Scan to know paper details and author's profile

# Implementation of an Efficient Hardware Architecture for Multimedia Encryption and Authentication using the Discrete Wavelet Transform

*Dhanalxmi Banavath, Srinivasulu Tadisetty*

*Kaktiya University*

## ABSTRACT

This paper 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. It allows building a key space for lightweight multimedia encryption. The parameterization yields rational coefficients leading to an efficient fixed point hardware implementation.? Comparison with existing approaches was performed to indicate the high throughput and low hardware overhead in adding the security feature to the DWT architecture. The project will be implemented using HDL. Simulation will be done to verify the functionality and synthesis will be done to get the NETLIST. Simulation and synthesis will be done using Xilinx Tools.

*Keywords:* compression, encryption, DWT, multimedia.
*Classification:* I.3.1, K.2
*Language:* English

London Journals Press

*LJP Copyright ID: 736180*
*Print ISSN: 2514-863X*
*Online ISSN: 2514-8648*

London Journal of Research in Computer Science and Technology

2 9 7 U K

Volume 17 | Issue 2 | Compilation 1.0

# Implementation of an Efficient Hardware Architecture for Multimedia Encryption and Authentication using the Discrete Wavelet Transform

Dhanalaxmi Banavath[α] & Srinivasulu Tadisetty[σ]

## I. ABSTRACT

*This paper 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. It allows building a key space for lightweight multimedia encryption. The parameterization yields rational coefficients leading to an efficient fixed point hardware implementation. Comparison with existing approaches was performed to indicate the high throughput and low hardware overhead in adding the security feature to the DWT architecture. The project will be implemented using HDL. Simulation will be done to verify the functionality and synthesis will be done to get the NETLIST. Simulation and synthesis will be done using Xilinx Tools.*

*Keywords:* compression, encryption, DWT, multimedia.

*Author α σ:* Ku College of Engineering & Technology, Kakatiya University, Warangal, T.s., India.

## II. INTRODUCTION

Digital image processing is an area characterized by the need for extensive experimental work to establish the viability of proposed solutions to a given problem. An important characteristic underlying the design of image processing systems is the significant level of testing & experimentation that normally is required before arriving at an acceptable solution. This characteristic implies that the ability to formulate approaches & quickly prototype candidate solutions generally plays a major role in reducing the cost and time required to arrive at a viable system implementation.

An image may be defined as a two-dimensional function f(x, y), where x & y are spatial coordinates, & the amplitude of f at any pair of coordinates (x, y) is called the intensity or gray level of the image at that point. When x, y & the amplitude values of f are all finite discrete quantities, we call the image a digital image. The field of DIP refers to processing digital image by means of digital computer. Digital image is composed of a finite number of elements, each of which has a particular location & value. The elements are called pixels.

## III. METHODOLOGY

A new parameterized construction of a DWT filter with rational coefficients is proposed. 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, is an essential part of modern multimedia compression algorithms, thus serves as a transformation-cum-encryption block. The main contribution of this work can be summarized as 'Introduction to the concept of the parameterized DWT architecture for providing security to the images'. The new DWT architecture implements DWT as an encryption operation, Optimize and pipeline the hardware architecture to achieve a high clock frequency of 244 MHz with minimum hardware requirements, Provide some experimental results of image encryption and watermarking using the parameterized DWT operation.

## IV. LITERATURE SURVEY

Image compression algorithm, have the property that the bits in the bit stream are generated in order of importance, yielding a fully embedded code. The embedded code represents a sequence of binary decision that distinguishes an image from the “null” image. Using an embedded coding algorithm, an encoder can terminate the encoding at any point there by allowing a target rate to be met exactly. Algorithm, which generates a separate embedded bit stream for each code-block, is named as Bi. The coder is essentially a bit-plane coder.

The wavelet transformation divides image to low and high pass filtered parts. The traditional JPEG compression technique requires lower computation power with feasible losses, when only compression is needed. The methods are intended to the applications in which the image analyzing is done parallel with compression. Furthermore, high frequency bands can be used to detect changes or edges. Wavelets enable hierarchical analysis for low pass filtered sub-images. The first analysis can be done for a small image, and only if any interesting result is found, the whole image is processed or reconstructed.

