Volume 4, Issue 6, June 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

ASIC Implementation of a Secure Image Coding Based on DWT and AES Processor

Mohamed Shahid S
PG Dept. ECE
EPCET,
Bangalore, India

Abdul Imran Rasheed
Dept. EEE
MSRSAS,
Bangalore, India

T. Christy Bobby
Dept. ECE
EPCET,
Bangalore, India

Abstract*— *In a digital world with the fast growing of digital data exchange, security information becomes much more important. Although several techniques have been proposed in order to protect the information, many of the methods provide limited security or introduce significant overhead. This paper proposes a secure image codec based on the Discrete Wavelet Transformation (DWT) and the Advanced Encryption Standard (AES) processor. We analyse the Advanced Encryption Standard (AES), and we add a Cipher key to AES to ensure improving the encryption performance; mainly for images characterised by reduced entropy. The prominent feature of this method is a partial encryption of key lengths of 128 or 192 or 256 bits. In this work ASIC Design is implemented with 65nm CMOS Technology by using Cadence tools. In order to implement proposed DWT-AES processor, the hardware design flow starts with modelling the design using Verilog HDL code, verified by Xilinx ISE-14.4. The RTL Synthesis is performed using Cadence RTL Compiler. The proposed codec contributes Peak Signal to Noise Ratio as 43.2531535 dB and Compression rate 1.3596.

Keywords*— *DWT, AES, Cryptography, Xilinx ise14.4, Cadence RTL Compiler

I. INTRODUCTION

The wide use of digital images and videos in various applications bring serious attention to the security and privacy issues today. Wavelet transform of a function is the improved version of Fourier transform capable of providing both time and frequency information simultaneously. The Discreet Wavelet Transform (DWT) of images is a transform based on the tree structure with 1D level that can be implemented by using an appropriate bank of filters. Image compression adopts DWT in most situations which possess the characteristics of simpleness and practicality [1].

The information contained in the images must be compressed by extracting only the visible elements, which are then encoded. The quantity of data involved is thus reduced substantially. For data communication and multimedia application, the cryptography has become an essential requirement for communication privacy and for the storage and transmission of digital images. Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity [2].

In this paper DWT and AES processor is designed and verified by using vertex-5 FPGA, and implemented using ASIC methodology. The important feature of this method is a partial encryption of bass frequency (LL bands) by AES-128 (128-bit keys), or AES-192 or AES-256 [3].

We combine the compression and encryption into single process upon user need. We improved an approach called band LL encryption to reduce encryption and decryption time in image communication and processing. The encryption-decryption effects are achieved by the AES algorithm. Encryption is a common technique to uphold image security. Image encryption has applications in various fields including internet communication, multimedia systems, medical imaging and military communication. Here using AES (Advanced Encryption Standard) to protect the confidential image data from unauthorized users. The rest of the paper is organized as follows. Section 2, describes methodology, 3, describes results and finally concluded the paper in section 4.

II. METHODOLOGY

An image size 100×100 pixel values is compressed using discreet wavelet transform with losses less compression and using lifting scheme. The compressed data is encrypted using AES algorithm by taking a key of 128bits. For the output sequence of AES the inverse discrete wavelet transform is applied to get back the synthesis image. To avoid the leakage of data to an opponent, it is also benefits if the cipher image allows little or no statistical similarity to the plain image. An image histogram show how pixels in an image are dispersed by graphing the number of pixels at each colour intensity level. To estimate the compression performance of image codec a Peak Signal-to-Noise Ratio is determined for the

synthesis image. The quality of synthesis image was calculated by Peak Signal to Noise Ratio (PSNR) in decibels (dB) according to the equation [1] and compression ratio is defined as ratio of original image and compressed image.

$$PSNR=10Log_{10}(255^2/MSE) \quad (1)$$

The Discrete Wavelet Transform, which is based on sub-band coding, is found to yield a fast computation of Wavelet Transform. The lifting scheme is an algorithm used for implementation of DWT. The lifting-based wavelet transform basically consists of three steps, which are called split, lifting, and scaling shown in figur1.Split step: The original signal, X (n), is split into odd and even samples and applying horizontal and vertical transformation by separating pixel into add and even component. Lifting step: This step is executed as N sub-steps (depending on the type of the filter), where the odd and even samples are filtered by the prediction and update filters, Pn(n) and Un(n). Normalization or Scaling step: After N lifting steps, a scaling coefficients K and 1/K are applied respectively to the odd and even samples in order to obtain the low pass band (YL(i)), and the high-pass sub-band (YH(i)).

