International Journal of Engineering Research and General Science Volume 4, Issue 2, March- April, 2016
ISSN 2091-2730

DATA COMPRESSION AND EXPANSION USING DISCRETE WAVELET TRANSFORM IN ENCRYPTED DOMAIN

VITTHAL SHELKE[1] ,PROF. R.A.PATIL[2]

1 Student, (M Tech) Department of Electrical Engineering, VJTI, Mumbai.Shelkev247@gmail.com, 9011502844.
2 Associate Professor, Department of Electrical Engineering, VJTI, Mumbai

ABSTRACT

The signal processing after encryption that is in cryptosystem is relatively somewhat new topic.The data size to store available information require large memory, so here we are proposing a method called multilevel discrete wavelet transform(DWT) in encrypted domain. We are suggesting a frame work for carry out DWT and its inverse DWT in the encrypted domain. With this proposed framework we carry out multilevel DWT and inverse DWT in Homomorphic encrypted domain. Encryption is the process of encoding data .The purpose of encryption is to ensure data security. Homomorphic encryption is useful of encrypted information for data computation.

Keywords-Dataprocessing, Discrete wavelet transform(DWT), Inverse Discrete wavelet transform(IDWT), Encryption, Decomposition, DFT,FFT

INTRODUCTION

Data processing[1] in encrypted domain is somewhat new topic. This new technique gives two kinds of application uses in the future. The first kind of application is in the scenario of network media distribution. The customer may be asked to embed a water mark in the media to find out illegal copies. Since the plain media can be easily attacked during the process of watermarking, a solution for this is to embed the watermark in the encrypted media, whose content is protected by the cryptosystem. Signal processing the encrypted domain provide powerful and accurate tools to carry out implementation quiet possible. The second Application is to protect privacy. Consider a case of a remote access system based on biometric data, the users sensitive information related to authentication will be stored in server .If server is unsecure or misused then, user will face some serious problems. Processing in the encrypted domain along with Cryptographic protocols in the encrypted domain. Cryptographic protocols [2], [3], can give an effective solution to the server store the user information in encrypted form in Data base. The signal processing in encrypted domain plays important role .But not all cryptosystem [4],[5],[6],[7] like advanced encryption standard (AES) and data encryption standard (DES) Does not retain the symmetrical relation with the plain text. The Homomorphic Cryptosystem [8] keep the algebraic structure of plain text Homomorphic cryptosystem are of two type .one is partially Homomorphic cryptosystem and fully Homomorphic cryptosystem which give permission to carry out addition and multiplication.

The Homomorphic Cryptosystem[8] was first introduced by Rivest. There are two operations regarding to each other one in the cipher text domain and other in plain text domain.consider two plain text m1and m2.

Then

$$D\{E[m1] \circ E[m2]\} = m1 \lozenge m2 \quad (1)$$

where D{} is decryption and
E{} is encryption

RELATED WORK

There have been works on signal processing in encrypted domain. Bianchi [9][10] investigated on implementation of discrete Fourier transform(DFT) and fast Fourier transform(FFT) in encrypted domain but due to limitation in encrypted domain discrete wavelet transform is used. DWT is general scheme for signal processing.This paper contains the performing of DWT actually. DWT can extract different type of information from given data or called media. DWT can be used as for application like water marking [11],reducing memory space,feature extraction.

PROCEDURE

The important feature to choose wavelet transform is that it allows Multiresolution decomposition and here we are taking image into consideration so an image that is decomposed by using wavelet transform can be reconstructed completely.

