AN EFFICIENT VLSI IMPLEMENTATION OF IMAGE ENCRYPTION WITH MINIMAL OPERATION

[1,]S.Lakshmana kiran, [2,]P.Sunitha
[1,]M.Tech Student,
[2,]Associate Professor,Dept.of ECE
[1,2,]Pragati Engineering college,Surampalem(A.P,IND)

Abstract

Traditional fast Discrete Cosine Transforms (DCT)/ Inverse DCT (mCT) algorithms have focused on reducing the arithmetic complexity. In this manuscript, we implemented a new architecture simultaneous for image compression and encryption technique suitable for real-time applications. Here, contrary to traditional compression algorithms, only special points of DCT outputs are calculated. For the encryption process, LFSR is used to generate random number and added to some DCT outputs. Both DCT algorithm and arithmetic operators used in algorithm are optimized in order to realize a compression with reduced operator requirements and to have a faster throughput. High Performance Multiplier (HPM) is being used for integer multiplications. Simulation results show that the encryption is done in the frequency domain. The throughput of this architecture is 656 M samples/s with a clock frequency of 82 MHz.

Keywords: DCT, ENCRYPTION, LFSR

I.Introduction

Security of multimedia information is used to protect the multimedia content from unauthorized access. Cryptography is the technique which is used for secure communication over the network. By using Cryptography technique readable information is converted into unreadable form. Image information is different from the text data, it has larger amount of data, higher redundancy and stronger correlation between pixels. Traditionally developed encryption algorithm such as RSA, DES is suitable for text encryption but not suitable for image encryption directly because of two reasons. One is that the image size is larger than that of text, so the traditional cryptosystems take much time to directly encrypt the image data.The other reason is that the decrypted text must be equal to the original text. However, this requirement is not necessary for image; a decrypted image containing small distortion is acceptable due to human perception [1].Figure 1 shows how original image converted into encrypted image. At present there are many image encryption algorithms are available but these algorithms doesn't satisfy the requirement of modern cryptographic mechanism and they are prone to attacks. In the recent years, the image encryption has been developed to overcome the above disadvantages.

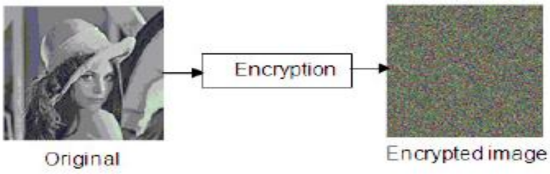


Figure1. Image Encryption System

Ii.Discrete Cosine Transform

Discrete cosine transform (DCT) is one of the major compression schemes owing to its near optimal performance and has energy compaction efficiency greater than any other transform. The principle advantage of image transformation is the removal of redundancy between neighboring pixels. This leads to uncorrelated transform coefficients which can be encoded independently. DCT has that de correlation property.The transformation algorithm needs to be of low complexity. Since the DCT is separable 2-D can be obtained from two 1-D DCTs. The 2-D DCT equation is given by Equation (1)

$$C(u,v)=\alpha(u)\alpha(v)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x,y)\cos\left[\frac{\pi(2x+1)u}{2N}\right]\cos\left[\frac{\pi(2y+1)v}{2N}\right],$$

For u,v= 0,1,2,…,N −1 .

The inverse transform is defined by Equation (2)

$$f(x,y)=\sum_{u=0}^{N-1}\sum_{v=0}^{N-1}\alpha(u)\alpha(v)C(u,v)\cos\left[\frac{\pi(2x+1)u}{2N}\right]\cos\left[\frac{\pi(2y+1)v}{2N}\right],$$

For x, y= 0, 1, 2,…, N −1. The 2-D basis functions can be generated by multiplying the horizontally oriented 1-D basis functions with vertically oriented set of the same functions.In image compression, the image data is divided up into 8x8 blocks of pixels. (From this point on, each color component is processed independently, so a "pixel" means a single value, even in a color image.) A DCT is applied to each 8x8 block. DCT converts the spatial image representation into a frequency map: the low-order or "DC" term represents the average value in the block, while successive higher-order ("AC") terms represent the strength of more and more rapid changes across the width or height of the block. The highest AC term represents the strength of a cosine wave alternating from maximum to minimum at adjacent pixels.

