Efficient Low Power Region Enhanced Architectures For DWT And AES For Protected Coding Image

Shanmugaraja T and Supriya M
1,2Assistant Professor/ECE, KPR Institute of Engineering and Technology, Coimbatore
shanmugarajatsr@gmail.com

Godwin Cryil N
3Assistant Professor/ECE, Sethu Institute of Technology
Technical lead, Oath Electronics, Bangalore

Kavin kumar K
2Assistant Professor (Senior Grade)/ECE, Kongu Engineering College

Pradeep M
4Assistant Consultant, TATA Consultancy Services

Abstract - In this article presents an HDL template on the ASIC platform. For quicker and safer image data transmission stable encoding of pictures via image compression and AES through encryption, the DWT was facilitated. The DWT calculation algorithm based on a lifting scheme and a multi-level sub-bands on the ASIC platform are created. 2D-DWT was built using it. The related sub-bands were chosen to minimize the compression time of the AES encryption, based on compression ratio and data recovery. To ensure high efficiency and latency, the DWT architecture was developed HDL model and AES algorithm for the area, timing and power performance of the ASIC platform have been developed and validated for the DWT architecture. Using 56 nm CMOS technology, the ASIC implementation was carried out.

Keywords - Encoding, data recovery, encryption, CMOS.

1. Introduction
In any area of life in the modern field of information digital images are widely used. Automatic delivery, collection and retrieval are a matter of waste in their efforts to keep pace with advancements in other areas of science and technology globally. Faster and safer imaging, storage and recovery methods are needed. The new project is a concentrated endeavour in this respect. In many cases, the existing picture transmission systems and techniques are handicapped. The key problem is that standard methods make encryption time and the huge scale of image data more time consuming. Nor are the security features trustworthy and secure. Developing novel methods for image transmission will solve these limitations. The investigators in the present analysis Demonstrate several specific ways to send and retrieve image data easily and securely.

By using image transmission, researchers are discovering new ways of transmitting images. Present technological know-how in literature. The researcher’s procedures the encrypted out of the receiver room by using the AES algorithm, sub-bands are prone to processes of decryption. Therefore, by using inverse DWT the default image is restored [4]. The match between the two of them original and reconstructed images are tested using multiple measures of image quality and Affirmative. Found. To promote high throughput, the DWT architecture was designed Latency and. By using DWT lifting and AES architectures they have built and validated hardware models for sector, timing and output recognition on the ASIC algorithm [5] platform. Current research is very important in the same manner that results will lead to most reaching change in transmission field of images and communication of data.

Increased protection picture transmission characteristics provided by the results of the current study may be in the different domains of human life, the cause of unparalleled change and progress trade and trade, defense, the mobile phone industry, medicine, education, scientific innovations and. The hardware was designed, created and validated by the innovative forms and means can be used to further improve investigators in order to tackle the world’s needs and requirements. These embedded components are extremely strong. Cost is extremely low and user can easily work, without quality sacrifices.
The current article is composed of 5 sections. Implementation is the first portion. The second section illustrates the generalized protected image transmission scheme. The 3rd segments the changed method for safe image transmission and the fourth segment are shown. It illustrates the implementation and performance of AES and DWT on the ASIC. The last segment is article's completion.

2. Scheme for Safe Image Encoding

This is a new approach used for the transfer of image data [6]. The encoding of the image input DWT is done, with sub-bands of various types rising. The sub-strips are quantified with sufficient techniques and encrypted. The information that is encrypted is encoded and thus compressed. The Protected Picture Information Below, the code is depicted diagrammatically as Figure 1. How the protected image is coded is shown in Figure 1. The original picture is revealed to DWT Yeah. This triggers the development of different sub bands. Defined by the quantize various value sets and the assigning of limited values to them. AES is capable of handling data of 128 bits with key lengths of 256, 192 or 128 bits at a time. Huffman code [7] activates the encoding in sub bands encrypted by AES of redundant details.