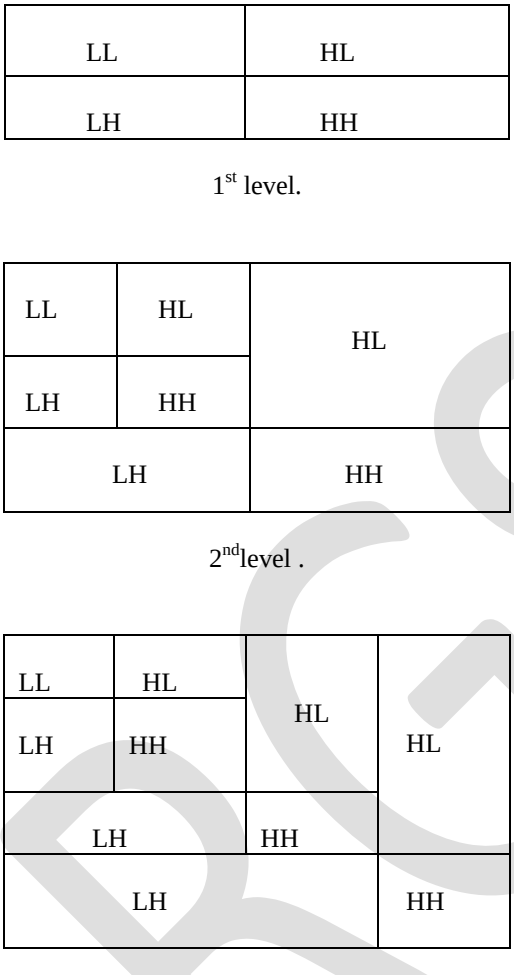

Figure 1: wavelet decomposition

The resulting decompositioncontain two-dimensional array Coefficients containing four sub levels. As LL (low low), HL (high low), LH (low high) and HH (high high). The LL level again can be decomposed in the same manner as in 1st level decomposition .like that we can produce any levels of decomposition.In this manner image is decomposed. Now here we are using discrete wavelet transform (DWT)

DISCRET WAVELET TRANSFORM

In Signal Processing the discrete wavelet transform based result better than DCT.The discrete wavelet transform (DWT) is a linear transformation that operates on adata vector whose length is an integer power of two, transforming it into a numerically different vector of the same length. It is a tool that separates data into different frequency components, DWT give temporal resolution that is it give frequency and location information.

According to Mallet algorithm [12] Discrete wavelet transform is defined as

DWT

$$a_j(k) = \frac{1}{\sqrt{2}} \sum_{l \in z} h_d(2k - l) a_{j-1}(l) \quad (2)$$

$$d_j(k) = \frac{1}{\sqrt{2}} \sum_{l \in z} g_d(2k - l) a_{j-1}(l) \quad (3)$$

where

J=1,2,3…..

$a_j(k)$is the approximation coefficient.

$d_j(k)$is detail coefficients.

and

$h_d(k)$= low pass decomposition filter coefficient.

$g_d(k)$ = high pass decomposition filter coefficient.

Both the plain text and cipher text are always represented by integers in encryption.
So for this all the data and parameters are represented with the help of integers.

Generally the filter coefficients are $h_d(k)$ and $g_d(k)$ are Real numbers. So in order to implement DWT in encrypted domain we have to consider integers instead of real numbers. The obtained integers instead of real numbers are obtained by quantization process as,

$$H(k) = \lfloor Q h_a(k) \rceil \quad (4)$$

$$G_d(k) = \lfloor Q g_d(k) \rceil \quad (5)$$

Where $\lfloor . \rceil$ is round of function.

According to discussion as we talked above we give the recursive definition of DWT

$$A_j(k) = \sum_{l \in z} H_d(2k-1) A_{j-1}(l) \quad (6)$$

$$D_j(k) = \sum_{l \in z} G_d(2k-1) A_{j-1}(l) \quad (7)$$

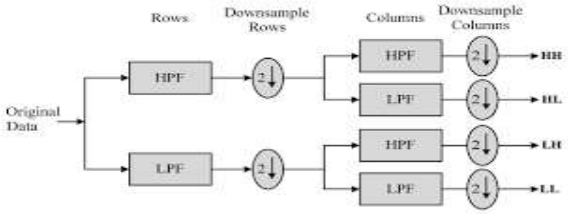

Figure 2: The block diagram of DWT:

In order to implement discrete wavelet transform DWT in encrypted domain we have to consider some issues,one of them is whether we are able to recover original Data from decryption. Other is to obtain plain wavelet coefficient.

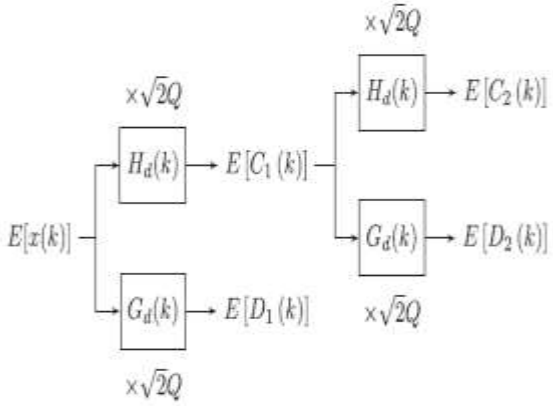

Figure 3: Block diagram of two levels DWT in encrypted domain

INVERSE DISCRETE WAVELET TRANSFORM

The mallet algorithm for[12] Inverse discrete wavelet transform(IDWT) is given as

$$a_j(k) = \frac{1}{\sqrt{2}} \sum_{l \in z} h_r(k-2l) a_{j+1}(l) + g_r(k-2l) d_{j+1}(l) \qquad (8)$$

where

$h_r$lowpass filter coefficients.

$g_r$high pass filter coefficients.