Multimedia data security is important for multimedia commerce. Previous cryptography studies have focused on text data. The encryption algorithms developed to secure text data may not be suitable to multimedia applications because of large data sizes and real time constraint. For multimedia applications, lightweight encryption algorithms are attractive.

While encryption standards such as DES and RSA can be used to encrypt the entire video file, but it main drawbacks, since multimedia data is usually large and requires real-time processing, DES and RSA incur significant overhead. Recent video encryption algorithms have focused on protecting the more important parts of the video stream to reduce this overhead.

The architecture of a fully pipelined AES encryption processor is made on a single chip FPGA. By using loop unrolling and inner-round and outer-round pipelining techniques, a maximum throughput of 21.54 Gbits/s is achieved. A fast and area efficient composite field implementation of the byte substitution phase is designed using an optimum number of pipeline stages for FPGA implementation. Advanced Encryption Standard has led to intensive study of both hardware and software implementations.

A high performance encryption/decryption core of the advanced encryption standard (AES) is also presented. This architecture is implemented on a single-chip FPGA using a fully pipelined approach. The results show that this design offers up to 25.06% less area and yields up to 27.23% higher throughput than the fastest AES. FPGA implementations reported to date

These restrictions can be alleviated by developing a scheme that integrates both encryption and compression operations into in a Figure 1.

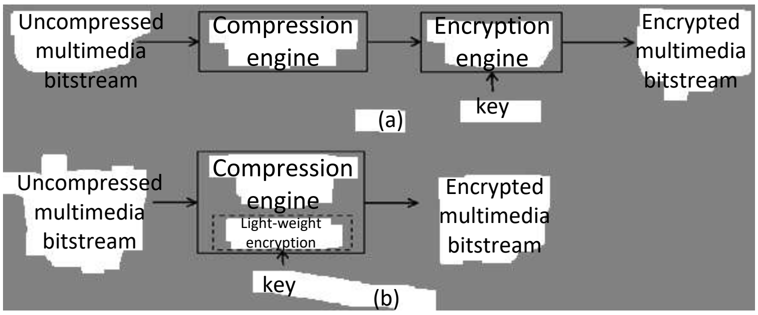
Uncompressed multimedia bitstream
Compression engine
Encryption engine
key
Encrypted multimedia bitstream
(a)
Uncompressed multimedia bitstream
Compression engine
Light-weight encryption
key
Encrypted multimedia bitstream
(b)

*Figure 1:* Lightweight multimedia encryption scheme

Consider an example to explain the significance of lightweight multimedia encryption schemes for embedded systems. In Figure 2 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. Moreover such conventional ciphers would incur a large latency in image transmission which can be critical for ground troops' (B) operation.

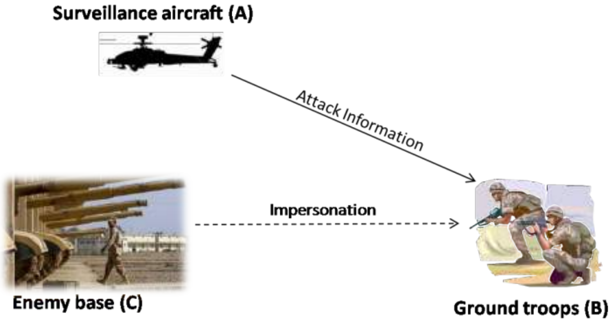

*Figure 2:* Example scenario for proposed lightweight multimedia encryption

### Efficient hardware architecture using parameterized DWT

For image compression purposes, JPEG 2000 recommends an alternate row/column-based structure as presented in Figure 3

