Critical Relational Data Tuple Transmission Using Integer Wavelet Transform

Prof. S. A. Shinde[1], Mr. Kushal S. Patel[2]

Assistant Professor, VidyaPratishthan's College of Engg, Baramati, India[1]
P.G. Student, VidyaPratishthan'sCollege of Engg, Baramati, India[2]

Abstract- Remote database systems are becoming increasingly popular due to their potential usage in information storage. However, digital tuple data (e.g. bank balance, account details) are themselves vulnerable to security attacks. There are various methods are available to secure critical tuples. In this scheme we propose a new method in which data tuples are embedded in a container image.

In this technique, we are using wavelet transform for hiding data in digital images by combining the use of adaptive hiding capacity function that hides secret data in the integer wavelet coefficients of the cover image with the optimum pixel adjustment (OPA) algorithm. The OPA algorithm is applied after embedding secret relational tuples to minimize the embedding error. The proposed system showed high hiding rates with reasonable imperceptibility compared to other steganographic systems.

This container image is encrypted to have more security against the attack. At the client end the image is decrypted and converted into original format. From this image the data touples are extracted.

Index Terms- Amplitude modulation, RNG mechanism, Adaptive steganography, Integer wavelet transform.

I. Introduction

Now days with emerging technology in computer science, an increased security of the remote data tuples is necessary in order to reduce attacks on data. Techniques based on steganography can be suitable for transferring critical information from a server to a client and reduce the chances of illegal modification of the critical remote data.

In the remote database system, various types of data is stored and send to user according to his request for data. This request may demand some data which is very much important as such. This type of data may contain bank balance, credit card number, passwords, etc. It is very much risky to send this data in unencrypted form. In server side data is stored in encrypted form for security purpose but once the data is decrypted this security is lost. So, to provide extended security to the critical relational data tuples, we use the method of steganography. This proposed method helps to secure the tuples from the communication channel attacks at the time of transmission of result of requested query. Server sends result of requested query in the form of image container. This image container is opened rightly at client side only when client provides correct secrete key.

Steganography is the art and science which deals with security of data. In steganographic system, data is kept hidden in any multimedia object of secure transmission of it. Any digital file such as image, video, audio, text or IP packets can be used to hide secret message. Generally the file used to hide data is known as cover-object, and the file containing secret message is known as stego-object. Generally the image files are normally used for the hiding of data as they have high hiding capacity due to the redundancy of digital information representation of an image data and have higher degree of distortion tolerance than other types of files.

There are various types of data embedding techniques are available now a days. These techniques are generally classified by the type of cover image and type of data is used. Another method to classify the steganographic technique uses the method of transformations. There are number of transformations are available with mathematical methods. The classification may be done by the domain of embedding process.

In the transform domain techniques which appeared to overcome the robustness and imperceptibility problems found in the spatial domain substitution techniques. There are various transforms that can be used in data hiding, the most widely used transforms are; the discrete cosine transform (DCT), the discrete wavelet transform (DWT) and the discrete Fourier transform (DFT). In some technique the secret message is embedded into the high frequency coefficients of the wavelet transform while leaving the low frequency coefficients subband unaltered. While in another, an adaptive (varying) hiding capacity function is employed to determine how many bits of the secret message is to be embedded in each of the wavelet coefficients.

In spatial domain technique, the Least Significant Bit (LSB) substitution is used most of the times to hide the data. In LSB method, least significant bit of cover image pixel is directly replaced by secrete data. This technique is most preferred technique used for data hiding because it is simple to implement offers high hiding capacity, and provides a very easy way to control stego-image quality. This has low robustness to modifications made to the stego-image such as low pass filtering and compression and also low imperceptibility. These limitations are not there in transform domain. This technique has high ability to tolerate noises and some signal processing operations but on the other hand they are computationally complex and hence slower [9].

To minimize the computational error rate we use an adaptive data hiding technique joined with the optimum pixel adjustment algorithm to hide data into the integer wavelet coefficients of the base image. This will maximize the hiding capacity by great extent. To increase the system security we use a pseudorandom generator function to select the embedding locations of the integer wavelet coefficients.

There are various cryptographic techniques are available in the area of information security to encrypt the multimedia objects. This image container is encrypted to have more security. Some sophisticated algorithms provides much security of confidential data and used for image data. In general we use the blue channel in pixel to embed information. Blue channel is used because blue color has less sensitive to human eyes comparing with the red or the green ones, so better invisibility can be achieved. At the receiver end the image container is decrypted and tuples are extracted from it.

II. DATA SERIALIZATION AND BIT ADJUSTMENT

In relational database system, the data is stored in the form of tables and entities in the table. To retrieve this data user has to specify a query for request. This query result is in the form of table. For the embedding process this table data need to be serialized first. There are various algorithms for serialization is available. This results into xml like structure which is used as input for embedding process. At the receiver side schema are extracted from Image container and tables are extracted from this xml like schema.

