International journal of basic and applied research
www.pragatipublication.com
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

Implementing Sparse Encryption for Real-Time Multimedia Systems Using Discrete Wavelet Transforms

Mr. B. Sudhir, Mr. J. Kiran Chandrasekhar, Mrs. B. Vijaya
Associate Professor[1,2], Assistant Professor

Department of Electronics & Communication Engineering,

Rajamahendri Institute of Engineering & Technology, Rajamahendravaram.

***Abstract*—** In wavelet transforms, discrete sampling of the wavelets is known as a discrete wavelet transform (DWT). Its ability to capture both frequency and position information gives it a significant advantage over Fourier transforms in terms of temporal resolution, as is true with other wavelet transforms. In order to meet the needs of the end user, the DWT filter offers a high compression ratio together with high-quality picture reconstruction. Low power consumption, high system throughput, and cheap hardware cost are further desirable attributes. For embedded multimedia systems operating in real time, the intended DWT presents an authentication and encryption method with zero overhead. To include a free parameter into the design, the Discrete Wavelet Transform (DWT) compression block is used in its parameterized formation.

Keywords— The discrete wavelet transform, multimedia encryption, and parameterization!

I. INTRODUCTION (*Heading 1*)

Several next-generation multimedia compression and transmission standards use the Discrete Wavelet Transform (DWT), which has facilitated research in image and video coding. A more effective implementation of the DWT has been developed in response to its growing significance in image and multimedia compression applications. You can see some of the limitations of the DWT filter's design in Figure 1. If it wants to meet the needs of its users, it has to have a good compression ratio and be able to rebuild images accurately. Low power consumption, high system throughput, and cheap hardware cost are further desirable attributes. When it comes to real-time multimedia systems, the suggested DWT design is perfect for those demanding top-notch security.

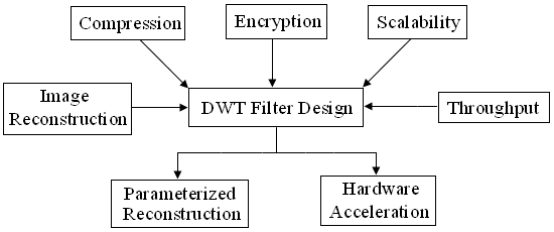

Fig. 1. DWT Filter Design Constraints

With its redesigned DWT filter, we can achieve great compression, flawless picture reconstruction, and compliance with security requirements.

Large amounts of computing power are needed by the currently used common encryption methods like AES and RSA. There is a very big delay for AES real-time applications since hardware implementations of AES are generally pipelined. Computationally intensive operations include video compression and data encryption. Figure 2(a) shows a plan that limits a DWT's bespoke hardware design to one with minimal hardware utilization and power consumption. A setup like this also makes it hard to efficiently send out video feeds that may grow in size. To get around these limitations, we need a system that can combine compression and encryption into a single operation without introducing heavy computing burdens. Figure 2(b) illustrates this idea. The compression engine incorporates a lightweight encryption block.

International journal of basic and applied research
www.pragatipublication.com
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

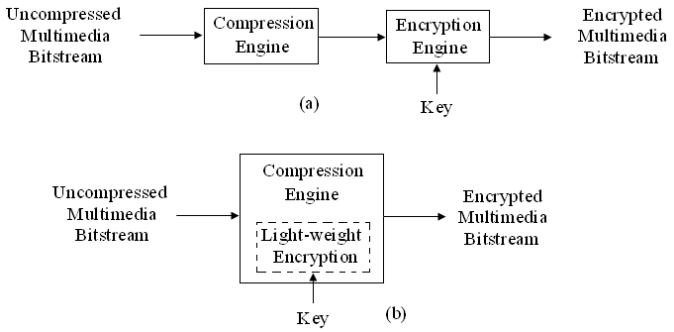

Fig. 2. (a) Traditional scheme for multimedia encryption and (b) Lightweight multimedia encryption scheme

Explaining the concept with a small example shown in fig. 3. A surveillance aircraft (A) is sending aerial surveys and other important information to the ground troops (B), crucial for their attack on the enemy base (C). In this scenario, typical encoding schemes would require large computational resources and hence high power consumption making them unsuitable for real-world embedded systems.

Some of the crucial security issues involved in this case are as follows:

The message (image) sent by A must not be easily perceptible to B.

B must be able to authenticate the incoming message (from A) to avoid impersonation from C.