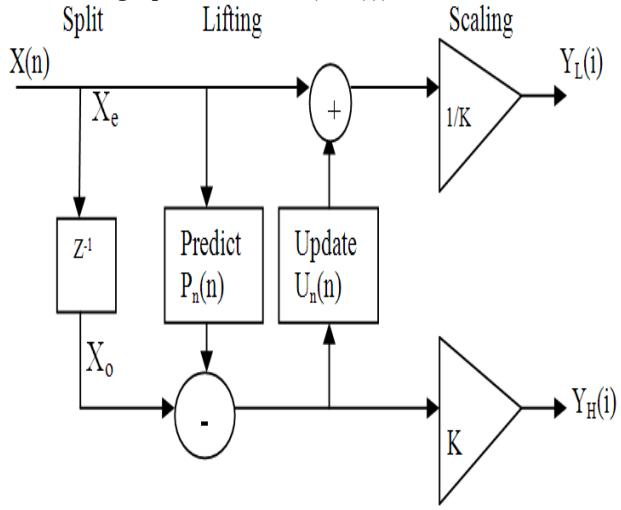


Figure 1: Split, Predict and Update phases in the lifting scheme.

A. Encryption process:

A message is plaintext which is denoted by simple binary data. The process of altering a message in such a way as to hide its substance is encryption. An encrypted message is cipher text which is denoted by binary data. The process of turning cipher text back into plaintext is decryption. Advanced Encryption Standard (AES), the algorithm is flexible in supporting any combination of data and key size of 128, 192, and 256 bits. The AES merely allows a 128 bit data length that can be divided into four basic operation blocks. These blocks operate on array of bytes and organized as a 4×4 matrix that is called the state. For full encryption, the data is passed through number of rounds Nr (Nr = 10, 12, and 14) [7], AES Encryption and Decryption are shown in figure 2.

These rounds are governed by the following transformations: SubByte transformation: A non-linear substitution step uses an S-box to perform a byte-by-byte substitution of the block. Shiftrows transformation: It's a simple permutation. A transposition step where each row of the state is shifted cyclically a certain number of steps. Mixcolumns transformation: It operates on each column individually. Each byte of a column is mapped into a new value that is a function of all four bytes in the column. Addroundkey transformation: A simple bitwise XOR of the current block with a portion of the expanded key.

B. Block diagram of secure image codec:

The encryption decryption effects are achieved by the AES algorithm. DWT based coding provides substantial improvements in picture quality at higher compression ratios. Its operation is shown in figure 3.

Discrete wavelet transform (DWT) Packets: DWT has been widely used in many different fields of audio and video signal processing [9]. DWT is being increasingly used as effective solutions to the problem of image compression. The lifting scheme is an algorithm used for implementation of DWT. Quantizer: The design of the quantizer has a significant impact on the amount of compression obtained and loss incurred in a compression scheme.

Advanced Encryption Standard (AES): AES is a very fast symmetric block algorithm with variable key length (128-bit, 192-bit, and 256-bit respectively) and block size of 128-bit. AES need very low memory to make it very well suited for restricted-space environments, in which it also demonstrates excellent performance.

Huffman coding: Huffman coding is a form of encoding that creates the most efficient set of prefix codes for a given text. The principle is to use a lower number of bits to encode the data that occurs more frequently. Controller: The controller is a module needed for optimizing applications security requirements based on a variable system resources [10].

