Technical Sciences
Academy of Romania
www.jesi.astr.ro

Journal of Engineering Sciences and Innovation
Volume 7, Issue 1 / 2022, p. 97-104

**F. Electrical, Electronics Engineering,
Computer Sciences and Engineering**

Received ***26 November 2021*** *Accepted* ***7 March 2022***
Received in revised form ***15 January 2022***

A new integer algorithm for an efficient VLSI implementation of DST using obfuscation technique

CHIPER DORU FLORIN[*]

Technical University Gheorghe Asachi, Iasi, 700050, Romania
Technical Sciences Academy of Romania-ASTR
Academy of Romanian Scientists-AOSR

Abstract. In this paper we propose a new VLSI algorithm for an integer based discrete sine transform (IntDST) that allows an efficient VLSI implementation using systolic arrays. The proposed algorithm have all the benefits of an integer transform as a good approximation of irrational transform coefficients and allows an efficient restructuring into a regular and modular computation structure that allows an efficient VLSI implementation using systolic arrays. An efficient VLSI architecture for discrete sine transform can be obtained that allows an efficient incorporation of the obfuscation technique that significantly improves the hardware security and offering high speed performances due to a concurrent computation and using pipelining technique at a low hardware complexity.

Keywords: discrete sine transform, Integer based transforms, VLSI algorithms, VLSI architectures, systolic arrays.

1. Introduction

amount of data at high speed and using resource constrained devices. It was one of the main beneficiaries of new researches in related fields as electronics, telecommunications, information technologies and VLSI (Very Large Scale Integrated Circuits) technology. It includes important research areas as image compression, accurate data transmission in real time using low area processors with high performance and working at high speed and more Some examples of such applications that benefit from the latest developments in the research area include for example image and video via the Internet, digital libraries and telemedicine.

[*] Correspondence address: chiper@etc.tuiasi.ro

With the advancement of the telemedicine field, applications in real-time multimedia have evolved in order to support the high requirements in this area, thus an efficient use of the VLSI technology using Field Programmable Gate Array (FPGA) or Application Specific Integrated Circuits (ASIC) has become necessary. One important algorithm used in data compression and transmission is the discrete sine transform (DST) [1] that represents a good approximation of the statistically optimal Karhunen-Loeve transform for low correlated images

In order to achieve an efficient VLSI implementation there is necessary to reformulate or to design dedicated algorithms.

To obtain a good VLSI algorithm for DST it is important to afford a special attention for the data flow in the algorithm. It is well known, as for example in case of Fast Fourier Transform (FFT), that the communication complexity is even more important than computational ones. So, it is important to find or to design regular and modular computational structures as for example cyclic convolution and circular correlation that have important advantages over other ones due to its specific data flow involving efficient input/output and data transfer operations especially in the case of using distributed arithmetic [2] or systolic arrays [3]. Thus, several solutions have been proposed for a VLSI implementation of some Digital Signal Processing (DSP) algorithms based on cyclic convolution or circular correlation [4]-[10].

It was shown that the important advantages of using circular correlation or cycle convolution from a VLSI implementation point of view can be extended to other structures as for example skew-circular and pseudo-circular correlations or band-correlation [11]-[13].

In this paper, we are presenting a new VLSI algorithm for DST based on small integers called Integer DST that allows an efficient algorithm transformation that allow an efficient solution for a VLSI implementation of DST. The obtained VLSI algorithm has a reduced hardware complexity leading to hardware implementation with a reduced number of multipliers. The obtained computational structures can be used to obtain all the advantages of the cyclic convolution and circular correlation structures-based VLSI implementations as a modular and regular architecture a high speed using pipelining and parallelism and local connections and a low I/O cost using a systolic array architectural paradigm. Besides the mentioned advantages the proposed computational structures can lead to an efficient incorporation of the obfuscation technique.

