every index)
        //calculate minvalue that is tow's power p minus one
        //calculate maxvalue that is tow's power q minus one
        if(minvalue<=index && maxvalue>=index){
                current_position=y;
                //calculate currentcost that is tow's power current_position
                if((currentcost-2)==index){
                        p=p+1;
                        y=y+1;
                }
        }
}
```

Step 5: Reconstruction of submatrices and assembling of submatrices

This step calculates the submatrices from the erroneous wavelet coefficients and assembles them in order to build the new frequency matrix. This new frequency matrix is nothing but the data to be published. For every index of non-changed appended part of the array, calculation is made in the following way to generate new values.

```
for every index of non-changed appended array
parent_index=index/2
while(parent_index > 0)
if(index%2==0){
        add the value at index to sum
        index=parent_index
        parent_index=parent_index/2
}
else{
        substract the value at index from sum
        index=parent_index
        parent_index=parent_index/2
}
add the sum to base coefficient
```

Due to the above code we will get the published data for single submatrix. This procedure is applied to every submatrix. Combine these submatrices to built final published table.

4. Experiments

We have implemented a system in java to publish patient database. For this system we have used a patient data set having attributes as Patient Name, Patient Address, Patient Status and Patient Age. This data set includes 3022 records. Out of 3022 records 1214 records have yes status and 1808 have no status. On this data set we apply Privelet+ method to calculate answer for the range count query. User enters the error magnitude and selects the attribute list. Then system calculates the published data. This system also measures the average absolute error, root mean squared error and maximum absolute error induced in the system.

The following graph shows the effect of error magnitude on various errors. From this graph we can conclude that as we increases the value of error magnitude there is linear growth in maximum absolute error, average absolute error and root mean squared error.

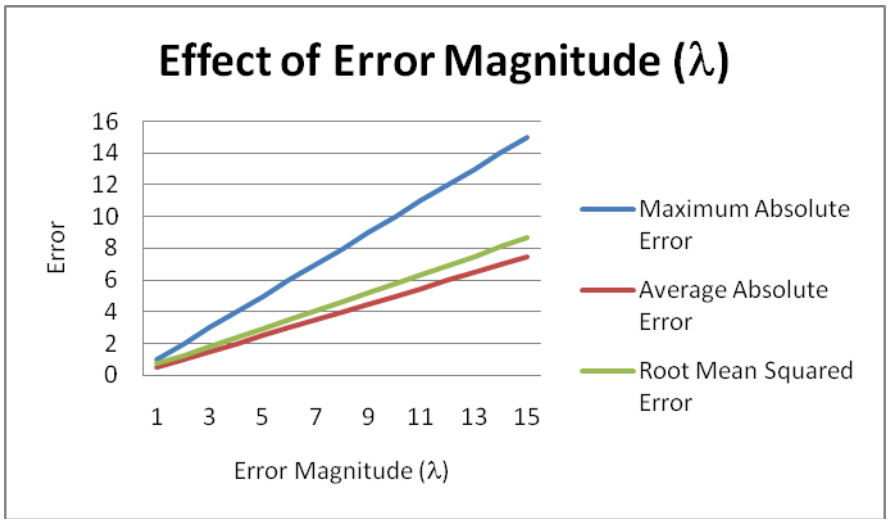

Figure 1 Effect of Error Magnitude

The following graph is ranges vs. range count query answer graph. From this graph we can conclude that the error added due to the privelet+ method is less than old method (Dwork's method) for each range count query answer.

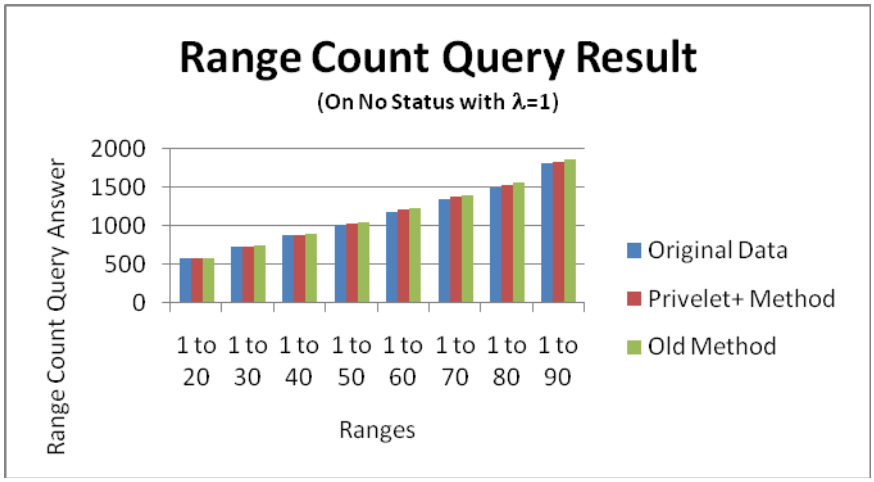

Figure 2 Range Count Query Result

5. Conclusion

Privelet+ method is data publishing technique. Privelet+ method provide improved results over a range count query applied. Experimental results provide the effectiveness of the Privelet+ method.

References

[1] Carlisle D. M., et. al. (2007): California inpatient data reporting manual, medical information reporting for California (5th Ed) Tech. rep., Office of Statewide Health Planning and Development.

[2] Dwork C., et. al. (2006): Calibrating Noise to Sensitivity in Private Data Analysis, Proc. Third Theory of Cryptography Conf. (TCC), pp. 265-284.

[3] Dwork Cynthia (2008): Differential Privacy: A Survey of Results, TAMC 2008, LNCS 4978, pp. 1–19,

[4] Fung B.C.M., et al, (2010): Privacy-Preserving Data Publishing: A Survey of Recent Developments, ACM Computing Surveys, vol. 42,no. 4, pp. 14:1-53
[5] Garofalkis M., Amit Kumar (2005): Wavelet Synopses for General Error Metrics, ACM Transactions on Database Systems, Vol. 30, No. 4, Pages 888–928.
[6] Karras P., Mamoulis N.(2008): Hierarchical Synopses with Optimal Error Guarantees, ACM Transactions on Database Systems, Vol. 33, No. 3, Article 18
[7] Machanavajjhala, Kifer, Gehrke and Venkitasubremaniam : l-diversity: Privacy beyond k-anonymity, ACM Trans. Knowl. Discov. Data 1,1.
[8] McSherry F. and Mironov I.(2009): Differentially private recommender systems: Building privacy into the netflix prize contenders., In KDD.
[9] Rastogi V. and Nath. S., (2010): Differentially private aggregation of distributed time-series with transformation and encryption, In SIGMOD.
[10] Samarati And Sweeney: Generalizing data to provide anonymity when disclosing information, In Proceeding of the 17th ACM SIGACT-SIGMOD-SIGRART, ACM New York, 188.
[11] Xiaokui Xiao, Guozhang Wang, and Johannes Gehrke(2011): Differential Privacy via Wavelet Transforms, IEEE Transactions on knowledge and data engineering, Vol. 23, No. 8.