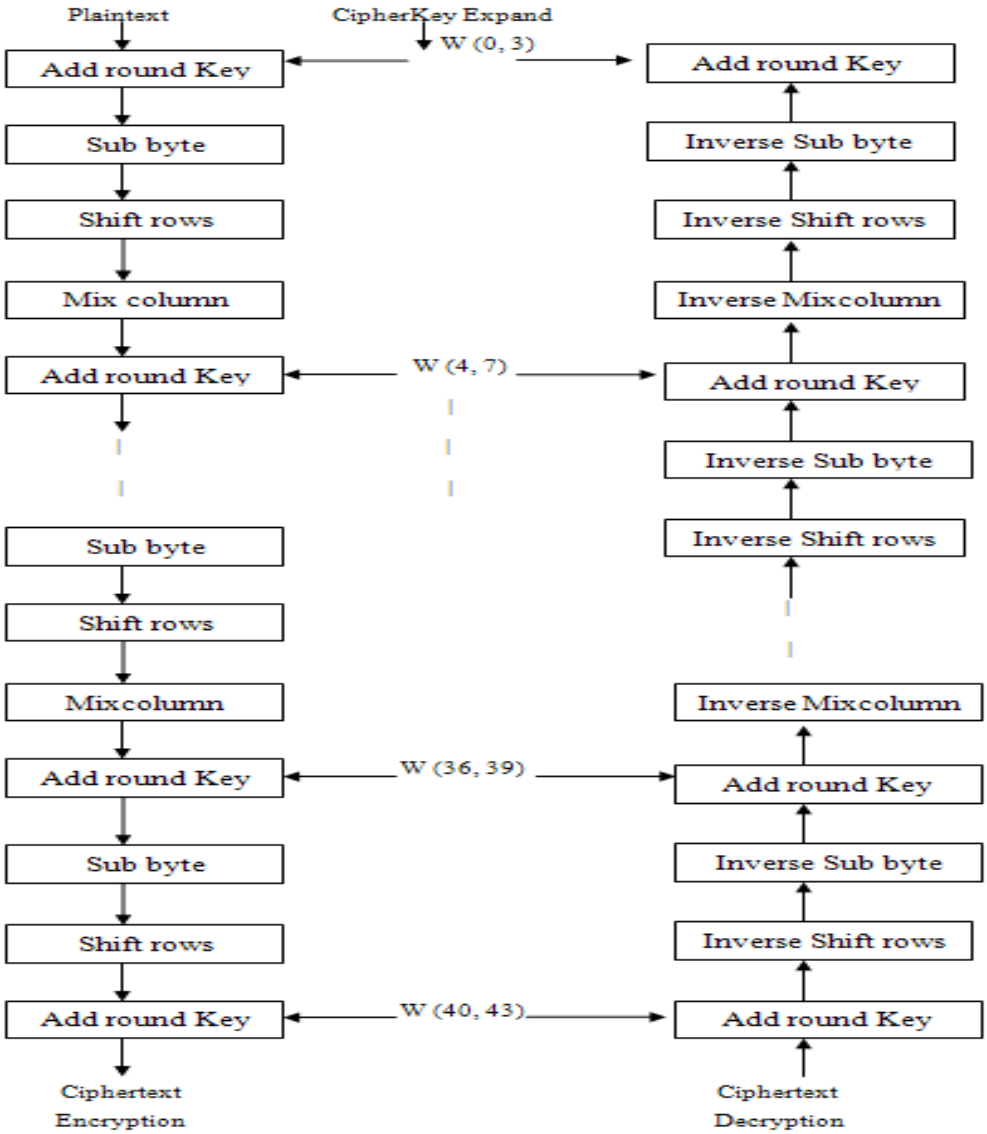


Figure 2: AES Encryption and Decryption

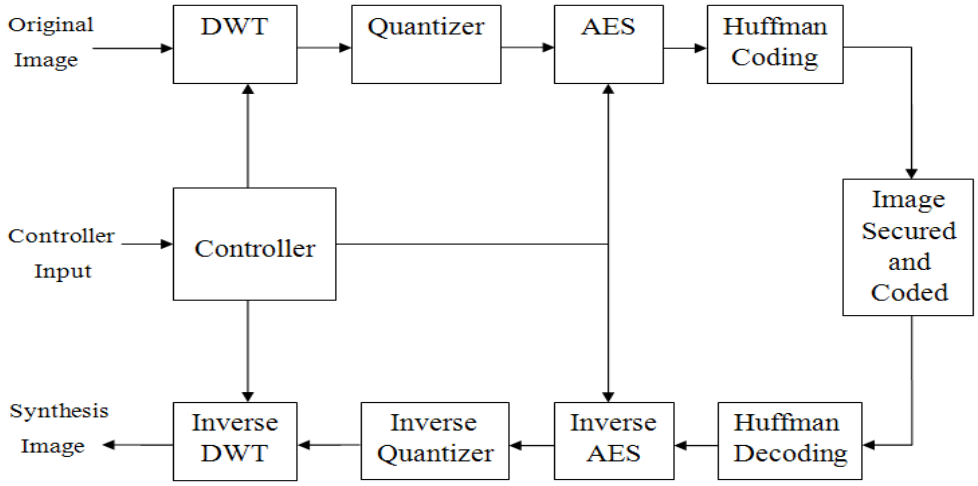
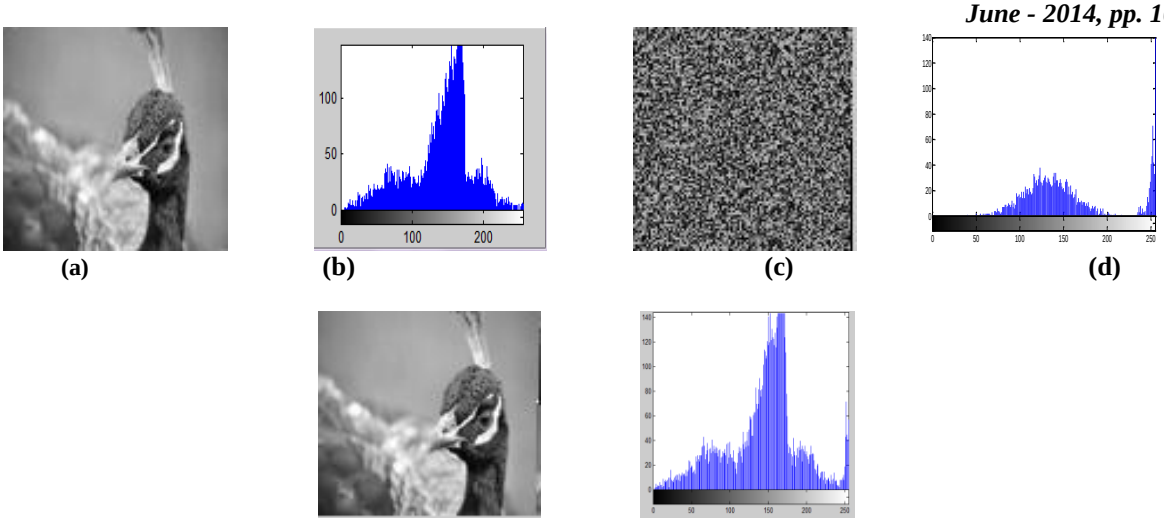


Figure 3: Block Diagram of Secure Image Codec

III. RESULT

Figure 4 (a), (c), (e) shows the Original image, encrypted image and the synthesized image and their corresponding Histogram is shown in figure (b) (d) (f) It is observed from the histogram that the pixel values are well distributed in original image and synthesized image when compared to cipher image. This shows that the cipher image is significantly different from that of the original image.



(a) **(b)** **(c)** **(d)**

(e) **(f)**

Fig 4: a) Original image 100×100 pixel; b) Histogram of original image; c) Encrypted image; d) Histogram of Encrypted image; e) Synthesis image; (f) Histogram of Decompressed image.