2. A low complexity algorithm for the VLSI Implementation of DST based on band-correlation structures

The 1-D DST is defined as:

$$Y(k)=\sum_{i=0}^{N-1} x(i)\cdot\sin[(2i+1)k\cdot\alpha] \qquad (1)$$

for k = 1, …, N
where:

$$\alpha = \pi/2N \tag{2}$$

We can write Equation (1) in a matrix-vector product as follows:

$$\begin{bmatrix} Y(1) \\ Y(2) \\ Y(3) \\ Y(4) \\ Y(5) \\ Y(6) \\ Y(7) \\ Y(8) \end{bmatrix} = \begin{bmatrix} \sin(\alpha) & \sin(3\alpha) & \sin(5\alpha) & \sin(7\alpha) & \sin(9\alpha) & \sin(11\alpha) & \sin(13\alpha) & \sin(15\alpha) \\ \sin(2\alpha) & \sin(6\alpha) & \sin(10\alpha) & \sin(14\alpha) & \sin(18\alpha) & \sin(22\alpha) & \sin(26\alpha) & \sin(30\alpha) \\ \sin(3\alpha) & \sin(9\alpha) & \sin(15\alpha) & \sin(21\alpha) & \sin(27\alpha) & \sin(33\alpha) & \sin(39\alpha) & \sin(45\alpha) \\ \sin(4\alpha) & \sin(12\alpha) & \sin(20\alpha) & \sin(28\alpha) & \sin(36\alpha) & \sin(44\alpha) & \sin(52\alpha) & \sin(60\alpha) \\ \sin(5\alpha) & \sin(15\alpha) & \sin(25\alpha) & \sin(35\alpha) & \sin(45\alpha) & \sin(55\alpha) & \sin(65\alpha) & \sin(75\alpha) \\ \sin(6\alpha) & \sin(18\alpha) & \sin(30\alpha) & \sin(42\alpha) & \sin(54\alpha) & \sin(66\alpha) & \sin(78\alpha) & \sin(90\alpha) \\ \sin(7\alpha) & \sin(21\alpha) & \sin(35\alpha) & \sin(49\alpha) & \sin(63\alpha) & \sin(77\alpha) & \sin(91\alpha) & \sin(105\alpha) \\ \sin(8\alpha) & \sin(24\alpha) & \sin(40\alpha) & \sin(56\alpha) & \sin(72\alpha) & \sin(88\alpha) & \sin(104\alpha) & \sin(120\alpha) \end{bmatrix} \cdot \begin{bmatrix} x(0) \\ x(1) \\ x(2) \\ x(3) \\ x(4) \\ x(5) \\ x(6) \\ x(7) \end{bmatrix} \tag{3}$$

where Y(k) represents the auxiliary output sequence and x(i) the real input sequence.
Using similar ideas as in [14] where the matrix used for integer DCT is:

$$\mathbf{C}_8 = \begin{bmatrix} 64 & 64 & 64 & 64 & 64 & 64 & 64 & 64 \\ 89 & 75 & 50 & 18 & -18 & -50 & -75 & -89 \\ 83 & 36 & -36 & -83 & -83 & -36 & 36 & 83 \\ 75 & -18 & -89 & -50 & 50 & 89 & 18 & -75 \\ 64 & -64 & -64 & 64 & 64 & -64 & -64 & 64 \\ 50 & -89 & 18 & 75 & -75 & -18 & 89 & -50 \\ 36 & -83 & 83 & -36 & -36 & 83 & -83 & 36 \\ 18 & -50 & 75 & -89 & 89 & -75 & 50 & -18 \end{bmatrix}. \tag{4}$$

we are designed a new integer DST given by the following equation:

$$\begin{bmatrix} Y(1) \\ Y(2) \\ Y(3) \\ Y(4) \\ Y(5) \\ Y(6) \\ Y(7) \\ Y(8) \end{bmatrix} = (1/64) \times \begin{bmatrix} 12 & 36 & 53 & 63 & 63 & 53 & 36 & 12 \\ 24 & 59 & 59 & 24 & -24 & -59 & -59 & -24 \\ 36 & 63 & 12 & -53 & -53 & 12 & 63 & 36 \\ 45 & 45 & -45 & -45 & 45 & 45 & -45 & -45 \\ 53 & 12 & -63 & 36 & 36 & -63 & 12 & 53 \\ 59 & -24 & -24 & 59 & -59 & 24 & 24 & -59 \\ 63 & -53 & 36 & -12 & -12 & 36 & -53 & 63 \\ 64 & -64 & 64 & -64 & 64 & -64 & 64 & -64 \end{bmatrix} \cdot \begin{bmatrix} x(0) \\ x(1) \\ x(2) \\ x(3) \\ x(4) \\ x(5) \\ x(6) \\ x(7) \end{bmatrix} \tag{5}$$

Besides the general advantages of integer algorithms as an efficient implementation of the multipliers due to the fact that the integer coefficients can be represented exactly using a small number of bits, the proposed integer algorithm allows an efficient algorithmic transformation for an efficient hardware implementation using systolic arrays. Moreover, the obtained algorithm based on computation structures of a specific form and its associated VLSI architecture allows an efficient incorporation of the obfuscation technique.