Iii.Efficient Design and Fpga Implementation of Jpeg Encoder Using Verilog Hdl

The JPEG encoder is a major component in JPEG standard which is used in image compression. It involves a complex sub-block discrete cosine transform (DCT), along with other quantization, zigzag and Entropy coding blocks. In this architecture, 2-D DCT is computed by combining two I-D DCT that connected by a transpose buffer. For the case of 8 x 8 block region, a one-dimensional 8- point DCT followed by an internal transpose memory, followed by another one dimensional 8-point DCT provides the 2D DCT architecture. The calculation is implemented by using eight multipliers and storing the coefficients in ROMs. At the first clock, the eight inputs x00 to x07 are multiplied by the eight values in column one, resulting in eight products (P00 to P07). At the eighth clock, the eight inputs are multiplied by the eight values in column eight resulting in eight 586 products (P070 to P077). From the equations for Z, the intermediate values for the first row of Z are computed. The values for Z0 (0 -7) be calculated in eight clock cycles. All 64 values of Z are calculated in 64 clock cycles and then the process is repeated. The values of Z correspond to the 1-DDCT of the input X. Once the Z values are calculated, the 2D-DCT function Y = C*Z.

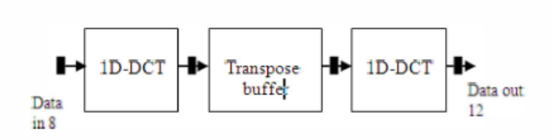


Figure 2. 2-D DCT Architecture

The maximum clock frequency is 78 MHz when implemented with a ALTERA FPGA CYCLONE-III device.

Iv. Pipelined Multiplierless 2-D Dct/Idct Architecture .

The 2-D DCT architecture achieves an operating frequency of 166 MHz. This architecture is used as the core of JPEG compression hardware. The 2-D DCT calculation is made using the 2-D DCT separability property, such that the whole architecture is divided into two 1-D DCT calculations by using a transpose buffer.

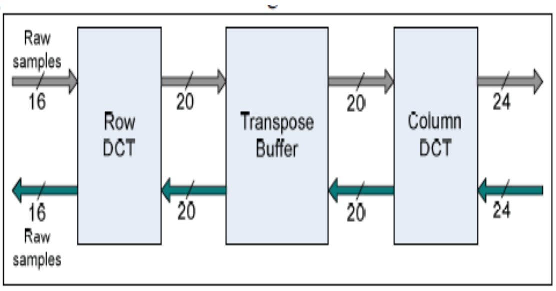


Figure .3 Architecture of 2-D DCT

Figure 3 shows the architecture of 2-D DCT. 2D-DCT/IDCT design is divided into three major blocks namely Row-DCT, Transpose Buffer, and Column-DCT. Row-DCT and Column-DCT contains both 1DDCT (Figure. 4) by Row.

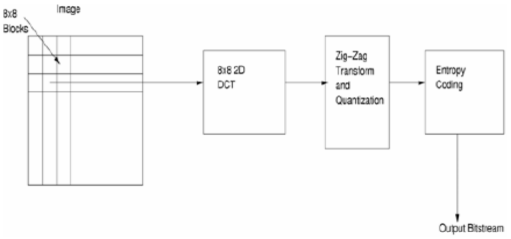


Figure. 4 Architecture of 2-D DCT

During Forward transform, 1D-DCT structure (Figure 4) is functionally active. Row-DCT block receives two 8-bit samples as an input in every cycle. Each sample is a signed 8- bit value and hence its value ranges from -128 to 127. The bit width of the transformed sample is maintained as 10-bit to accommodate 2-bit increment during