3. Image Compression Using Dwt

A technique used internationally as a standard is the 2D DWT for image processing. Its approach is facilitated by low-pass filter and low-pass optical image. Modes of high pass the DWT method is known as the decomposition of the Mallat-tree. The IDWT is known as the inverse method of DWT. The DWT of a given picture LL, LH, HL and HH are the four sub bands that were obtained.

These sub-bands include components of low frequency and high frequency and components of frequency (Edges with horizontal axes, vertical axes and diagonal axes) [8, 9]. The fig.2 demonstrates pyramidal decomposition using the DWT of the input image. In the first stage transformation the given input image is divided into four different images as LL, LH, HL and HH sub bands. In the second stage each component is again split into the above different sub bands and it goes on. The outcomes of the initial the decomposition of levels is shown in Figure 2 and the second step, as shown in Figure 2 and Figure 3.

The quantization of sub-bands in higher end is not necessary and transmission with no quantization, LL sub band leads to resize of images. A picture with the scale N: N will lead to rise of 7 sub bands (three higher bands) after decomposition at two stages. Stage sub bands of N2 Scale N44s at the first stage, three N4 at low frequency one and one the N2 sub band and N2 during the second level.

4. Encryption and Decryption of AES

The symmetric encryption algorithm, which is more well-known and widely adopted, they’re the AES these days. It is detected somewhere about six times faster than it is somewhere around Conventional algorithms such as DES triple [10]. In Block cyphers certain algorithms are used which is used for encryption of data for individual block where AES is a part. The AES uses bytes instead of bits to perform the entirety of its calculations. Henceforth, AES handles a plaintext block’s 128 bits as 16 bytes. The arrangement of four rows and four columns are made with 16 bytes of data which is arranged like a matrix. Since AES is 128 bits in length, 128 bits of cipher text for each 128 bits of plaintext, they’re made. A similar key is used since the AES equation is symmetric in Encryption and decryption.

In AES, the number of rounds is variable and depends on the main duration. The round of number for the length of 128,192 and 256 bits will be 10, 12 and 14 respectively. To deliver an arrangement of round keys from the underlying
key, the AES key schedule is used. In AES, as a contribution to add round key assignment the basic key is underlet. In the different bit adaptions like 128, 192 and 256 of AES, different round keys are delivered like 10, 12 or 14.

5. Modified Algorithm for Safe Image Coding

Key restrictions of conventional image encoding will lead to excess use of time to compute the AES algorithm. The researchers in the present analysis using DWT, the input image was converted to several sub-bands, each of which by using AES, it was quantized and also encrypted. It then took very low time to encrypt method. The block diagram for safe image encoding that has been updated is shown in the Figure 3.

This demonstrates the dividing of the image which is given as input into seven high sub-bands and modules of less frequency. The LL2 sub band was encrypted by the researchers using Algorithm of AES with no quantization [11]. The other sub bands like LH2, HL2 and HH1 were quantized and encrypted independently. The total number of encoded bits is shown in Table 1 after 2D DWT and quantization.

The number of bits encoded using the AES algorithm is presented in Table 1 above. With pictures of different sizes. In the encoding scheme for images without DWT, the number of frames to be encoded (128 bits each) is shown in column brackets. The number of frames to be generated after decomposition with 2D-DWT using two levels in column 5, the encoded value is shown in brackets. The pixels are depicted after DWT, Using nine pieces. After DWT, the total number of frames to be encrypted is lowered by fifty percent. The computational time for the AES algorithm is therefore reduced to less than 8 s (16 s).

The time with no DWT is just seconds, sub bands are encoded by the AES algorithm since the time taken totally for encoding is less in the newly designed algorithm by two seconds.

