VLSI Design of Secured Cryptosystem

Geetha G
M.E VLSI Design,
Anna University of Technology
Madurai,
E-mail : ggeethu19@gmail.com

Muthukrishnan A
Assistant Professor of ECE,
Anna University of Technology
Madurai, Madurai.

Abstract - This project proposes Image cryptosystem scheme to achieve High speed and to improve the security level by using Discrete Wavelet Transform (DWT) and Chaos based approach in to the image. Internet now a day is one of the most popular modes of communications, and it suffers from a vital issue of not supporting the security of the confidential data during transmission. In this work, a high-speed cryptosystem for image data has been developed for efficient and secured communication over Internet. In order to build high quality image of JPEG 2000 codec, an effective 2-D FDWT algorithm has been performed on input image file to get the decomposed image coefficients. The Lifting Scheme reduces the number of operations execution steps to almost one-half of those needed with a conventional convolution approach. Initially, the lifting based 2-D FDWT algorithm has been developed using Matlab. The security of the proposed cryptosystem depends on the Discrete Wavelet Transform (DWT) and Chaos based approach.

Keywords: *Discrete Wavelet Transform(DWT), Chaos equation, BB equation, VLSI, Image encryption, Image decryption.*

I. INTRODUCTION

Images are very important documents now a day; to work with them in some applications they need to be compressed, more or less depending on the purpose of the application. There are some algorithms that perform this compression in different ways; some are lossless and keep the same information as the original image, some others loss information when compressing the image. Some of these compression methods are designed for specific kinds of images, so they will not be so good for other kinds of images. Some algorithms change parameters they use to adjust the compression better to the image. To compress the image Discrete Wavelet Transform (DWT) is used while compared to Discrete Cosine Transform (DCT).With low memory wavelet image compression is proposed in [1]-[3]. Data compression is a powerful, enabling technology that plays a vital role in the information age. Among the various types of data commonly transferred over networks, image and video data comprises the bulk of the bit traffic. For example, current estimates indicate that image data take up over 40% of the volume on the Internet. The explosive growth in demand for image and video data, coupled with delivery bottlenecks has kept compression technology at a premium. Among the several compression standards available, the JPEG image compression standard is in wide spread use today. JPEG uses the Discrete Cosine Transform (DCT) as the transform, applied to 8-by-8 blocks of image data. The newer standard JPEG2000 is based on the Wavelet Transform (WT) [4]-[7].Wavelet Transform offers multi-resolution image analysis, which appears to be well matched to the low level characteristic of human vision. The DCT is essentially unique but WT has many possible realizations. Wavelets provide us with a basis more suitable for representing images. This is because it can represent information at a variety of scales, with local contrast changes, as well as larger scale structures and thus is a better fit for image data.

II. DISCRETE WAVELET TRANSFORM

A discrete wavelet transform (DWT) is any wavelet transform for which the wavelets are discretely sampled. The DWT of images is a transform based on the tree structure with D-levels that can be implemented by using an appropriate bank of filters[8].

Although the discretized continuous wavelet transform enables the computation of the continuous wavelet transform by computers, it is not a true discrete transform. The wavelet series is simply a sampled version of the Cosine Wavelet Transform (CWT), and the information it provides is highly redundant as far as the reconstruction of the signal is concerned. This redundancy requires a significant amount of computation time and resources. The discrete wavelet transform (DWT), provides sufficient information both for analysis and synthesis of the original signal, with a significant reduction in the computation time. The DWT is considerably easier to implement when compared to the CWT.

A time-scale representation of a digital signal is obtained using digital filtering techniques. The CWT is a correlation between a wavelet at different scales and the signal with the scale (or the frequency). The CWT was computed by changing the scale of the analysis window, shifting the window in time, multiplying by the signal, and integrating over all times. In the discrete case, filters of different cutoff frequencies are used to analyze the signal at different scales. The signal is passed through a series of high pass filters to analyze the high frequencies, and it is passed through a series of low pass filters to analyze the low frequencies.

The resolution of the signal, which is a measure of the amount of detailInformation in the signal is changed by the filtering operations, and the scale ischanged by up sampling and down sampling (subsampling) operations.

Sub sampling a signal corresponds to reducing the sampling rate, or removing some of the samples of the signal. For example, subsampling by two refers to dropping every other sample of the signal. Subsampling by a factor *n* reduces the number of samples in the signal *n* times.

Up sampling a signal corresponds to increasing the sampling rate of a signal by adding new samples to the signal. For example, up sampling by two refers to adding a new sample, usually a zero or an interpolated value, between every two samples of the signal. Up sampling a signal by a factor of *n* increases the number of samples in the signal by a factor of *n*.

