International Journal of Electronics and Electical Engineering

Volume 3 | Issue 1 Article 12

July 2014

FPGA IMPLEMENTATION OF A DWT AND AES PROCESSOR FOR SECURE IMAGE CODING

SANTHOSH KUMAR R
VLSI and Embedded Systems, Sri Siddhartha Institute of Technology, Tumkur, India, santhoshrkumar@yahoo.com

CYRIL PRASANNA RAJ
Dept.,EEE, M.S.R.S.A.S, Bangalore, India, cyrilyahoo@gmail.com

Y. MANJULA
E&C, Sri Siddhartha Institute of Technology, Tumkur,India, manju-yerva@gmail.com

M.Z. KURIAN
Dept.,ECE , Sri Siddhartha Institute of Technology, Tumkur, India, m.z.kurian@gmail.com

FPGA IMPLEMENTATION OF A DWT AND AES PROCESSOR FOR SECURE IMAGE CODING

SANTHOSH KUMAR R[1], CYRIL PRASANNA RAJ[2], Y. MANJULA[3] & M.Z. KURIAN[4]

[1]VLSI and Embedded Systems, Sri Siddhartha Institute of Technology, Tumkur, India
[2]Dept.,EEE, M.S.R.S.A.S, Bangalore, India
[3]E&C, Sri Siddhartha Institute of Technology, Tumkur,India
[4]Dept.,ECE , Sri Siddhartha Institute of Technology, Tumkur, India
Email: santhoshrkumar@yahoo.com, cyrilyahoo@gmail.com, manju-yerva@gmail.com

Abstract*:* With the fast growing of digital data exchange, security information becomes much important in data storage and transmission. Due to the increasing use of images in industrial process, it is essential to protect the confidential image data from unauthorized access. Better identification of which data is relevant to human perception at higher compression ratio is needed. In this DWT-AES processor a Reconfigurable Secure Image Coding is proposed. The prominent feature of this method is a partial encryption of key lengths of 128, 192 or 256 bits. Considerable Security level also mentioned. This paper presents the AES algorithm with regard to FPGA. However, linking these two designs to achieve secure image coding is leading.

Key words: *AES, DWT, Security Level, Key length.*

1. INTRODUCTION

With an astounding growth in the field of network technology and multimedia technology, the widespread dissemination of digital multimedia data is increasing at a fast pace. In the ever growing data communication and multimedia application, the cryptography protocols have become an essential requirement for communication privacy and for the storage and transmission of digital images. Besides, special and reliable security is needed in many applications, such as Internet communication, multimedia systems, medical imaging, pay-TV and military communication.

In the past decade, several efforts have developed image-video encryption schemes for secure information transfer. These techniques can be classified into three types according to the target data selected from compression stages. A "Spatial Domain", this algorithm transforms all the RGB data of each pixel of every frame in order to get satisfactory security level [3]. A "Bitstream Domain", in this algorithm, the MPEG encoder compresses the original video data firstly, and then the result bitstream is encrypted directly by standard cryptographic algorithms [4]. A "Frequency Domain", this schemes selectively encrypt the result data of motion estimation process or DCT transformation process, so that they belong to the selective encryption[5].

At present, the usage of autonomous vehicles is growing especially in applications such as manufacturing, hazardous materials handling, surveillance, etc. The basic task in any such application is the perception of the environment through one or more sensors. Processing of the sensor input results in a particular representation of the unknown environment, which can then be used for navigating and controlling the vehicle. The general sensors used for autonomous vehicles include infra-red, sonar, laser, radar and so on [1]. For example, patent discusses a navigation and control system including an emitter sensor configured to locate objects in a predetermined field of view from a vehicle and describe the techniques which make use of characteristics of infrared sensitive video data, in which heat emitting objects appear as hot spots. Compared to these types of sensors, vision sensors provide a whole new way for autonomous vehicles to create an image of the environment.

Many different types of unmanned vehicles (UVs) are being developed for use in aerial-Unmanned aerial vehicle (UAV), ground- Unmanned ground vehicle(UGV), and underwater-Autonomous underwater vehicle(AUV) environments. Unmanned robotics are actively being developed for both civilian and military use to perform dull, dirty, and dangerous activities.

Unmanned aircraft are uniquely capable of penetrating areas which may be too dangerous for piloted craft. UAVs can be used to perform Surveillance applications include wildfire mapping, pipeline security, home security, road patrol and anti-piracy, geophysical surveys in particular geomagnetic surveys this monitoring activity could be performed using digital cameras.

These unmanned vehicles(UVs) are remote-operated and the vehicle is controlled by a human operator via a communications link. All actions are determined by the operator based upon either direct visual observation or remote viewing through a camera. Since digital video or images taken from UVs transmission system usually includes a compression module that aims to reduce the transmitted bit rate, the cryptography techniques have to be carefully designed. In this encrypt the image using particular key while getting the original image the same key has to be used, so if someone sends other encrypted images also only from true encrypted images will get original image.

