Implementation of Lightweight Encryption for Real Time Multimedia System using Discrete Wavelet Transforms

Baji Babu Shaik[1], Ratna Babu. Y[2]
Department of Electronic Communication Engineering
Vignan's Lara Institute of Technology and Science
Vadlamudi, India

Abstract— ***A discrete wavelet transform (DWT) is any wavelet transform for which the wavelets are discretely sampled. As with other wavelet transforms, a key advantage it has over Fourier transforms is temporal resolution as it captures both frequency and location information. DWT filter provides a high compression ratio and image reconstruction quality so as to serve the end user requirements. Some other desired features include low hardware cost, low power requirements and high throughput of the system. The purposed DWT introduces a zero-overhead encryption and authentication scheme for real time embedded multimedia systems. The parameterized construction of the Discrete Wavelet Transform (DWT) compression block is used to introduce a free parameter in the design***

Keywords— Parameterization, Discrete Wavelet Transform, Multimedia encryption.

I. INTRODUCTION (*Heading 1*)

The Discrete Wavelet Transform (DWT) has enabled research in image and video coding and has become a part of multiple next generation multimedia compression and transmission standards. The increasing importance of the DWT in image and multimedia compression applications has inspired the development of efficient hardware for implementations. Figure 1 shows some constraints in the design of DWT filter. It must provide a high compression ratio and image reconstruction quality so as to serve the end user requirements. Some other desired features include low hardware cost, low power requirements and high throughput of the system. The proposed DWT architecture is suited for high end security demands for real-time multimedia systems.

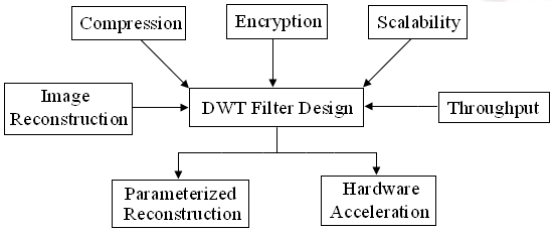

Fig. 1. DWT Filter Design Constraints

The re-design of the DWT filter can meet the security demands in addition to provide the perfect image reconstruction and high compression.

The existing popular encryption algorithms such as AES and RSA have large computational requirements. Hardware implementations of AES are often pipelined, leading to a significantly large latency for real-time applications for AES. Video compression and data encryption are both computationally expensive tasks. The scheme presented in Fig. 2(a) restricts a custom hardware design for the DWT that requires low power consumption and hardware usage. Such a design also limits an efficient delivery of scalable video streams. These restrictions can be alleviated by developing a scheme that integrates both encryption and compression operations into one without any significant computational overheads. This concept is presented in Fig. 2(b). A light weight encryption block is built into the compression engine.

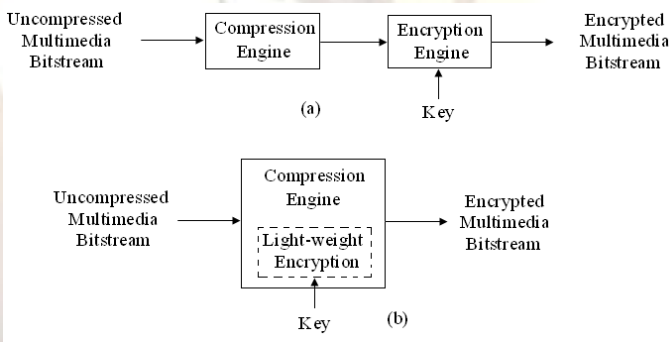

Fig. 2. (a) Traditional scheme for multimedia encryption and (b) Lightweight multimedia encryption scheme

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.

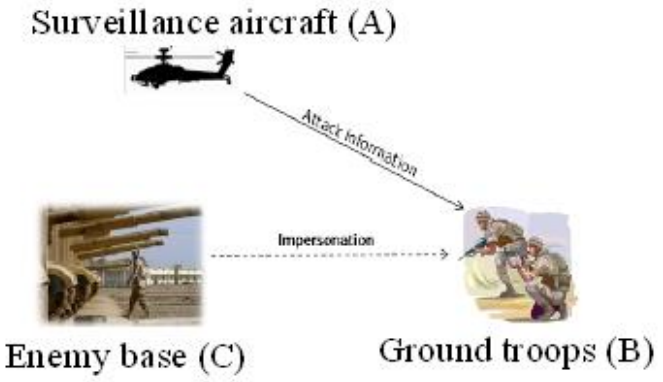

Fig. 3. An example scenario for proposed lightweight multimedia encryption scheme

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.