The Two-Dimensional DWT (2D-DWT) is a multi-level decomposition technique. It converts images from spatial domain to frequency domain. One-level of wavelet decomposition produces four filtered and sub-sampled images, referred to as sub bands. The sub band image decomposition using wavelet transform profits analysis for non-stationary image signal and has high compression rate.

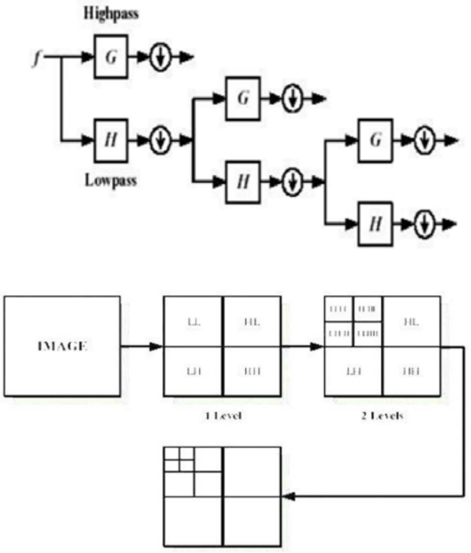

Figure 1: 2-D DWT for Image

The 2-D DWT for image is shown as fig 1.1 and it can be computed in cascade by filtering the rows and columns of images with 1-D filters. At the first level of decomposition, input image is decomposed into two sub bands(L, H) by filtering along the rows and L, H bands are decomposed again into four sub bands(LL, LH, HL, HH) by filtering along the columns. The multi-level decomposition is performed with LL band instead of input image. It decomposes DWT operations into finite sequences of simple filtering steps. In splitting step, input signals are split into even samples and odd samples. The prediction step computes high pass coefficients by predicting odd samples from even samples and calculates the difference between the odd samples and the prediction values. In update step, the low pass coefficients are computed from high pass coefficients.

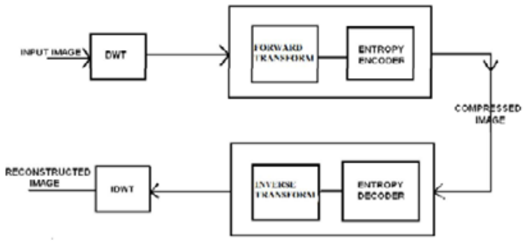

Figure 2: Block Diagram of Lifting Based DWT

The block diagram of Lifting based DWT [9] is shown as fig 1.2. The input image is given to DWT which consists of lifting scheme[10],[11] where the image is splitted into sequence of even and odd series coefficients. These splitted series are passed to compression block where the image is compressed using Forward transform**.** Compressed image is converted into bit streams using Entropy encoder. The reconstructed image is obtained by passing the compressed image through decompression block and IDWT.

III. DWT PROCESSOR

It consists of a DWT processor and a pair of external dual-port memories. The two memories are initialized with the pixel values of a gray scale image. The input is provided to the DWT processor by importing an image from the workspace in Matlab. The DWT processor includes DWT filter, memory controller and crossbars. The crossbars are used for interleaving the image pixels i.e. the output of the high pass and low pass filter will be distributed alternatively to the two memory banks.

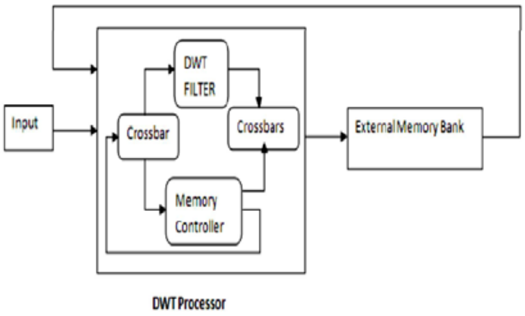

Figure 3: Block Diagram of DWT Processor

The DWT filter is designed using discrete wavelet transform. The Discrete Wavelet Transform can be implemented using high pass and low pass filters. Transformations are performed on each pixel using these filters and this is done as per line basis where lines are defined by start-of-line (sol) and end-of-line (eol). The high pass and low pass filters decompose the image into detail and approximate information respectively. The detail information is basically low scale, high frequency components of the image and it imparts nuance. Whereas the approximate information is high scale, low frequency components of the image and it impart the important part of the image.

In the high pass and low pass filter, the new inputs are accepted at one end before previously accepted inputs appear as outputs at the other end. This process is known as pipelining which helps to enhance the speed of the processor. The output of the H and L filters will be alternately distributed to the two memory banks.