Table I: Compression Ratio and PSNR Result

Parameters			
Image	**Size**	**Compression ratio**	**PSNR(dB)**
Peacock	100×100	1.3596	43.2531535

The table 1 shows compression ratio and PSNR of the LL band encrypted image. The higher, the PSNR, the better the quality of the compressed or reconstructed image. Typical values for lossy compression of an image are between 30 and 50 dB In this method the PSNR value obtained is 43.25dB and compression ratio as 1.3 which gives high quality image when compared with other methods [10]. The RTL (Register Transfer Logic) Schematic is shown in Figure 5. It mainly consists of memory module, DWT, IDWT, AES, Inverse AES and Counters.

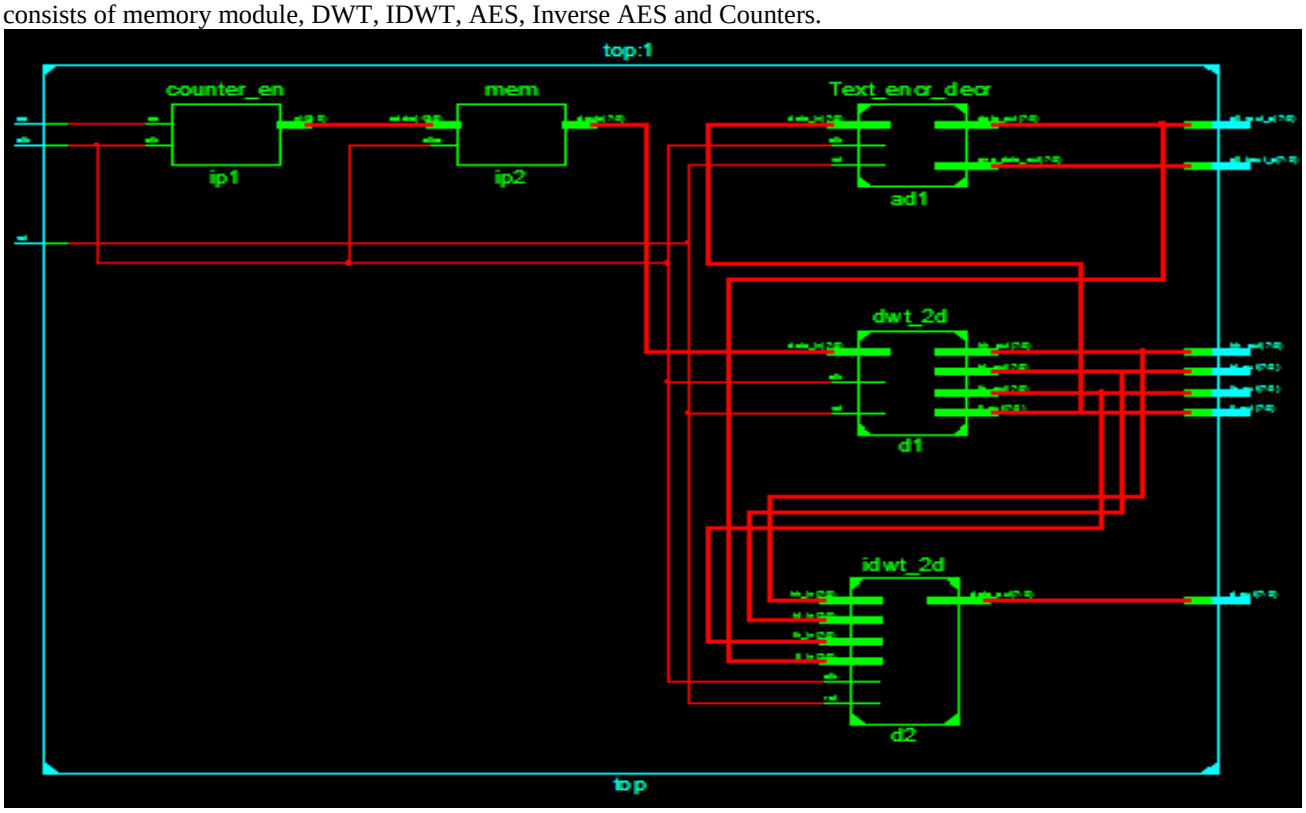


Figure 5: RTL Schematic of Top Module.