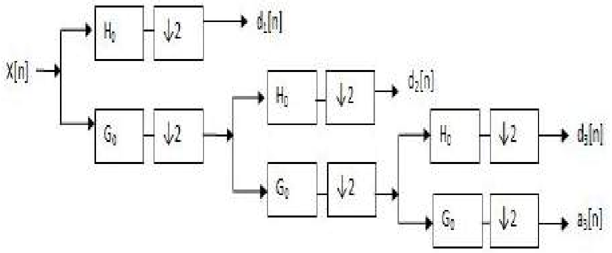

*Figure 3:* 3-Level DWT decomposition tree

To obtain the first transformation level of DWT the BWFB derivation was done. Through this derivation two filter characteristic equations namely synthesis low pass filter and analysis high pass filter characteristic equations were obtained, which are as follows:

$$H_1\,(z) = [(-9/64)\ a+ (1/32)\ a^2 + (15/64) - (1/8)\ (1/a)]\ (z^4+1/z^4) + [(-1/16)\ a^2 + (11/32)\ a - (11/16) + (1/2)\ (1/a)]\ (z^3+1/z^3) + [(1/8) - (1/2)\ (1/a)]\ (z^2+1/z^2) + [(-11/32)\ a + (1/16)\ a^2 + (15/16)-(1/2)\ (1/a)]\ (z+1/z)+[(9/32)\ a-(1/16)\ a^2 - (7/32) + (5/4)\ (1/a)] \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(1)$$

$$H_2\,(z) = [(1/32)-(1/32)\ a](z^3+1/z^3) + [(1/8)-(1/16)\ a]\ (z^2+1/z^2) + [(7/32) + (1/32)\ a]\ (z+1/z) + [1/4+ (1/8)\ a] \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(2)$$

These two equations mainly consists of more number of adders, multipliers, and irrational coefficients which results in much requirement of hardware, thus more power consumption, more delay and reduced amount of efficiency. Thus to overcome the above problem the above equations are simplified to their binary equivalent form, which can be expressed as follows:

$$H_1\,(z) = [-(1/2^3+1/2^6)\ a + (1/2^5)\ a^2 + (1/2^2-1/2^6) - (1/2^3)\ (1/a)]\ (z^4+1/z^4) + [(-1/2^4)\ a^2 + (1/2^2+1/2^4+1/2^5)\ a + (1/2+1/2^3+1/2^4) + [(1/2)\ (1/a)]\ (z^3+1/z^3) + [(1/2^3-1/2\ (1/a))]\ (z^2+1/z^2) +[-(1/2^2+1/2^4+1/2^5)\ a + (\ 1/2^4)\ a^2 + (1-(\ 1/2^4) - (1/2)(1/a)](z+1/z)+[\ (1/2^2+1/2^5)\ a -(\ 1/2^4)\ a^2 - (1/2^2-1/2^5) + (1+ 1/2^2)\ (1/a)] \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(3)$$

$$H_2\,(z) = [(1/2^5-(1/2^5)\ a]\ (z^3+1/z^3) + [(1/2^3- (1/2^4)\ a]\ ((z^2+1/z^2) + [(1/2^2-(1/2^5) + (1/2^5)\ a])]\ (z+1/z) + [(1/2^2 + (1/2^3)\ a] \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(4)$$

Thus it can be concluded that the above equations mainly consists of less number of adders, multipliers and shifting operations only, which can be implemented using less amount of hardware.

## V. DATA ENCRYPTION

Mounting concern over the new threats to privacy and security has lead to widespread adoption of cryptography. Cryptography is the science of transforming documents. It has main functions are encryption and decryption. Figure 4 shows process of Encryption and Decryption only after decoding the cipher text using the key the content of the document is revealed to the common people Figure 4: Encryption and Decryption.