The lightweight encryption scheme can provide a reasonable degree of security with little or no overhead in power or other requirements.

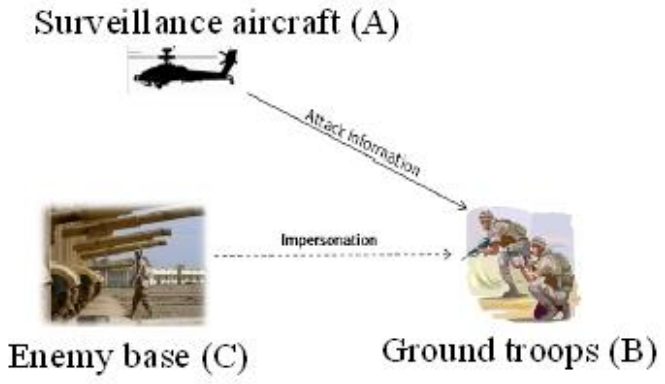

Fig. 3. An example scenario for proposed lightweight multimedia encryption scheme

In this paper we present a new parameterized construction DWT filter with rational coefficients. The parameterized construction can be used to build a key scheme while the rational coefficients of the DWT enable an efficient hardware architecture using fixed point arithmetic. The DWT, an essential part of modern multimedia compression algorithms, thus serves as a compression-cum-encryption block. The main contributions of this work can be summarized as follows:

We introduce the concept of the parameterized DWT architecture for multimedia encryption.

The new DWT architecture implements DWT as an encryption operation.

We optimize and pipeline the hardware architecture to achieve a high clock frequency of 242 MHz with minimum hardware requirements.

We provide some experimental results of image encryption and watermarking using the parameterized DWT operation.

International journal of basic and applied research
www.pragatipublication.com
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

The rest of the paper is organized as follows:

Section II gives a brief introduction to the DWT. Section III provides the parameterized construction of the DWT to yield a free parameter A in DWT operation. The rational coefficients in the parameterized DWT allow us to build an efficient hardware architecture which is explained in section IV.

II. BRIEF INTRODUCTION OF DWT

Prior works in signal processing establish that the 1-D DWT can be viewed as a signal decomposition using specific low pass and high pass filters. A single stage of image decomposition can be implemented by successive horizontal row and vertical column wavelet transforms. Thus, one level of DWT operation is represented by filtering with high and low pass filters across row and column successively. After each filtering down sampling is done by a factor of 2 to remove the redundant information.

The two most common DWT filters used in image compression are the Le Gail's 5/3 filter and Daubechies' 9/7 filter [5], accepted in the JPEG2000 standard. The Le Gall's filter has rational coefficients and its hardware implementation requires less resources. The Daubechies' 9/7 filter has better compression performance; however, it has irrational coefficients and leads to lossy compression.

III. PARAMETERIZED DWT DERIVATION

In this part, we will go over the 9/7 DWT filter's rational coefficient parameterized construction, which will be the new DWT architecture's backbone. The accuracy of Daubechies' 9/7 filter's implementation of fixed point hardware is limited by its irrational coefficients. Image compression makes use of bi-orthogonal wavelet filter banks due to their superior compression capabilities. Perfect Reconstruction (PR) is a requirement that they must meet. In wavelet-based picture compression standards, the Daubechies 9/7 filter is used because of its excellent compression properties. Compression quality is directly proportional to the PSNR ratio; a high PSNR ratio (as shown in Figure 4) indicates a parameter value of 2.Let H1(z) and H2(z) denote the analysis and synthesis low pass filter coefficients. On introducing a free parameter A in the equations for H1(z), the corresponding value of H2(z) is obtained by solving for conditions for linear phase, PR and low pass filter.

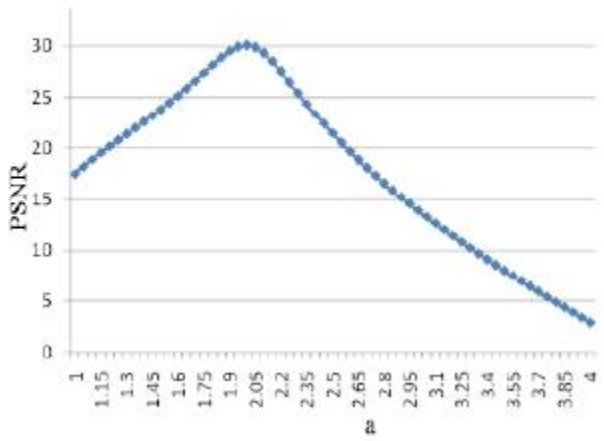

Fig. 4. Variation in PSNR with parameter a

The rational terms in the expressions for these filters can be implemented in hardware using shifts and adds instead of multiplication operations. This is a big savings over the original Daubechies filter in terms of hardware requirements. However, we

International journal of basic and applied research
www.pragatipublication.com
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

need to perform multiplication with the free parameter a and its exponents. This filter is implemented in our DWT architecture and is explained below.