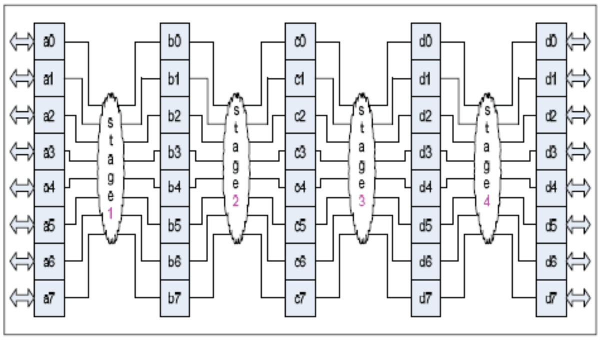
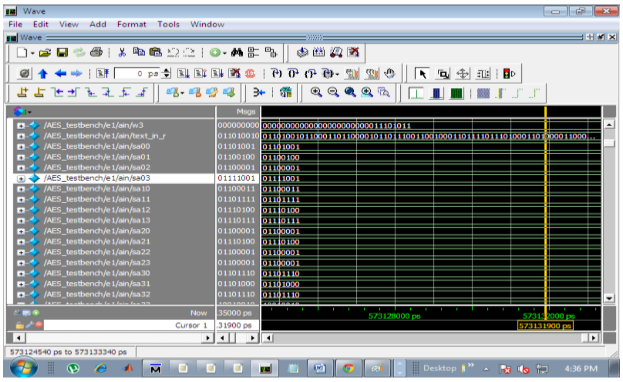


Figure .5 Four Stage Pipeline 1D-DCT.

1D-DCT computation architecture (Figure. 5) has a four stage internal pipeline shown in Figure 4.Transpose Buffer receives two 10-bit samples as an input every cycle. Each sample is a signed 10-bit value and hence its value ranges from -512 to 511. Since there is no data Manipulation in the module the output sample width remains as input sample width i.e. 10-bit. Transpose buffer has sixty-four 10-bit registers to store one 8X8 block 1D-DCT samples. Transpose operation on 8X8 block data is performed by writing the transformed samples in row-wise and reading them in column-wise and vice versa. Transpose Buffer block guarantees that the nth 8X8 block data will be written into the registers after (n-1)th 8X8 block data has been completely read out for further processing. The latency of the block is 31 cycles since the data can be read only after full 8X8 block is written in the registers. Column DCT block receives two 10-bit samples as an input in every cycle.The 2D-DCT/IDCT architecture efficiently operates up to 166Mhz. Pipeline latency for the initial 8x8 block with each element of 8 bits is 45 clock cycles which is due to 7 cycles at Row-DCT, 31 cycles for Row-DCT operation to complete, 7 cycles at Column-DCT. Effectively to perform complete 2D DCT on one 8x8 will take 33 Clock cycles on availability of continuous input data to process. For operating frequency of 166 MHz, the processing time of 8x8 blocks is 0.198µs.