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

This section discusses the rational coefficient parameterized construction of the 9/7 DWT filter to serve as the backbone for the new DWT architecture. The irrational coefficients in Daubechies' 9/7 filter limit its precision of implementation of fixed point hardware. The Bi-orthogonal wavelet filter banks are used in image compression because of their excellent image compression properties. They must satisfy Perfect Reconstruction (PR) condition. The Daubechies 9/7 filter has good compression property and is being used in wavelet-based image compression standards. If the PSNR ratio is high then the compression quality is more, in fig. 4 shows the PSNR ratio is more at a value 2 so we see the parameter as 2 for compression.

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.

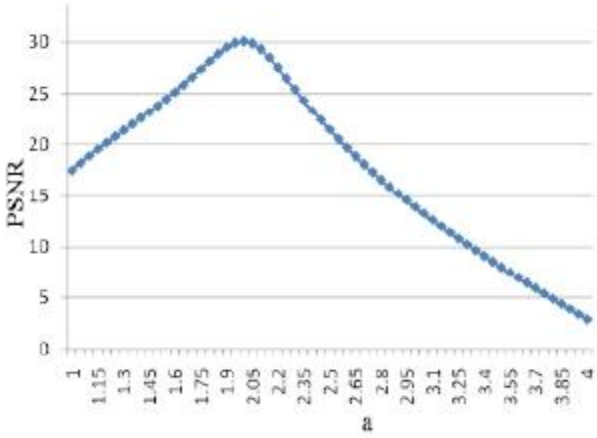

Fig. 4. Variation in PSNR with parameter a

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 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 architecture. The input data (one pixel input per cycle) x is further computations. In fig. 5, eight of the nine inputs are passed through four adders to reduce the number of variables to five. These values (labled w0, w1, w2, w3 and w4) are multiplied with a and a*2 and a/1 to get the necessary intermediate values which are input to the shift and add logic. In this block, we perform shifts and add operations to implement additions and multiplications with rational fractions. The high and low pass filter coefficients are the final output of the DWT filter. We performed several optimization steps to reduce the cost of the underlying hardware. They are summarized below:

Division by binary coefficients was performed using arithmetic shift operations. This eliminates the need for multipliers in the circuits. The low and high pass filter coefficients are same so they can be grouped together to reduce the hardware complexity. These coefficients are labled as w0, w1, w2, w3 and w4 in fig.5. This optimization gives a tremendous savings in hardware. The input stream was pipelined. As shown in fig.5 our architecture takes one pixel (or channel input) as the input and outputs the low and high pass signal coefficients with a finite latency. Increasing the system latency allows us to achieve a higher clock speed (and hence higher throughput).

The main advantage of the lightweight encryption scheme is that, while maintaining competitive compression performance and providing security, it comes at extremely low computational overhead.

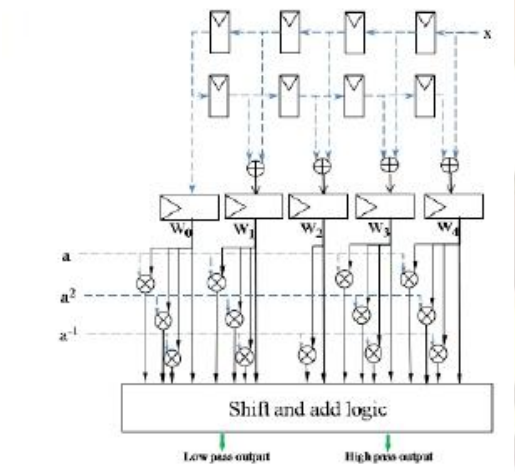

Fig. 5. Overview of Discrete Wavelet Transform architecture

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.

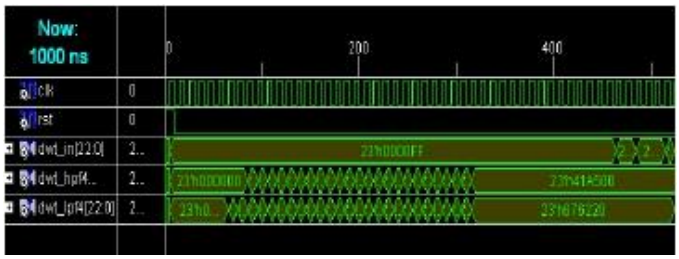

Fig. 6. Simulation Results

VI. CONCLUSION

This paper introduces a multimedia encryption based on parameterized construction of DWT. The parameterization enables an efficient, high throughput implementation.

REFERENCES

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

[2] D. Zheng, Y. Liu, J. Zhao and A.E. Saddik, "A Survey of RST invariant image watermarking algorithms", ACM Computer survey, Vol. 39, No. 2, p.5, 2007.

[3] C. Chakrabarti, M. Vishwanath and R.M. Owens, "A Survey of Architectures for the Discrete and Continuous Wavelet Transforms".