![Fig. 4: Modified Algorithm for Safe Image Coding](image)

Table 1: Decomposition using 2D DWT

| Input image size | Bits per frame | LL2/LH2/LH2 | LH2/LH1/HH1 (in No. of bits) | No. of bits to be encoded using AES after selection |
|-----------------|---------------|-------------|-----------------------------|-----------------------------------------------|
| 64 × 64         | 32768 (256)   | 2034        | 9126                        | 15228 (119)                                  |
| 128 × 128       | 131072 (1024) | 9126        | 36864                      | 64242 (502)                                  |
| 256 × 256       | 524288 (4096) | 36864       | 147456                     | 258048 (2016)                               |
| 512 × 512       | 2097152 (16384)| 147456     | 589824                     | 1032192 (8064)                              |
| 1024 × 1024     | 8388608 (65536)| 589824     | 2359296                    | 4129768 (3225)                              |

6. DWT and AES Architectures

Implementation DWT Filter Range

For safe image coding, selection of the required wavelet philtre is of prime importance. The choice of philtres is dependent on two important parameters: first, the complexity of the hardware Adaptability in implementation and second for all possible pictures. There are, there are Different wavelet philtres available, including bi-orthogonal 4.4 (bio4.4) Due to its characteristics listed in [12, 13, 14] and [15], it is the better one.

DWT And AES Fast Architectures

Quick architectures for DWT and IDWT over the ASIC platform are built in this segment. 2-D DWT and IDWT with two multipliers have been suggested [16] Architectures that use Filters 4-tap. 100% of the architecture was used. Hardware and ultra-low power consumption, consistent structure, trouble free flow of control, greater throughput and scalability. With the overall aim of lessening the Complexity and increased computation speed, DWT linear algebra equations using [17] VHDL implementation.

This approach to linear algebra offers almost a comparable performance with very few hardware resources being used. Furthermore, a more effective solution has been taken by the parallel feedback, which is eight coefficients of a picture at a time to adjust time needed by serial inputs and resources. A DWT processor was developed [18] with Parallel design and improved throughput by having two outputs in a single architecture Cycle of the clock. This architecture's speed does not depend on the amount of the philter the sum of bits per sample and the taps. Furthermore, the IDWT processor provides reasonably Perfect one-dimensional signal reconstruction [19]. A lifting system dealt with folded DWT and IDWT architecture was suggested, which Low latency but increased hardware region utilization.

Complicated routing, as well, for the converters used in this architecture, and interconnections were necessary. The Verilog HDL code was synthesized and physical modeling was done using 65 nm CMOS technology. In [20] DWT has a high-speed area-efficient architecture. A partly serial processor in this processor is Pipelining architecture has been used to increase speed and maximize utilization on the target FPGA, of hardware capital. The findings showed that this is the design that will operate with consumption of maximum power frequency of 231MHz from 117mw. AES encryption and decryption have been enforced in [21] Usage of VHDL and confirmed FPGA on Spartan 3. It was observed that the encryption of both on 50 and 100 MHz, decryption and decryption models were used. A thoroughly pipelined The AES encryption processor was implemented in FPGA and Ingrid Verbauwhede from [22]. The pipelining techniques were used by this architecture, such as Loop unrolling, inner and outer round and a maximum output of 21.54 Gbits / s was achieved.
ASIC Implementation of The DWT Architecture Proposed

In this work, as part of the implementation, the lifting-based DWT has been developed. The lifting equations are defined where \( \alpha = -1.586134342, \beta = -0.052980118, \gamma = 0.882911075, \delta = 0.443506852, \zeta = 1.149604398 = 0.149604398 \). Scaling of the coefficients Multiplied by 8192, i.e., to 213 to achieve 13-bit accuracy using arithmetic of fixed integer for floating point numbers for operations of both addition and multiplication is shown in Table 2.

**Table 2: DWT operations**

| DWT       | Scaled coefficient \((2^{13})\) |
|-----------|---------------------------------|
| \( \alpha = -1.586134342 \) | 12993                           |
| \( \beta = -0.052980118 \)   | 6716                            |
| \( \gamma = 0.882911075 \)    | 3633                            |
| \( \delta = 0.443506852 \)    | 3633                            |
| \( 1/\zeta = 1.149604398 \)   | 9417                            |
| \( R = 1/\zeta = 0.869864522 \) | 7125                           |

The results are rounded to 255 if greater than 255, from the arithmetic operations. The value is rounded to zero when the desired arithmetic operation is negative. Such rounding operations are performed because of the pixel value range of the picture is just 0–255. The input image which is processed at the level 1 processing is performed in the three-level DWT as in the Eq. per the lifting equations. After the processing of level-1 rows, the Outputs were obtained from low pass and high pass coefficients. Further processing is performed to get four sub band outputs LH1, HL1 and HH1, respectively, for bad performance of a step in a column level-1 processor. The LL1 is continued and the processing of philtres for low-pass and high-pass results in the level-2 row processor. These outputs are processed separately and four sub-band outputs, such as LL2, LH2, HL2 and HH2, have been generated by column processors of level 2.