2. IMAGE COMPRESSION

Image compression is very important for efficient transmission and storage of images . With the use of digital cameras, requirements for storage, manipulation, and transfer of digital images, has grown explosively.

The basic objective of image compression is to find an image representation in which pixels are less correlated. The two fundamental principles used in image compression are redundancy and irrelevancy. Redundancy removes redundancy from the signal source and irrelevancy omits pixel values which are not noticeable by human eye. In lossless compression schemes, the reconstructed image, after compression, is numerically identical to the original image. In lossy compression contains degradation relative to the original.

In recent times, much of the research activities in image coding have been focuses on the DWT, which has become a standard tool in image compression applications because of their data reduction capability. DWT can provide better image quality than DCT, especially on a higher compression ratio [6]. DWT is used as basis for transformation in JPEG 2000 standard [7]. DWT provides high quality compression at low bit rates. DWT performs better than DCT in the context that it avoids blocking artifacts which degrade reconstructed images.

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 [8] basically consists of three steps, which are called split, lifting, and scaling shown in Figure 1.

Split step: The original signal, X(n), is split into odd and even samples.

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 lowpass band (YL(i)), and the high-pass sub-band (YH(i)).

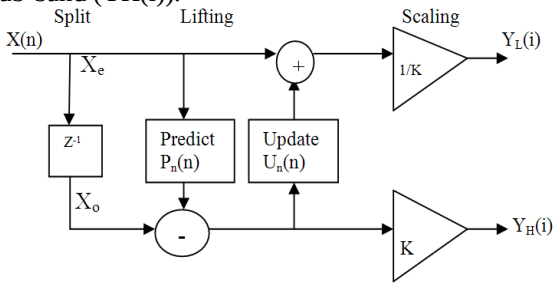

Figure 1: Split, Predict and Update phases in the lifting scheme

The quality of synthesis image was calculated by Peak Signal to Noise Ratio (PSNR) in decibels (dB) according to the equation (1):

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

Where image coded in 8 bits and MSE the cost function named Mean Squared Error (MSE) given by equation (2):

$$MSE=\frac{}{}^{2} \quad (2)$$

3. ENCRYPTION PROCESS

An original message is known as the plaintext, while the coded message is called the ciphertext. The process of converting from plaintext to ciphertext is known as enciphering or encryption restoring the plaintext from the ciphertext is deciphering or decryption. Advanced Encryption Standard(AES), the algorithm [2] is flexible in supporting any combination of data and key size of 128, 192, and 256 bits. However, 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, 14), AES Encryption and Decryption are shown in Figure 2.

These rounds are governed by the following transformations [10] :

SubByte transformation: A non-linear substitution step where each byte is replaced with another according to a lookup table.

Shiftrows transformation: A transposition step where each row of the state is shifted cyclically a certain number of steps.

Mixcolumns transformation: Is equivalent to a matrix multiplication of columns of the states. Each column vector is multiplied by a fixed matrix. It should be noted that the bytes are treated as polynomials rather than numbers.

Addroundkey transformation: Is a simple XOR between the working state and the roundkey. Each Round Key consists of Block Size Nb words from the key schedule.

The cipher transformation is inverted and implemented in reverse order to produce a straightforward inverse cipher for AES algorithm. Invshiftrows, invsubbyte, invmixcolumn and addroundkey are the transformation performed in decryption.