A memory controller performs the read and writes operation simultaneously. It does not account for latency of getting data from memory or latency of the filter. The memory control signals are all derived from two free-running counters. The reset holds the counts at zero until a start pulse arrives. The bulk of control is determined on per phase basis from the master counter. The state register defines the number of phases. The address logic is derived by recombination of bits from the master counter for each phase. In fact, the read addresses are just the count value -- i.e. the memory read for this phase is just a stride 1 loop through the whole memory bank. The write addresses for this phase repeat each address twice.

The discrete wavelets transform (DWT), which transforms a discrete time signal to a discrete wavelet representation. The first step is to discretize the wavelet parameters, which reduce the previously continuous basis set of wavelets to a discrete and orthogonal / orthonormal set of basis wavelets.
The 1-D DWT is given as the inner product of the signal x (t) being transformed with each of the discrete basis functions.

The 1-D inverse DWT is given as:

$$x(t) = \sum_{m}\sum_{n} W_{m,n}\psi_{m,n}(t) \text{ ; m, n } \in Z$$

The generic form of 1-D DWT is depicted in fig 1.4. Here a discrete signal is passed through a low pass and high pass filters H and G, then down sampled by a factor of 2, constituting one level of transform. The inverse transform is obtained by up sampling by a factor of 2 and then using the reconstruction filters H*'* and G*',* whichin most instances are the filters Hand Greversed.

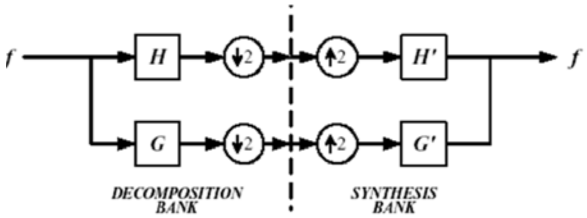

Figure 4: Perfect Reconstruction Filter Bank for Used for 1-D DWT

The 1-D DWT can be extended to 2-D transform using separable wavelet filters. With separable filters, applying a 1-D transform to all the rows of the input and then repeating on all of the columns can compute the 2-D transform. When one-level 2-D DWT is applied to an image, four transform coefficient sets are created. As depicted in Fig 1.5, the four sets are LL, HL, LH, and HH, where the first letter corresponds to applying either a low pass or high pass filter to the rows, and the second letter refers to the filter applied to the columns.

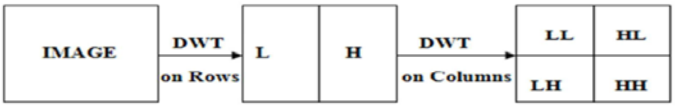

Figure 5: Level one 2-D DWT Applied on an Image

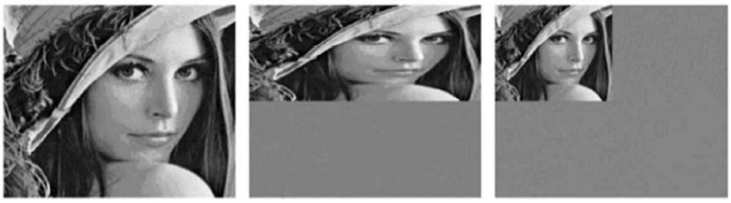

Figure 6: DWT for Lena image (a) Original Image (b) Output image after the 1-D Applied on Column Input (c) Output Image After the Second 1-D Applied on Row Input

The Two-Dimensional DWT (2D-DWT) converts images from spatial domain to frequency domain. At each level of the wavelet decomposition, each column of an image is first transformed using a 1D vertical analysis filter-bank. The same filter-bank is then applied horizontally to each row of the filtered and subsampled data. The DWT for Lena original Image is shown as fig 1.6(a).

One-level of wavelet decomposition produces four filtered and sub sampled images, referred to as sub bands. The upper and lower areas of Fig. 1.6(b),respectively, represent the low pass and high pass coefficients after vertical 1D-DWT and sub sampling. The result of the horizontal 1D-DWT and sub sampling to form a 2D-DWT output image is shown in Fig.1.6(c).

The straight forward convolution implementation of 1D-DWT requires a large amount of memory and large computation complexity. An alternative implementation of the 1D-DWT, known as the lifting scheme, provides significant reduction in the memory and the computation complexity. Lifting also allows in-place computation of the wavelet coefficients. Nevertheless, the lifting approach computes the same coefficients as the direct filter-bank convolution.