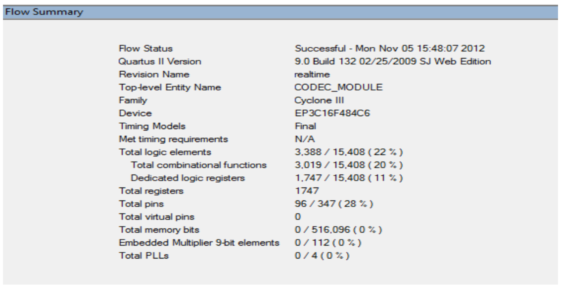
V. RESULT AND DISCUSSION:MODEL SIM OUTPUT:



```
/AES_testbench/e1/ain/w3          000000000  0000000000000000000000001110 1011
/AES_testbench/e1/ain/text_in_r   0110100 10 0110100101100011011000010110111001100100011011101110100011010000 11000...
/AES_testbench/e1/ain/sa00        01101001   01101001
/AES_testbench/e1/ain/sa01        01100100   01100100
/AES_testbench/e1/ain/sa02        01100001   01100001
/AES_testbench/e1/ain/sa03        01111001   01111001
/AES_testbench/e1/ain/sa10        01100011   01100011
/AES_testbench/e1/ain/sa11        01101111   01101111
/AES_testbench/e1/ain/sa12        01110100   01110100
/AES_testbench/e1/ain/sa13        01110111   01110111
/AES_testbench/e1/ain/sa20        01100001   01100001
/AES_testbench/e1/ain/sa21        01110100   01110100
/AES_testbench/e1/ain/sa22        01100001   01100001
/AES_testbench/e1/ain/sa23        01100001   01100001
/AES_testbench/e1/ain/sa30        01101110   01101110
/AES_testbench/e1/ain/sa31        01101000   01101000
/AES_testbench/e1/ain/sa32        01101110   01101110
                          Now     35000 ps          573128000 ps         5731[illegible]2000 ps
                     Cursor 1     31900 ps                                573131900 ps
573124540 ps to 573133340 ps
```

Figure 6. Simulated output.

AREA UTILIZATION REPORT:

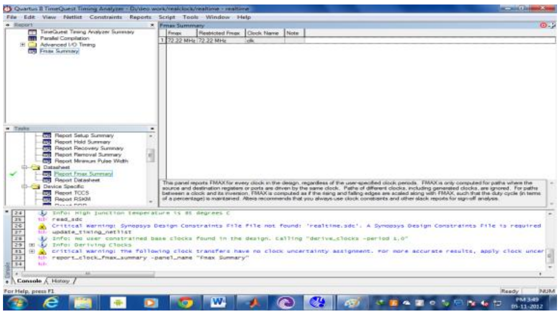


Flow Summary

Flow Status	Successful - Mon Nov 05 15:48:07 2012
Quartus II Version	9.0 Build 132 02/25/2009 SJ Web Edition
Revision Name	realtime
Top-level Entity Name	CODEC_MODULE
Family	Cyclone III
Device	EP3C16F484C6
Timing Models	Final
Met timing requirements	N/A
Total logic elements	3,388 / 15,408 (22 %)
Total combinational functions	3,019 / 15,408 (20 %)
Dedicated logic registers	1,747 / 15,408 (11 %)
Total registers	1747
Total pins	96 / 347 (28 %)
Total virtual pins	0
Total memory bits	0 / 516,096 (0 %)
Embedded Multiplier 9-bit elements	0 / 112 (0 %)
Total PLLs	0 / 4 (0 %)

Figure 7.Flow summary report

PERFORMANCE REPORT:



Fmax Summary

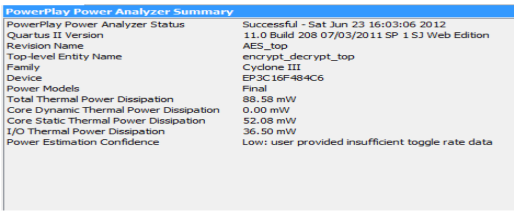
	Fmax	Restricted Fmax	Clock Name	Note
1	72.22 MHz	72.22 MHz	clk	

This panel reports FMAX for every clock in the design, regardless of the user-specified clock periods. FMAX is only computed for paths where the source and destination registers or ports are driven by the same clock. Paths of different clocks, including generated clocks, are ignored. For paths between a clock and its inversion, FMAX is computed as if the rising and falling edges are scaled along with FMAX, such that the duty cycle (in terms of a percentage) is maintained. Altera recommends that you always use clock constraints and other slack reports for sign-off analysis.

```
24    Info: High junction temperature is 85 degrees C
25    read_sdc
26    Critical Warning: Synopsys Design Constraints File file not found: 'realtime.sdc'. A Synopsys Design Constraints File is required
27    update_timing_netlist
28    Info: No user constrained base clocks found in the design. Calling "derive_clocks -period 1.0"
29    Info: Deriving Clocks
31    Critical Warning: The following clock transfers have no clock uncertainty assignment. For more accurate results, apply clock uncer
33    report_clock_fmax_summary -panel_name "Fmax Summary"
34
```

Figure 8. Fmax.Summary report of slow carner.