Implementation & Simulation is done by using Xilinx 14.4 ISE software. The ISim simulator is used for simulation of different image data input DWT output, Encryption output, Decryption output and IDWT output is shown in Figure 6.

Figure 6: Simulation results for Secure Image Codec for a 128 bit Cipher key.

Table II: Synthesis Power Report in Cadence RTL Compiler.

Instance	Cells	Leakage Power (nW)	Dynamic Power (nW)	Total Power (nW)
Top Module	10439	517.89	652945.48	653463.3

The Synthesis Power Report for DWT-AES processor is shown in Table II. These results are obtained by using 65nm technology, all sub modules will take area and power and also the clock module takes some amount of area and power, including all these total area and power is called top level area and power is as shown.

IV. CONCLUSIONS

An approach for image compression, encryption and decryption has been proposed and implemented based on a new modified version of DWT-AES. It uses partial encryption technique based on AES-128 bit and the DWT transform used to achieve good PSNR. The results demonstrate that the proposed secure codec is well suited to provide high security communication and high compression ratio.

REFERENCES

[1] P. Melih and D. Vadi, "A MPEG-2-transparent scrambling technology", *IEEE Transactions* on Consumer Electronics, 48, pp.345–355, 2002.

[2] A. Menezes, P. Van Oorschot, and S. Vanstone, "Handbook of applied cryptography", CRC press, New York, , pp. 81-83, 1997.

[3] Ashwini M. Deshpande, Mangesh S. Deshpande and Devendra N. Kayatanavar, "FPGA implementation of AES Encryption and Decryption ", International Conference on Control, Automation, Communication and Energy Conservation , 2009.

[4] L. Qiao and K. Nahrstedt, "Comparison of MPEG encryption algorithms", International Journal on Computer and Graphics, Special Issue on Data Security in Image Communication and Network, 22 , pp.437–448,1998.

[5] Sugreev Kaur and Rajesh Mehra,"High Speed and Area Efficient 2D DWT Processor Based Image Compression", Signal & Image Processing : An International Journal (SIPIJ) Vol.1, No.2, 2010.

[6] D.Santa-Cruz and T.Ebrahimi, "A study of JPEG 2000 still image coding versus other standards", X European Signal Processing Conference, Tampere, Finland, 2000.

[7] A. Mansouri, A. Ahaitouf, and F. Abdi, "An Efficient VLSI Architecture and FPGA implementation of High-Speed and Low Power 2-D DWT for (9, 7) wavelet Filter", IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.3, 2009.

[8] National Institute of Standards and Technology (NIST), "Advanced Encryption Standard (AES)", Federal Information Processing Standards Publications (FIPS PUBS), pp. 197-26, 2001.

[9] A. E. Rohiem, F. M. Ahmed and A. M. Mustafa "FPGA Implementation of Reconfigurable Parameters AES Algorithm", 13th International Conference on Aerospace Sciences and Aviation Technology, ASAT- 13,pp.26 – 28, 2009.

[10] Lossy Image Compression Using Discrete Wavelet Transform and Thresholding Techniques *The Open Cybernetics & Systemics Journal, 7, pp.32-38 , 2013*

[11] G.Liu, T.Ikenaga, S.Goto and T.Baba, "A Selective Video Encryption Scheme for MPEG Compression Standard", in IEICE Transactions on Fundamentals of Electronics, communications and Computer Sciences, 89, pp. 194-202. 2006

[12] M. Vetterl Mand and J. Kovacevic, "Wavelets and Subband Coding", Englewood Cliffs, New Jersey, Prentice Hall, Reissued by authors, http://cm.belllabs.com/who/jelena/Book/home.html 2007

[13] C.E. Shannon "Communication theory of secrecy system", Bell systems Tech journal, pp. 656–715. 1999

[14] Douglas J Smith, "HDL chip design using VHDL or Verilog", Doone publications, 1996

[15] Michael John Sebastian Smith, "*Application Specific Integrated Circuits", 2004*