LL2 is stored for high-gage and low-gate outputs and saved separately in level-3 processors, resulting in four LL3, LH3, HL3 and HH3 sub band outputs in the level-3 row processor. The ten DWT outputs of the sub-band are integrated together to achieve the corresponding DWT output of the image. The DWT level Three Ones is built with HDL and a practical testing bench is created. There are 16 input numbers, each of which has a width of 20-bit. Those inputs were forwarded using SIPO (Serial Input Parallel Output). Multipliers, multiplexers and registers are supported from the DWT Adders. The data is divided into even and strange components, wherever the inputs are transmitted through SIPO. These parts are put away in the temporary registers. The temporary registry data becomes null at the point where Big is reset. The reset is small, separated into even and peculiar data sets at every point as shown in Figure 5 and Figure 6.

The data input is scanned up to 16 clock cycles and the data scanning is based on the lifting device technique. The following table includes both low and high pass elements (Table 3). The DWT is the 1D and the DWT are the low-and high-pass elements. Again, it can be divided into LL, LH and HH, HL elements. The net list of DWT and IDWT syntheses is shown in Figure 4. A synthesized net list is analysed for its pacing, and a scheduling report is given in
Table 3 and Table 4. Timing performance for zero slack Changed to 2 ns for time length. Post DFT with Prime (Time Table 4) produces optimum performance results. The IDWT takes up more area and still power due to the intermediate memory.

Table 5: DWT timing result

| Report        | PD  |
|---------------|-----|
| Power (mW)    | 11.7689 |
| Setup timing  | 0.5 |
| Setup slack   | 0.197 |
| Hold timing   | 0.25 |
| Hold slack    | 0.214 |

Table 6: IDWT timing result

| Report        | PD  |
|---------------|-----|
| Power (mW)    | 19.7074 |
| Setup timing  | 0.5 |
| Setup slack   | 0.246 |
| Hold timing   | 0.25 |
| Hold slack    | 0.258 |

After physical design, Tables 5 and 6 shows the timing effects. The physical architecture It is carried out with models of real wire loads. The timing findings provide insight into the maximum frequency and dissipation of maximum force.

The plan of the floor determines the design die size for the border and core area and allows for normal cell structure wire tracks Figure 5. It is a process that positions block or macros on the die.

The aspect ratio, center-to-left, center-to-right, center— to-bottom, center-to-top, i.e., the core application, depends on the main area, which divides the straps and stubs. When architecture library is set up, floor planning’s must be used to define boundary and core area and control rings and braces should be created Figure 6 Electricity and ground links must be created.

Snapshot of the DWT and IDWT architecture IR drop map analysed and analysed this is illustrated in Fig. The drop map in the IR consists of a drop map based on Vdd and a drop map based on Vss (Figure 7). After physical design, power information of DWT and IDWT are clearly shown in the Table 7. It is found that the IDWT absorbs significant power when compared to DWT.

7. Conclusion

The present study provides important results that are highly significant in area of both encrypting and decrypting of images. Results may have long-reaching influence on outcome. The compression and encryption of image data is region, time and power efficiency. The findings of this analysis show the advantages as a test of AES: picture and other content encryption. In AES the followed procedure may able to through using an algorithm that fits the situation in question and is more susceptible, it is also possible to encrypt a complex input image. A DWT lifting system has been developed for and enacted. The top configuration is synthesized with a 65 nm compatible Synopsys tool technology for CMOS. The DWT introduced the operating frequency maximum of 350 MHz for consumption.

References

[1]. Chen LG, Huang CT, Chen CY, Cheng, VLSI design of wavelet transform, analysis, architecture, and design examples. Imperial College Press,2007.