No.	Cust Name	Value
1	Johm	54000
2	Kushal	52000
3	Kedar	69235
4	San	22589

The converted serialized form will be like this:

```
<xml>
<info1>
<No> 1 </No>
<Cust Name>Johm</Cust Name>
<Value> 54000 <Value>
</info1>
<info2>
<No> 2 </No>
<Cust Name>Kushal</Cust Name>
<Value> 52000 <Value>
</info1>
<info3>
<No> 3 </No>
<Cust Name>Kedar</Cust Name>
<Value> 69235<Value>
</info1>
<info4>
<No> 4 </No>
<Cust Name> San </Cust Name>
<Value> 22589<Value>
</info1>
</xml>
```

The main idea of using the optimum pixel adjustment(OPA) algorithm is to minimize the error difference between the original coefficient value and the altered value by checking the right next bit to the modified LSBs so that the resulted change will be minimal. This will result in very less distortion in base image. For example, if a binary number 1000 (decimal number 8) is changed to 1111 (decimal number 15) because its three LSB's were replaced with embedded data; the difference from the original number is 7. This difference in the original value is called the embedding error. By adjusting the fourth bit from a value of I to a value of 0, the binary number now becomes 0111 (decimal number 7) and the embedding error is reduced to I while at the same time preserving the value of the three embedded bits. It is observed that this OPA algorithm minimizes the error by half. In OPA algorithm we check the bit right next to the last changed LSBs. It is used to decrease the error resulted after insertion of message bits.

The algorithm is depend on calculating the difference δi between original value P(x, y) and the modified value P'(x, y)

δi*(x, y) = Pi'(x, y) - Pi(x, y)*

After calculating the δi, the algorithm modifies the changed value in the following manner:

```
Case 1 $(-2^k < \delta_i <-2^{k-1})$
        If $P_i'(x, y) < 256 – 2^k$
        Then $P_i'(x, y)^* = P_i'(x, y) + 2^k$
        Else $P_i'(x, y)^* = P_i'(x, y)$
Case 2 $(-2^{k-1} \leq \delta_i \leq 2^{k-1})$
        $P_i'(x, y)^* = P_i'(x, y)$
Case 3: $2^{k-1} < \delta_i < 2^k$
        If $P_i'(x, y) \geq 2^k$
        Then $P_i'(x, y)^* = P_i'(x, y) - 2^k$
        Else $P_i'(x, y)^* = P_i'(x, y)$
```

III. INTEGER WAVELET TRANSFORM

Integer wavelet transform maps an integer data set into another integer data set. In discrete wavelet transform, the used wavelet filters have floating point coefficients so this may cause the loss of data when any truncations of the floating point values are done. To avoid these problems instead of using floating point data we use the integer format and in this case there will be no loss of information through forward and inverse transform.

This is an adaptive data hiding scheme. In this which randomly selected integer wavelet coefficients of the base image are modified with critical relational tuple bits. Each of these selected coefficients hides different number of message bits according to the hiding capacity function. Once the data is inserted we apply optimum pixel adjustment algorithm to reduce the error induced due to data insertion.

A. Insertion Algorithm:

Data elements : Sequence[ ], I [ ][ ] : Image, I'[ ] [ ] : image, block[ ][ ][ ] , n : no of bits in input tuple data. s[ ] : bit stream, Co : absolute value of wavelet coefficients, k: min length used in each coefficient, k1: secrete Key, x,n,I,d : iterators.

```
Step 1:  I = ReadImage(BaseImage)

Step 2: for i=0 to no_of_pixels do
If  pixel[i]>255 || pixel[i]<0 then
Modify_pixel(pixel[i]);
          End if;
        End for;

Step 3:  divide_image_into_8x8_blocks.
Step 4: for i=1 to no_of_blocks do
IWT(block[i]);
        End for;

Step 5: //Calculate hiding capacity of each coefficient, we used a
modified version of the hiding capacity function. The
length of LSBs of wavelet coefficients (L) is determined
as:
```

$$L = \begin{cases} k+3, if Co \geq 2^{k+3} \\ k+2, if\, 2^{k+2} \leq Co < 2^{k+3} \\ k+1, if\, 2^{k+1} \leq Co < 2^{k+2} \\ k, if Co < 2^{k+1} \end{cases}, 0 \leq k \leq 4$$

*/**
*It is observed that as we lower the bits used to hide the secret message in the LL subband the resulted distortion in the stego-image becomes lower; so that we modified this hiding capacity function by using different ranges for k for the LH, HL and HH subbands where its values are form 1 to 4. For the LL subband the value of k is equal to 0 and in some cases the bits used is fixed to only bits to enhance the stego-image quality. */*

```
Step 6:  sequence=generateSeq(k1);
fori= 1 to n do
for j=0 to L do       // L bits of message
Embed(sequence[i], s[j]);
end for
end for

Step 7:  for i= 1 to n do
for j=0 to L do       // L bits of message
OPA(sequence[i]);
end for
end for

Step 8: end;
```