We can reformulate (5) as two quasi-circular correlation structures and obtain a matrix-vector product as follows:

$$\begin{bmatrix} Y(1) \\ Y(3) \\ Y(7) \\ Y(5) \end{bmatrix} = (1/64) \times \begin{bmatrix} 12 & 36 & 63 & 53 \\ 36 & 63 & -53 & 12 \\ 63 & -53 & -12 & 36 \\ 53 & 12 & 36 & -63 \end{bmatrix} \cdot \begin{bmatrix} x(0)+x(7) \\ x(1)+x(6) \\ x(4)+x(3) \\ x(2)+x(5) \end{bmatrix} \qquad (6)$$

where Y(k) represents the output sequence and x(i) the input sequence

We have noted

$x_p(0,7) = x(0) + x(7)$ (7)

$x_p(2,5) = x(2) + x(5)$ (8)

$x_p(4,3) = x(4) + x(3)$ (9)

$x_p(6,1) = x(6) + x(1)$ (10)

As it can be seen in (6), all the elements from the inverse diagonal coincide obtaining the specific form called quasi-circular correlation.

$$\begin{bmatrix} Y(2) \\ Y(6) \end{bmatrix} = (1/64) \times \begin{bmatrix} 24 & 59 \\ 59 & -24 \end{bmatrix} \cdot \begin{bmatrix} x_n(0,7) + x_n(3,4) \\ x_n(2,5) + x_n(1,6) \end{bmatrix} \qquad (11)$$

where Y(k) represents the auxiliary output sequence and x(i) the auxiliary input sequence

The matrix-vector product from equation (11) has the same specific form as in equation (6) but at a half-length.

We have noted

$x_n(0,7) = x(0) - x(7)$ (12)

$x_n(3,4) = x(3) - x(4)$ (13)

$x_n(2,5) = x(2) - x(5)$ (14)

$x_n(1,6) = x(1) - x(6)$ (15)

$$Y(8) = x(0) - x(1) + x(2) - x(3) + x(4) - x(5) + x(6) - x(7) \qquad (16)$$

$$Y(4) = (1/64)[x(0) + x(1) - x(2) - x(3) + x(4) + x(5) - x(6) - x(7)] \times 45 \qquad 17)$$

We have noted

$x_n(0,7,3,4) = x_n(0,7) – x_n(3,4)$ (18)

$x_n(2,5,1,6) = x_n(2,5) – x_n(1,6)$ (19)

Based on (18) and (19) we can reformulate (16) and (17) as below:

$$Y(8) = x_n(0,7,3,4) + x_n(2,5,1,6) \qquad (20)$$

$$Y(4) = (1/64) \times [x_n(0,7,3,4) + x_n(2,5,1,6] \times 45 \qquad (21)$$

3. Architecture of the VLSI implementation of integer DST

In the Fig.1 and Fig.2 we present the hardware core of the VLSI architecture that implements the integer based DST. In Fig. 1 it is presented the systolic array that implements equation (11) and in Fig. 2 we have the systolic array that implements equation (6) of the VLSI implementation of the integer DST. Thus, the hardware core is formed of two linear systolic arrays as presented below: we have 4 elementary processors PEs for the implementation of equation (6) and 2 elementary processors PEs for the implementation of equation (11) in each processor element we have one simple multipliers where one of the operands has only 6 bits. This allow a significant reduction of the hardware complexity.