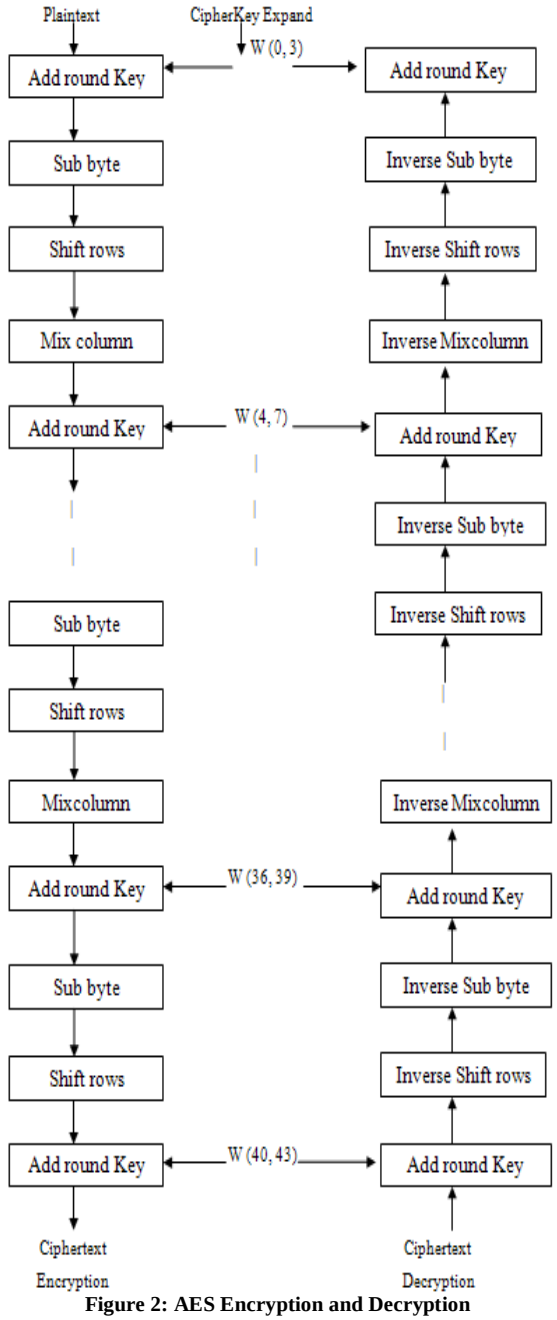

Figure 2: AES Encryption and Decryption

4. 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 [9] is shown in Figure 3.

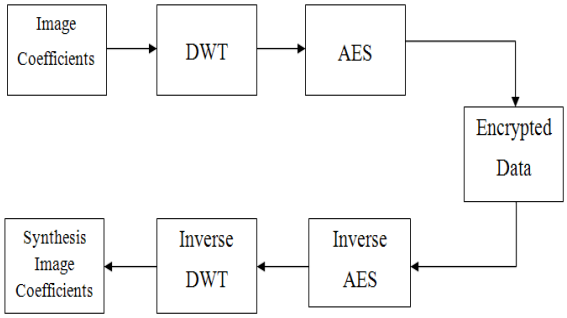

Figure 3: Block Diagram of Secure Image Codec

The primary goal of any image compression technique is to reduce the number of bits needed to represent the image with little perceptible distortion. The flow of data is through DWT module and then AES module. DWT and AES blocks compress and encrypt the image data respectively where as bottom Inverse AES and Inverse DWT blocks decrypt and reconstruct the image from the compressed data.

Discrete wavelet transform (DWT) : DWT has been widely used in many different fields of audio and video signal processing. 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. It is constituted by predictions and updating steps.

Advanced Encryption Standard(AES): AES is a block cipher 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.

5. SIMULATION RESULTS:

Below figures shows the simulated results of Key expansion, Encryption and Secure Image Codec for a 128 bit key length.

5.1 Key Expansion of a 128 bit Cipher key:

This section contains the key expansion of the following cipher key of 128 bits.
Cipher Key = 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f (in hexadecimal).
The detailed simulation key expansion result of all 10 rounds is shown in Figure 4.

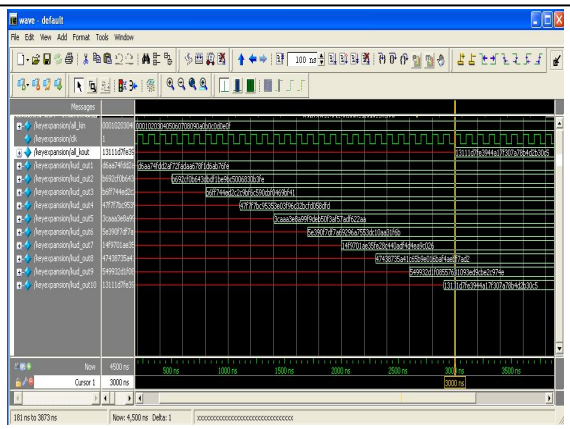

Figure 4: Simulation results of 128 bit Key Expansion

5.2 Encryption and Decryption for a 128 bit Cipher key:

A 128 bit plain text is encrypted under a 128 bit cipher key.

Plain Text = 00 11 22 33 44 55 66 77 88 99 aa bb cc dd ee ff (in Hexadecimal)

Cipher Key = 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f (in Hexadecimal).

The detailed simulation Encryption result for all 10 rounds is shown in Figure 5.

Output Ciphertext: 69 c4 e0 d8 6a 7b 04 30 d8 cd b7 80 70 b4 c5 5a (in Hexadecimal).

Decryption Result = 00 11 22 33 44 55 66 77 88 99 aa bb cc dd ee ff (in Hexadecimal)

The detailed simulation Decryption result for all 10 rounds is shown in Figure 6.