B. Extraction algorithm :

Data elements : Sequence[ ], I [ ][ ] : Image, I'[ ] [ ] : image, block[ ][ ][ ] , n : no of bits in input tuple data. s[ ] : bit stream, Co : absolute value of wavelet coefficients, k: min length used in each coefficient, k1: secrete Key, x,n,I,d : iterators.

```
Step 1:  I = ReadImage(BaseImage)

Step 2:  divide_image_into_8x8_blocks.

Step 3: for i=1 to no_of_blocks do
IIWT(block[i]); // Inverse IWT
        End for;

Step 4: //Calculate hiding capacity of each coefficient, we used a
modified version of the hiding capacity function. The
length of LSBs of wavelet coefficients (L) is determined
as:
```

$$L = \begin{cases} k+3, if Co \geq 2^{k+3} \\ k+2, if\, 2^{k+2} \leq Co < 2^{k+3} \\ k+1, if\, 2^{k+1} \leq Co < 2^{k+2} \\ k, if Co < 2^{k+1} \end{cases}, 0 \leq k \leq 4$$

```
Step 5:  sequence=generateSeq(k1);
fori= 1 to n do
for j=0 to L do       // L bits of message
s'[j]=  s'[j]+Extract(sequence[i]);
end for;
end for;

Step 6: convert_xml_to_relation(s');

Step 7: end;
```

IV. CONCLUSION

In this paper we proposed a novel method for transmitting the critical relational tuples at remote database systems. This scheme hides relational data tuples in an image by using integer wavelet transformation and the optimum pixel adjustment algorithm to increase the hiding capacity of the system compared to other systems. This method hides entities in tuples at random location in image. This uses the secrete key which is only known to both sender and receiver. This will increase the data invisibility and ability to detect the data from any unauthorized user in the communication channel. In this mechanism we used the hiding capacity function to improve the visual effects of base image. Any relational data type can be used as the secret message since our method was made on a binary stream of data. There was no error in the recovered message (perfect recovery) at any hiding rate.

REFERENCES

[1] G. J. Simmons, "The prisoners' prober and the subliminal channel," in Proceedings of Crypto' 83, pp. 51-67, 1984.

[2] N. Wu and M. Hwang. "Data Hiding: Current Status and Key Issues," International Journal of Network Security, Vol.4, No.1, pp. 1-9, Jan. 2007.

[3] W. Chen, "A Comparative Study of Information Hiding Schernes UsingAmplitude, Frequency and Phase Embedding," PhD Thesis, National Cheng Kung University, Tainan, Taiwan, May 2003.

[4] C. K. Chan and L. M. Cheng, "Hiding data in images by simple LSB substitution," Pattern Recognition, pp. 469-474, Mar. 2004.

[5] K. Changa, C. Changa, P. S. Huangb, and T. Tua, "A Novel bnage Steganographic Method Using Tri-way Pixel-Value Differencing," Journal of Multimedia, Vol. 3, No.2, June 2008.

[6] H. H. Zayed, "A High-Hiding Capacity Technique for Hiding Data in hnages Based on K-Bit LSB Substitution," The 30th International Conference on Artificial Intelligence Applications (ICAIA - 2005) Cairo, Feb. 2005.

[7] A. Westfeld, "F5a steganographic algorithm: High capacity despite better steganalysis," 4th International Workshop on Information Hiding, pp.289-302, April 25-27, 2001.

[8] B. Lai and L. Chang, "Adaptive Data Hiding for bnages Based on Harr Discrete Wavelet transform," Lecture Notes in Computer Science, Volume *4319/2006.*

[9] P. Chen, and H. Lin, "A DWT Approach for bnage Steganography," International Journal of Applied Science and Engineering 2006. 4, 3: 275:290.

[10] H. W. Tseng and C. C. Chnag, "High capacity data hiding in jpegcompressedimages," Informatica, vol. 15, no. I, pp. 127-142,2004.

[11] S. Lee, C.D. Yoo and T. Kalker, "Reversible image watermarking based on integer-to-integer wavelet transform," IEEE Transactions on Information Forensics and Security, Vol. 2, No.3, Sep. 2007, pp. 321- 330.

AUTHORS

First Author – Prof. S. A. Shinde**,** Assistant Professor, VidyaPratishthan's College of EnggBaramati, India.
Email id- meetsan_shinde@yahoo.com

Second Author – Mr. Kushal S. Patel, P.G. Student, VidyaPratishthan's College of Engg ,Baramati, Maharashtra, India.
Email id - patelkushal4444@gmail.com