IV. SIMULATION RESULTS

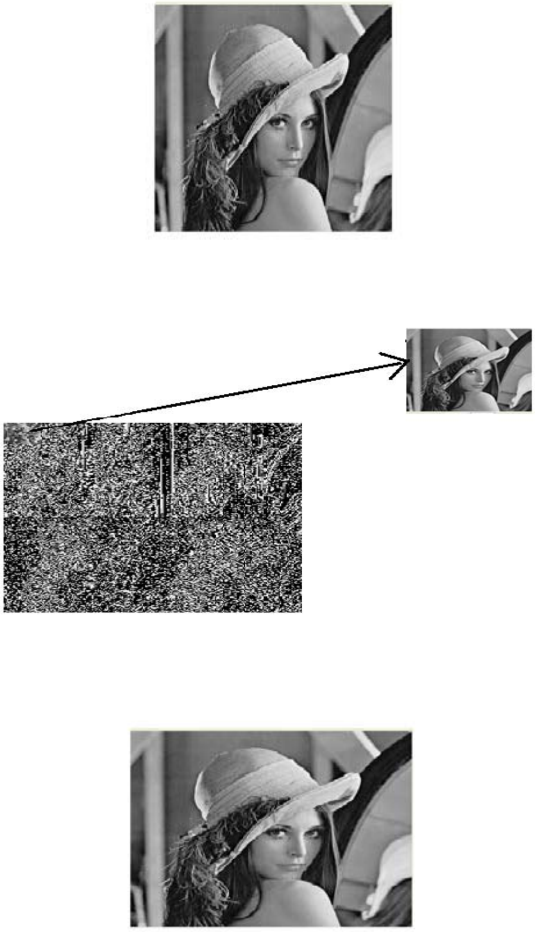

Figure 7: (a) Input Image (b) Compressed Image (c) Output Image

V. CONCLUSION

The Cryptosystem scheme for Image that depends upon Discrete Wavelet Transform is used to compress the image. This is done by implementing 2-D lifting based scheme in Discrete wavelet Transform for image. On comparing the Cosine Transform, Wavelet Transform results in better high speed and security level.

REFERENCES

1. Grangetto.M, Magli.E, Martina.M, and Olmo.G, (June 2002) “Optimization and Implementation of the Integer Wavelet Transform for Image Coding,” IEEE Trans. Image Processing, vol. 11, no. 6, pp. 596-604.
2. M. Antonini, M. Barlaud, P. Mathieu, and I. Daubechies, "Image Coding Using Wavelet Transform," IEEE Trans. on Image Processing, Vol.1, No.2, pp. 205-220, April 1992.
3. Chrysafis.C and Ortega.A, (Mar.2000) “Line-Based, Reduced Memory, Wavelet Image Compression,” IEEE Trans. Image Processing. vol. 9, no. 3, pp. 378-389.
4. Dillen et al.G, (Sept. 2003) “Combined Line-Based Architecture for the 5-3 and 9-7 Wavelet Transform of JPEG2000,” IEEE Trans. Circuits and Systems for Video Technology, vol. 13, no. 9, pp. 944-950.
5. Wu.P and Chen.L, (Apr. 2001) “An Efficient Architecture for Two-Dimensional Discrete Wavelet Transform,” IEEE Trans. Circuits and Systems for Video Technology, vol. 11, no. 4, pp. 536-545.
6. Christopoulos.C, Skodras.A, and Ebrahimi.T, (Nov. 2000) “The JPEG2000 Still Image Coding System: An Overview,” IEEE Trans. Consumer Electronics, vol. 46, no. 4, pp. 1103-1127.
7. B.-F.Wu and C.-F. Lin, “An efficient architecture for JPEG2000 coprocessor,” IEEE Trans. Consum. Electron., vol. 50, no. 4, pp. 1183– 1189, Nov. 2004.
8. "Wavelet filter evaluation for image compression". al., J. Liao et. August 1995, IEEE Trans. Image Process., Vol. 4, pp. 1053–1060.
9. XinTian, Lin Wu, Yi-Hua Tan, and Jin-Wen Tian, (August 2011) “Efficient Multi-Input/Multi-Output VLSI Architecture for Two-Dimensional Lifting-Based Discrete Wavelet Transform,” IEEE Transactions On Computers, Vol. 60, No. 8.
10. I. Daubechies and W. Sweldens, "Factoring Wavelet Transforms into Lifting Schemes," Journal of Fourier Analysis and Applications, Vol. 4, pp. 247-269, 1998.
11. Andra, K., Chakrabarti, C, Acharya,T.: A VLSI Architecture for Lifting-Based Forward and Inverse Wavelet Transform. IEEE Transactions On Signal Processing, vol. 50. No. 4. (2002) 966-977.
12. Acharya, T., Chen, P.: VLSI Implementation of DWT Architecture. Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS). Monterey, CA. (1998).
13. Acharya, T.: Architecture for Computing a Two-Dimensional Discrete Wavelet Transform. US Patent 6178269. (2001).
14. W. Philips, “The lossless DCT for combined lossy/lossless image coding,” in Proc. ICIP 1998.
15. Integer Cosine Transform for Image Compression, TMO Progr. Rep.TDA PR 42-105, May 15, 1991.