In encrypted domain to Implement Inverse discrete wavelet transform(IDWT) the filter coefficients 1st converted suitable form that is in integer form.

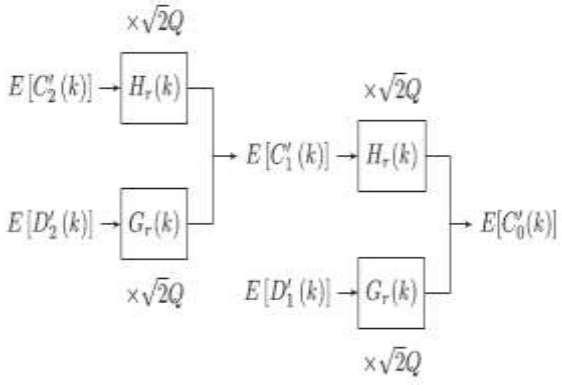

Figure 4: Block diagram two-level IDWT in the encrypted domain

METHODS FOR REDUCE DATA EXPANSION

While performing discrete wavelet transform and inverse discrete wavelet transform data is expanded due to expanding factor

A) Data expansion came into account due to absence of Normalization factor $\frac{1}{\sqrt{2}}$ in (6) and (7) and other is quantization process.So for that considers scale factor Q determine the precision of approximation of discrete wavelet transform and inverse discrete wavelet transform integers.

B) Rational filter coefficient:
Consider rational filter coefficients such as Haar wavelet. This can be expressed as two prime numbers which are relative as quotient.

Q mod L=0

This can be achieved by using Haar wavelet.

Multiplicative inverse method does not require not additional information about input. It is applicable to both cases, that is for discrete wavelet transform and inverse discrete wavelet transform.In Multiplicative inverse method the scaling factor Q is selected relatively prime. Multiplicative inverse method used to increase performance in application as data hiding, data compression and also feature extraction.

CONCLUSION

This paper shows the implementation of discrete wavelet transform DWT in the encrypted domain and problem of data expansion due to quantization process is tackled. And also proposed frame work to implement discrete wavelet transform and inverse discrete wavelet transform in Homomorphic cryptosystem. DWT and IDWT is implemented using rational filter coefficients.
Also multiplicative inverse method is discussed to improve capacity of signal processing.

REFERENCES:

[1] Z. Erkin, A. Piva, S. Katzenbeisser, R. Lagendijk, J. Shokrollahi, G. Neven, and M. Barni, "Protection and retrieval of encrypted multimedia content:Whencryptography meets signal processing," EURASIPJ. Inf. Security, vol. 2007, pp. 1–20, Jan. 2007.

[2] A. Yao, "Protocols for secure computations," in Proc. 23rd Annu. Symp. Foundations Computer Science, 1982, pp. 160–164.

[3] O. Goldreich, S. Micali, and A. Wigderson, "How to play ANY mental game," in Proc. 19thAnnu. ACM Conf. Theory Comput., 1987, pp. 218–229.

[4]T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," IEEE Trans. Inf. Theory, vol. 31, no. 4, pp. 469–472, Jul. 1985.

[5] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in Proc. Adv. Cryptology, 1999, pp. 223–238.

[6] I. Damgård and M. Jurik, "A generalisation, a simplification and some applications of Paillier's probabilistic public-key system," in Proc.Public-Key Cryptography, 2001, pp. 119–136.

[7] C. Gentry, "Fully homomorphic encryption using ideal lattices," in Proc. 41st Annu. ACM Symp. Theory Comput., 2009, pp. 169–178.

[8] R. Rivest, L. Adleman, and M. Dertouzos, "On data banks and privacy homomorphisms," in Foundations of Secure Computation. Cambridge, MA, USA: MIT Press, 1978, pp. 169–178

[9] T. Bianchi, A. Piva, and M. Barni, "On the implementation of the discrete Fourier transform in the encrypted domain," IEEE Trans. Inf.ForensicsSecurity, vol. 4, no. 1, pp. 86–97, Mar. 2009.

[10]M. Barni, P. Failla, R. Lazzeretti, A. Sadeghi, and T. Schneider,"Privacy-preserving ECG classification with branching programs andneural networks," IEEE Trans. Inf. Forensics Security, vol. 6, no. 2,pp. 452–468, Jun. 2011

[11] P. Zheng and J. Huang, "Walsh-Hadamard transform in the Homomorphic encrypted domain and its application in image watermarking," in Proc. 14th Inf. Hiding Conf., 2012, pp. 240–254.

[12] S. Mallat, "A theory for multiresolution signal decomposition: The wavelet representation," IEEETrans. Pattern Anal. Mach. Intell., vol. 11,no. 7, pp. 674–693, Jul. 1989