IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified

Vol. 5, Issue 7, July 2016

Multilevel Image Compression in Encrypted Domain

Vitthal Shelke[1], Prof. R.A. Patil[2]

M Tech, EXTC, Electrical Department, VJTI, Mumbai, India[1]

Associate Professor, Electrical Department, VJTI, Mumbai, India[2]

Abstract: Image compression is nothing but reducing the size of data required to represent an image. In the few recent years there is tremendous growth of data intensive and multimedia based applications, efficient image compression solutions are becoming critical. The main objective of Image Compression is to reduce redundancy of the data and improve the efficiency. The main techniques used are Fourier Analysis, Discrete Cosine Transform vector quantization method, sub-band coding method. The drawbacks in the above methods are, they cannot be used for real time systems. In order to overcome these problems, the Wavelet Transform method has been introduced. 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.

Keywords: Data Processing, Discrete Wavelet Transform (DWT), Inverse Discrete Wavelet Transform (IDWT), Encryption, Decomposition, DFT, FFT.

I. INTRODUCTION

In the last few years, there has been a lot of technological transformation in the way of communication. This transformation includes the satellite communication, digital TV, ever present, ever growing internet, the rapid development in mobile communication and ever increasing importance of video communication. Data Compression is one of the technologies for each of the aspect of this multimedia revolution. Memory carrying devices would not be able to provide communication with increasing clarity, without data compression. Data compression is one of the art and science of representing information in compact form. Uncompressed multimedia data requires considerable storage capacity and transmission bandwidth. Despite rapid progress in mass-storage density, processor speeds, and digital communication system performance, demand for data storage capacity and data-transmission bandwidth continues to outstrip the capabilities of available technologies. Image Compression is an important component of the solutions available for creating image file sizes of manageable and transmittable dimensions.

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

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

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

II. RELATED WORK

There have been works on signal processing but there is very few work done on signal processing in encrypted domain Bianchi [9][12] investigated on implementation of discrete Fourier transform (DFT) and fast Fourier transform(FFT) in encrypted domain but there are some limitation on DFT here in this paper 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 [10], reducing memory space, feature extraction.

III. PROCEDURE

The important feature to choose wavelet transform is that it allows Multiresolution decomposition that is both frequency as well as time resolution information which other techniques doesn't give. Here in this paper we are taking image as data into consideration so an image that is decomposed by using wavelet transform can be reconstructed completely.

1st level

LL	HL
LH	HH

2nd level

<table>
<tr><td>LL</td><td>HL</td><td rowspan="2">HL</td></tr>
<tr><td>LH</td><td>HH</td></tr>
<tr><td colspan="2">LH</td><td>HH</td></tr>
</table>

Fig 1: Decomposition of image

The resulting decomposition contain 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)

IV. DISCRET WAVELET TRANSFORM

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

According to Mallet algorithm [11] Discrete wavelet transform is defined as DWT
DWT

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

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

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 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 no are obtained by quantization process as

$$H_d(k)=Qh_d(k) \qquad (4)$$

$$G_d(k)=Qh_d(k) \qquad (5)$$

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

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

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

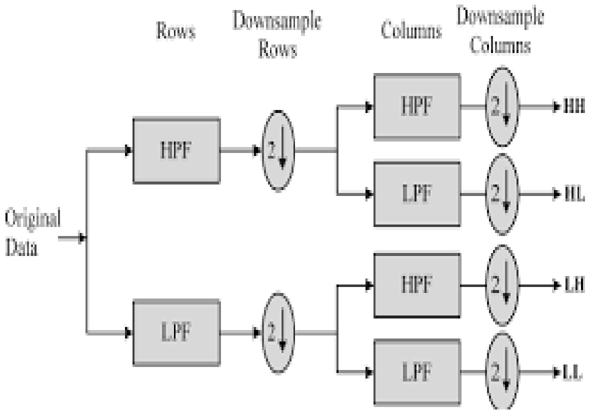

Fig 2: The block diagram of DWT

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.

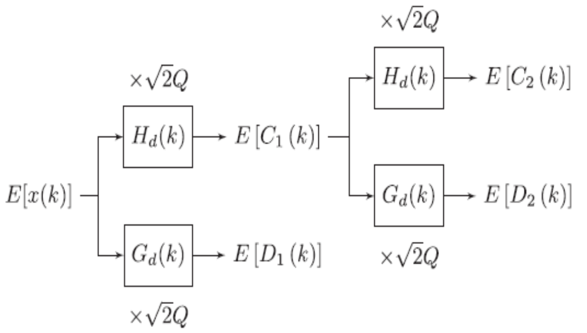

Fig 3 Block diagram of two levels DWT in encrypted domain

V. INVERSE DISCRETE WAVELET TRANSFORM

The mallet algorithm for[6] Inverse discrete wavelet transform(IDWT) is given as

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

where

h_r low pass 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.