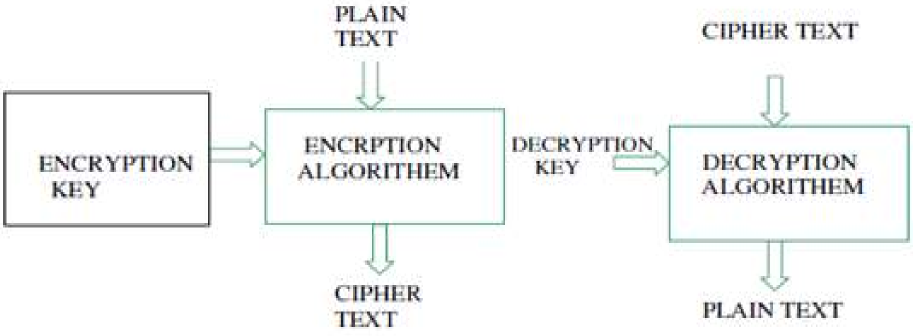

*Figure 4:* Encryption and Decryption

### *5.1 Implementation of Encryption through DWT Architecture*

Using free parameter ‘a’ which is introduced in previous Parameterized DWT, we can provide encryption for image with a zero-overhead of hardware. Number of bits of keyspace ‘a’ depends of image which is going to transmit and DWT decomposition. For Example the number of DWT operations ‘N’ in an image of size M×M pixels is bounded by the limit N≤ $log_e(M)$ . we can obtain go up to maximum of nine levels of wavelet decomposition for an image of size 512×512 pixels. One level of wavelet decomposition involves two filtering operations: one each along the row and column directions. 9x2 (rows + column) =18. Thus, we can choose up to 18 different ‘a’ values, one each for the 18 different instances of DWT kernels being used in the operation. Each ‘a’ represents 8-bits so totally 144-bits of keyspace for 512x512 image. 18x8=144-bits keyspace. These 144-bits keyspace can be used to encrypt the input frame. This level of security is sufficient for any mobile multimedia application.

## VI. CONCLUSION

This paper introduces a multimedia encryption and watermark authentication framework based on parameterized construction of DWT. The parameterization enables an efficient, pipelined, high throughput implementation in hardware. The qualitative and quantitative results in terms of both hardware performance and image security promise a secure framework for real-time multimedia delivery over embedded systems

### *Future scope*

The idea of parameterization can also be extended to other multimedia encoding blocks to obtain a more powerful integrated-encryption-scheme for embedded multimedia systems.

## REFERENCES

1. Ali Saman Tosun and Wu-chi Feng “Lightweight Security Mechanisms for Wireless Video Transmission”, Department of Computer and Information Science.
2. Ankush Mittal “Content-based Network Resource Allocation for Mobile Engineering Laboratory Applications”
3. Chakrabarti. C, Vishwanath. M, and R. M. Owens, “‘A Survey of Architectures for the

Discrete and Continuous Wavelet Transforms."

4. Changgui Shi and Bharat Bhargava "An Efficient MPEG Video Encryption Algorithm", Department of Computer Sciences".
5. Dominik Engel and Andreas Uhl "Parameterized Biorthogonal Wavelet Lifting for Lightweight JPEG2000 Transparent Encryption"
6. Herrero, J. Cerdà, R. Gadea, M. Martínez, A. Sebastià "Implementation of 1-D Daubechies Wavelet Transform on FPGA"
7. Abdullah Al Muhit, Md. Shabiul Islam and Masuri Othman "VLSI Implementation of Discrete Wavelet Transform (DWT) for Image Compression" 2nd International Conference on Autonomous Robots and Agents December 13-15, 2004 Palmerston North, New Zealand.
8. Acharya. T and Chakrabarti. C, "A Survey on Lifting-based Discrete Wavelet Transform Architectures," Journal of VLSI Signal Processing Systems, vol. 42, no. 3, pp. 321–339, 2006.
9. Bilgin .A, "Quantifying the parent-child coding gain in zero-tree-based coders," Signal Processing Letters, IEEE, vol. 8, no. 3,pp. 67–69, Mar 2001.
10. Christopoulos. C, Skodras. A, and Ebrahimi. T, "The JPEG2000 still image coding system: an overview," IEEE Transactions on Consumer Electronics, vol. 46, no. 4, pp. 1103–1127, Nov 2000.
11. Joseph J.K. _O Ruanaidh and Thierry Pun "Rotation, Scale and Translation Invariant Digital Image Watermarking"
12. http://technet.microsoft.com/en-us/library/cc750036.aspx
13. http://tektalkin.blogspot.com/2008/09/types-of-encryption.html
14. https://security.berkeley.edu/MinStds/unencrypted.auth.html
15. http://docstore.mik.ua/orelly/java-ent/security/ch07_01.htm
16. https://developer.mozilla.org/en/Introduction_to_Public-Key_Cryptography
17. http://cnx.rice.edu/content/m11156/latest/?format=pdf
18. http://en.wikipedia.org/wiki/Biorthogonal_wavelet

*This page is intentionally left blank*