POWER ANALYZES:



PowerPlay Power Analyzer Summary

PowerPlay Power Analyzer Status	Successful - Sat Jun 23 16:03:06 2012
Quartus II Version	11.0 Build 208 07/03/2011 SP 1 SJ Web Edition
Revision Name	AES_top
Top-level Entity Name	encrypt_decrypt_top
Family	Cyclone III
Device	EP3C16F484C6
Power Models	Final
Total Thermal Power Dissipation	88.58 mW
Core Dynamic Thermal Power Dissipation	0.00 mW
Core Static Thermal Power Dissipation	52.08 mW
I/O Thermal Power Dissipation	36.50 mW
Power Estimation Confidence	Low: user provided insufficient toggle rate data

Figure. 9 Power dissipation report

CONCLUSION

The proposed encryption method uses the Selective Encryption approach where the DC coefficients and some selective AC coefficients are encrypted, hence the DC coefficients carry important visual information, and it's difficult to predict the selective AC coefficients, this give a high level of security in comparison with methods mentioned above. The algorithm will not encrypt bit by bit the whole image but only selective DCT coefficients will be encrypted, and extra security has been added to the resulted encrypted blocks by using Block Shuffling method depending on two prime numbers, where these two primes will generate sequences or row and column numbers to be used in shuffling. The algorithm considered as a fast image encryption algorithm, due to the selective encryption of certain portion of the image (the DC and some AC coefficients).

References

[1] Xiliang Liu, "Selective encryption in distribution networks: challenges and new directions", Proceedings of Communications, Internet, and Information Technology (CIIT 2003), Scottsdale, AZ, USA, Nov. 2003.

[2] Fonteneau C., Motsch J., Babel M., and D´eforges O., "a hierarchical selective encryption technique in a scalable image codec", International Conference in Communications, Bucharest, Romania 2008.

[3] Han Shuihua* and Yang Shuangyuan**, Non-members, "An Asymmetric Image Encryption Based on Matrix Transformation ", ecti transactions on computer and information technology
vol.1, no.2 november 2005.

[4] M. Van Droogenbroeck and R. Benedett, “Techniques for a Selective Encryption of Uncompressed and Compressed Images,” in Proceedings of Advanced Concepts for Intelligent Vision Systems (ACIVS) 2002, Ghent, Belgium, Sept. 2002.

[5] M. M. Fisch, H. Stgner, and A. Uhl, “Layered Encryption Techniques for DCT-Coded Visual Data,” in European Signal Processing Conference (EUSIPCO) 2004, Vienna, Austria, Sep., 2004.

[6] Rodrigues, J.M. Puech, W. Bors, A.G. "Selective Encryption of Human Skin in JPEG Images", IEEE International Conference on Image Processing, 2006.

[7] L. Tang. Methods for Encrypting and Decrypting MPEG Video Data Efficiently. In Proc. ACM Multimedia, volume 3, pages 219–229, 1996.

[8] H. Cheng and X. Li. Partial Encryption of Compressed Images and Videos. IEEE Trans. On Signal Processing, 48(8):2439–2445, Aug. 2000.

[9] R. Lukac and K. Plataniotis. Bit-Level Based Secret Sharing for Image Encryption. Pattern Recognition, 38(5):767–772, May 2005.

[10] C. Wu and C. Kuo. Design of Integrated Multimedia Compression and Encryption Systems. IEEE Trans. on Multimedia, 7(5):828–839, Oct. 2005.

[11] M. V. Droogenbroeck and R. Benedett. Techniques for a Selective Encryption of Uncompressed and Compressed Images. In Proc. of Advanced Concepts for Intelligent Vision Systems (ACIVS) 2002, Ghent, Belgium, pages 90–97, Sept. 2002.