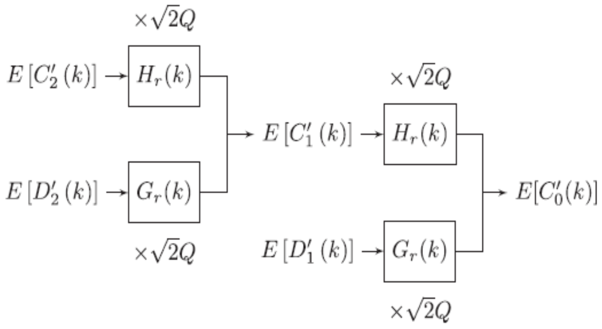

Fig4: Block diagram two-level IDWT in the encrypted domain.

Algorithms steps:

1. Take an image as input
2. Apply Encryption technique
3. Take integers of 2 step and perform DWT
4. Step 4 gives four sub level as 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
5. If want further Decomposition then go to step 3
6. Stop

VI. RESULTS

By using single level decomposition the result here got is

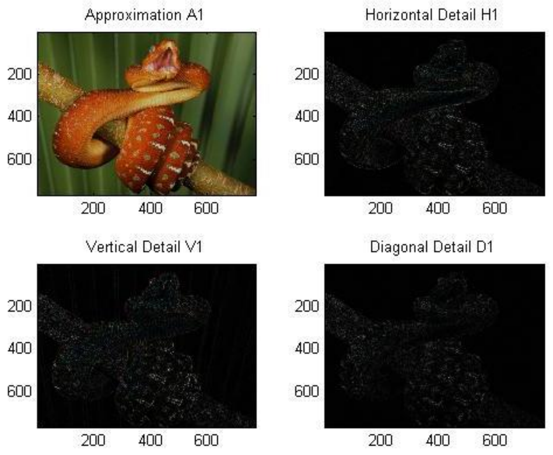

Fig4: 1st level decomposition

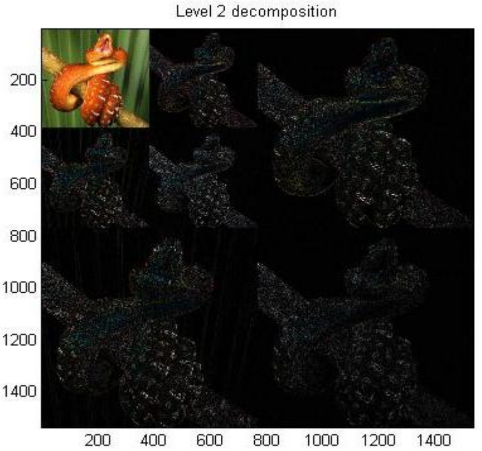

Fig5: 2nd level decomposition

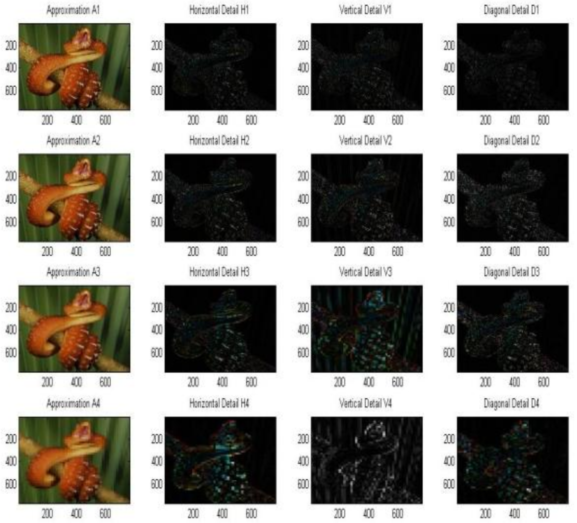

Fig6: 4th level decomposition

Like this for any no of decomposition can be carried out.

IDWT result:

The fig shown below is obtained from 4th level of decomposition by using inverse discrete wavelet transform.

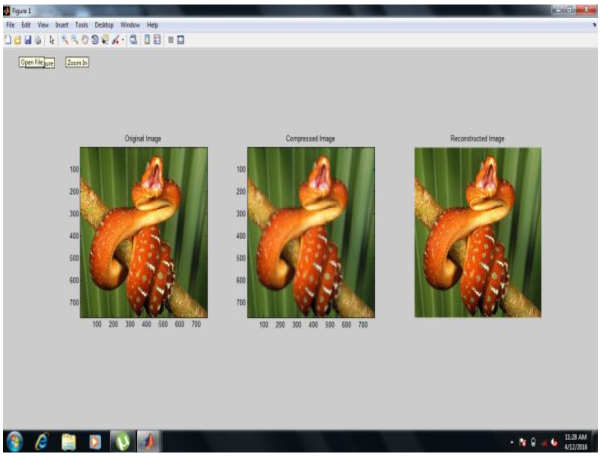

Fig7: IDWT

VII. CONCLUSION

This paper shows the implementation wavelet transform by using discrete wavelet transform DWT in the encrypted domain and problem of data expansion due to quantization process is tackled. And also proposed a frame work to implement multilevel 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 proposed to improve capacity of signal processing. Here the size of original image is reduced.

REFERENCES

[1] Z. Erkin, A. Piva, S. Katzenbeisser, R. Lagendijk, J. Shokrollahi, G. Neven, and M. Barni, “Protection and retrieval of encrypted multimedia content:When cryptography meets signal processing,” EURASIP J. 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. 19th Annu. 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. Forensics Security, vol. 4, no. 1, pp. 86–97, Mar. 2009.

[10] 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.

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

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