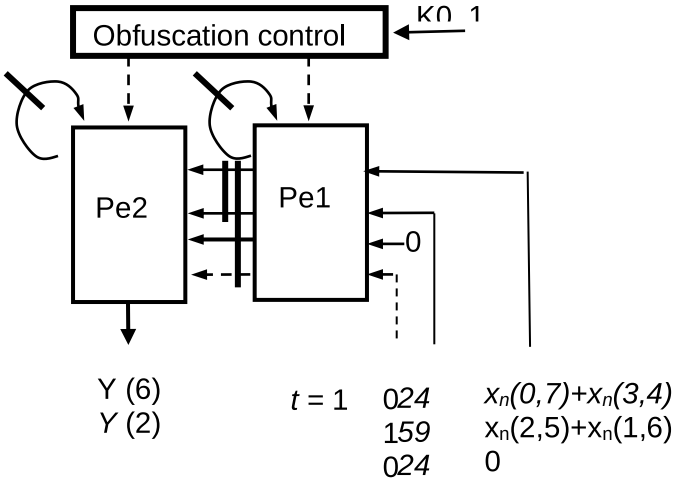


Fig. 1. The systolic array for the equation (11).

As it can be seen from equations (6), (9), (11), (16) and (17), the number of multiplications is significantly reduced in a such way that instead of 64 multiplications from equation (3) we are using only 7 simple multipliers with small integers represented on 6 bits.

The pre-processing and post-processing stages are used to implement the equations (7)-(10, (12)-(15) and (18),(19) ,which are only additions and subtractions and are used to compute the input and the output sequences.

The function of the elementary processing elements PEs from the two systolic arrays presented in Fig. 1 and Fig. 2 it is shown in Fig. 3.

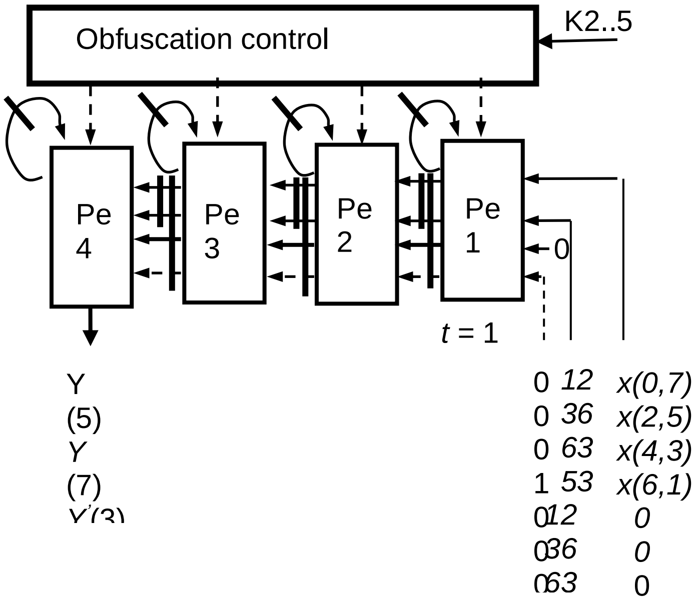
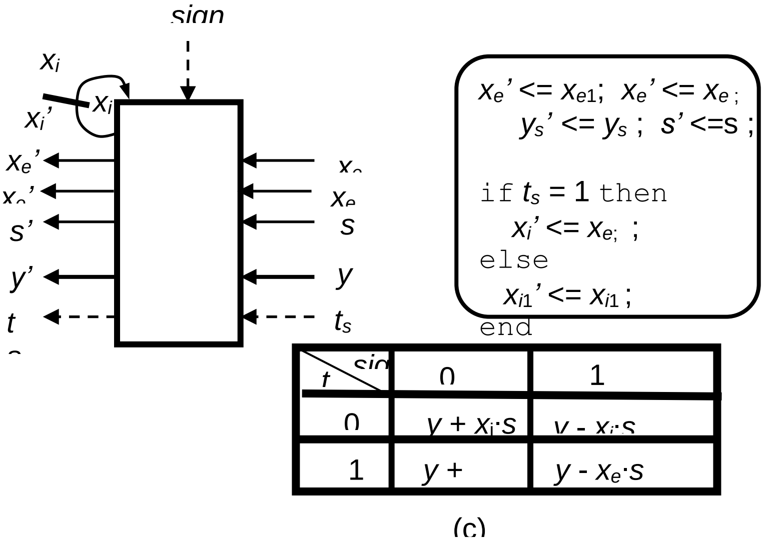


Fig. 2. The systolic array for the equation (6).



```
$x_e' <= x_{e1}$;  $x_e' <= x_e$ ;
    $y_s' <= y_s$ ;  $s' <= s$ ;

if $t_s = 1$ then
   $x_i' <= x_e$; ;
else
   $x_{i1}' <= x_{i1}$ ;
end
```

t \ sign	0	1
0	$y + x_i \cdot s$	$y - x_i \cdot s$
1	$y +$	$y - x_e \cdot s$

(c)

Fig. 3. The function of a Pe.