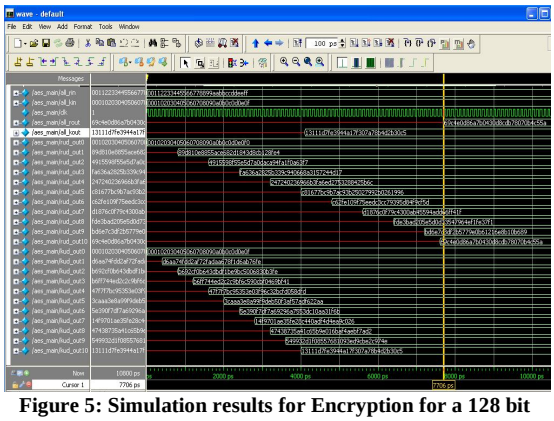

Figure 5: Simulation results for Encryption for a 128 bit Cipher key.

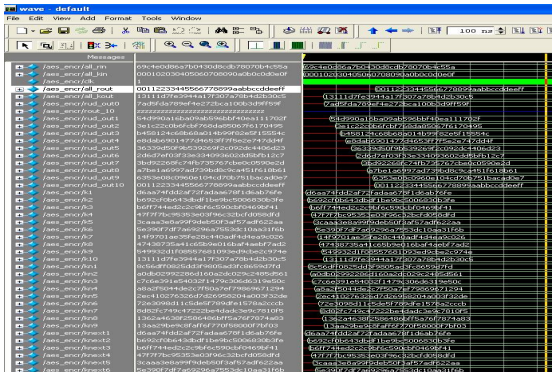

Figure 6: Simulation results for Decryption for a 128 bit Cipher key.

5.3 Secure Image Codec for a 128 bit Cipher key:

For different data input DWT output, Encryption output, Decryption output and IDWT output is shown in Figure 7.

From Figure 7 below it is observed that input data and final output data are same.

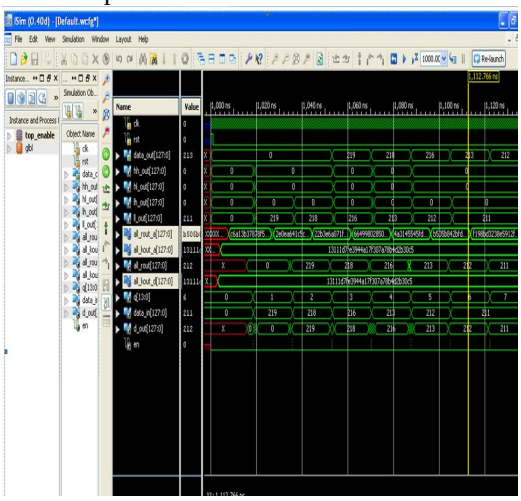

Figure 7: Simulation results for Secure Image Codec for a 128 bit Cipher key.

6. FPGA RESULTS

Below Figures 8 shows the FPGA Chipscope results of a Secure Image Codec for a 128 bit key length of different image coefficients.

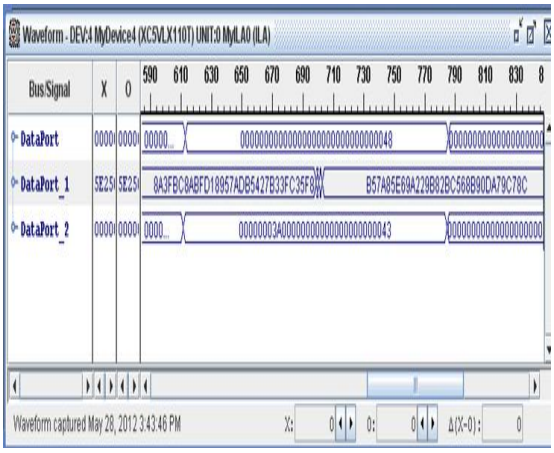

Figure 8: Chipscope results for Secure Image Codec for a 128 bit Cipher key.

7. CONCLUSION

In this a new modified version of AES with DWT, to design a compressed and secure image encryption technique, has been proposed. The DWT performs a multiresolution analysis of a signal with localization in both time and frequency domain. The key stream generator has an important influence on the encryption performance. The block size has a minimum of 128 and a maximum of 256 and key sizes in any multiple of 32 bit. This advantages our proposed model compared to other models.

REFERENCES

[1] Mattos L., Grant E. Passive sonar applications: Target tracking and navigation of an autonomous robot. In Proc of the 2004 IEEE Int Conf on Robotics and Automation, New Orleans, LA, USA May 2004; 5: 4265-4270.

[2] 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, 4th-6th June 2009

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

[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 (1998), pp.437–448.

[5] 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 (2006), pp. 194-202.

[6] 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, December 2010.

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

[8] 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, March 2009.

[9] D.Dia, M.Zeghid, M.Atri, B.Bouallegue, M.Machhout and R.Tourki, "DWT-AES Processor for a Reconfigurable Secure Image Coding", International Journal of Computer Science and Engineering,vol.1,no.2,june 2009.

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