IV. DWT ARCHITECTURE

Figure 5 gives the overview of our parameterized DWT building design. Data input (one pixel per cycle) x represents further calculations. Figure 5 shows that the number of variables is reduced from nine to five by passing eight of the inputs through four adders. A, a*2, and a/1 are multiplied by the values labeled w0, w1, w2, w3, and w4 to provide the intermediate values that are fed to the shift and add logic. The operations of adding and shifting are used in this block to create multiplication and addition using rational fractions. The DWT filter's final output consists of the coefficients for the high pass and low pass filters. We optimized the underlying hardware in many levels to lower its cost. Here is a brief overview of them:

Mathematical shift procedures were used to divide by binary coefficients. As a result, the circuits will no longer need multipliers. Since the coefficients for the low pass and high pass filters are identical, they may be combined to simplify the circuitry. Coefficients w0, w1, w2, w3, and w4 are labeled in figure 5. Significant hardware reductions are achieved by this optimization. Streams of input were piped together. Figure 5 shows that our design accepts a single pixel (or channel input) and, with a limited delay, produces the low pass and high pass signal coefficients. We may increase the clock speed (and by extension, the throughput) by increasing the system latency.

Despite offering security and competitive compression efficiency, the lightweight encryption scheme's primary benefit is the very little computational cost it incurs.

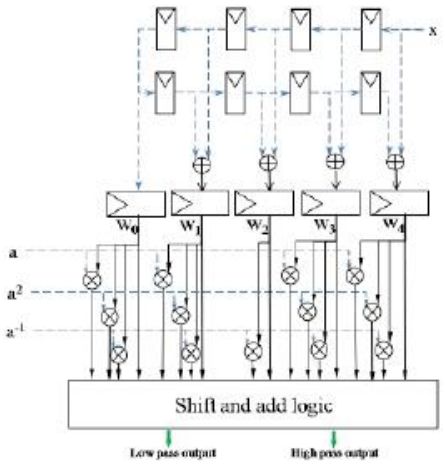

Fig. 5. Overview of Discrete Wavelet Transform architecture

V. EXPERIMENTAL RESULTS

Implementation of DWT is done on Xilinx FPGA, using Xilinx ISE 9.1 for simulation and synthesis purpose. A fixed point implementation of the DWT leads to image reconstruction error and gives no security promise. Our new architecture inputs an eight bit block every cycle which obtained the sufficient clock frequency due to its long critical path and also the hardware requirements are low.

The experimental results are shown in fig. 6 which are simulated in ISE 9.1.

International journal of basic and applied research
www.pragatipublication.com
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

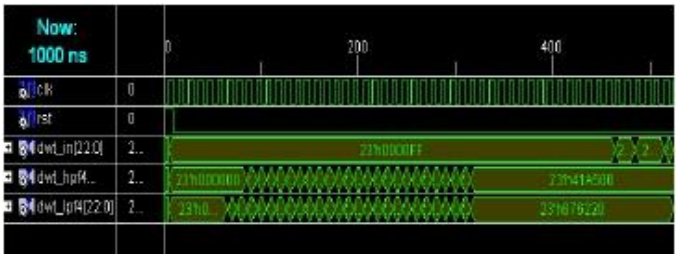

Fig. 6. Simulation Results

VI. CONCLUSION

A parameterized architecture of DWT based multimedia encryption is introduced in this work. A high-throughput, efficient implementation is made possible by the parameterization..

REFERENCES

[1] "Polymorphic Wavelet architecture over reconfigurable hardware," in 2008's IEEE International Conference on Field Programmable Logic and Applications, edited by A. Pnade and J. Zambreno, pages 471-474.

[2] In a 2007 article published in the ACM Computer Survey, D. Zheng, Y. Liu, J. Zhao, and A.E. Saddik reviewed RST invariant picture watermarking techniques.

An analysis of several designs for discrete and continuous wavelet transforms was conducted by Chakrabarti, Vishwanath, and Owens [3].