[2]. Sundararajan D., discrete wavelet transform: a signal processing approach. Wiley, London,2016

[3]. Daemen J, Rijmen V the design of Rijndael: AES- the advanced encryption standard. Springer, New York,2013

[4]. Wilson P., Design recipes for FPGAs: using verilog and VHDL. Elsevier,2011.

[5]. Smith MJS., Application-specific integrated circuits, vol 7. Addison-Wesley Reading, MA,1997.

[6]. Dia D, ZeghidM, AtriM, Boulallegue B, Machhout M, Tourki R Dwt-aes processor for a reconfigurable secure image coding. Int J Computer Sci Eng 1(2),2009.

[7]. Acharya T, Tsai PS., JPEG2000 standard for image compression: concepts, algorithms and VLSI architectures. Wiley, London,2005.
[8] Ravi RV, Subramaniam K., Image compression and encryption using optimized wavelet filter bank and chaotic algorithm. Int J Appl Eng Res 12(21):10595–10610, 2017.

[9] Ravi RV, Subramaniam K., Optimized wavelet filters and modified huffman encoding based compression and chaotic encryption for image data. Int J Appl Eng Res 12(13):3961–3977, 2017.

[10] Parametric optimization of architectural modified fir filter. Shanmugaraja, T., Jai Shankar, Siddharthraju K., Venkatesh T., Dhivyadevi, R., Supriya, M. International Journal of Advanced Science and Technology, 2020, 29(7 Special Issue), pp. 1481-1487

[11] Ravi RV, Mahalakshmi R., Dwt-aes based information security system for unmanned vehicles, vol 3. p 101, 2014.

[12] Multi-ported memory on fpga for a high performance fir filters. Supriya, M., Dhivyadevi, R., Shanmugaraja, T., Siddharthraju K., Venkatesh, T., Jai Shankar, B. International Journal of Advanced Science and Technology, 2020, 29(7 Special Issue), pp. 1464-1472

[13] Liu H, Zhai LP, Gao Y, Li WM, Zhou JF., Image compression based on biorthogonal wavelet transform. In: IEEE international symposium on communications and information technology, 2005. ISCIT 2005. vol 1, IEEE, pp 598–601, 2005.

[14] Rout S., Orthogonal vs. biorthogonal wavelets for image compression. Master’s thesis, Virginia Polytechnic Institute and State University (Virginia Tech), 2003.

[15] Raajan N, Vijayabhaskar P, Shiva G, Mithun P., Evaluation of wavelet filters in image coding using spiht. J Appl Sci 14(14):1618, 2014.

[16] Sung TY, Shieh YS, Yu CW, Hsin HC., Low- power multiplierless 2-d dwt and idwt architectures using 4- tap daubechies filters. In: 7th international conference on parallel and distributed computing, applications and technologies, 2006. PDCAT’06. IEEE, pp 185–190, 2006.

[17] Al Muhit A, Islam MS, Othman M., Vlsi implementation of discrete wavelet transform (dwt) for image compression. In: Proceedings of international conference on autonomous robots and agents, vol 4. ICARA, 2004.

[18] A critical review on applications of adaptive filters. Shanmugaraja, T., Dhivyadevi, R., Supriya, M., Murugan K., Venkatesh, T., Siddharthraju, K. Journal of Critical Reviews, 2020, 7(6), pp. 656-659

[19] Parhi KK, Nishitani T., Vlsi architectures for discrete wavelet transforms. IEEE Trans Very Large Scale Integ (VLSI) Systems 1(2):191–202, 1993.

[20] Kaur S, Mehra R., High speed and area efficient 2d dwt processor-based image compression. Sign Image ProcessInt, 2010 (SIPIJ). https://doi.org/10.5121/sipij.2010.1203

[21] Deshpande AM, Deshpande MS, Kayatanavar DN., Fpga implementation of aes encryption and decryption. In: 2009 international conference on control, automation, communication and energy conservation, 2009. INCACEC 2009. IEEE, pp 1–6

[22] Hodjat A, Verbauwheide I., A 21.54 gbits/s fully pipelined aes processor on fpga. In: 12th annual ieee symposium, 2009.