As can be seen in Fig.3, the data enters in the processing element PE's and is controlled by the control bit, t_s. The input sequence x(i) is stored in the corresponding PE, thus x(0,7) will be memorized in PE1, x(2,5) will be memorized in PE2, x(4,3) will be memorized in PE3 and x(6,1) will be memorized in PE4; Then they will be used to calculate one line from the computational structure presented in equation (6). The data and the coefficients are circulating at half the speed of the partial results which are circulating through the second pipeline. The control bit is used to memorize the input data is the right processor and then used for the next computations. When the control bit is 1, the data is memorized and after this the recorded data is used in the next computations.

The main advantage of the proposed solution consists in its reduced computational complexity that imply a reduced hardware complexity. Thus, as can be seen in equation (3), instead of 64 multipliers we are using in the final implementation only 7 multipliers and their complexity has been significantly reduced as they implement a multiplication with a small integer represented exactly using only 6 bits. So, the hardware complexity is significantly smaller as in [15]. Also the number of the adders can be significantly reduced using sub-expression sharing using equations (7)-(10) and (12)-(15). Moreover the proposed solution has all the advantages of using modular and regular computational structures as cycle-convolution and circular correlation in the VLSI implementation of the discrete transforms as regularity, modularity and local interconnections and also a high throughput specific to systolic arrays by using pipelining and parallelism.

Moreover, due to the specific form of the computational structure used called quasi-cycle convolution it is possible to efficiently implement a hardware security technique called obfuscation using similar ideas as presented in [16].

4. Conclusion

In this paper it is proposed an integer algorithm for the VLSI implementation of DST that allows an efficient algorithm transformation for an efficient hardware implementation based on a special computation structure. As it has been shown, the proposed algorithm has a low arithmetic complexity which leads to a low hardware complexity and high-speed performance. Moreover, due to the fact that all the coefficients used are represented using small integers that can be represented exactly using a small number of bits we can obtain an efficient implementation of multipliers. The obtained systolic array besides a small number of I/O channels, low hardware complexity and a high performance with low I/O costs, allows an efficient implementation of the obfuscation technique. The VLSI architecture proposed is modular, it has a low bandwidth and is highly regular.

References

[1] Jain A.K., *A fast Karhunen-Loeve transform for a class of random processes*, IEEE Trans. Comm., vol. COM-24, no.10, Oct.1976, p.1023-1029.

[2] White S.A., *Applications of distributed arithmetic to digital signal processing: A tutorial review*, IEEE ASSP Mag., **6**, 3, Jul.1989, p. 5-19.

[3] Kung H.T., *Why systolic architectures*, IEEE Comp., vol. 15, Jan. 1982.

[4] Meher P.K., *Systolic designs for DCT using a low-complexity concurrent convolutional formulation*, IEEE Trans. Circuits Syst. Video Technol., **16**, 9, 2006, p. 1041–1050.

[5] Chiper D.F., Swamy M.N.S., Ahmad M.O., *An Efficient Unified Framework for the VLSI Implementation of a Prime-Length DCT/IDCT with High Throughput*, IEEE Transactions on Signal Processing, Regular Papers, **54**, 6, June 2007.

[6] Chiper D.F., Swamy M.N.S. and Ahmad M.O., *An efficient systolic array algorithm for the VLSI implementation of prime-length DHT*, in Proc. of Int. Symp. on Signals, Circuits and Systems (ISSCS2005), vol. 1, Jul. 2005, p. 167-169.

[7] Cheng C. and Parhi K. K., *Hardware efficient fast DCT based on novel cyclic convolution structures*, IEEE Trans. Signal Processing, **54**, 11, Nov. 2006, p. 4419–4434.

[8] Chiper D.F.,B*A novel VLSI DHT algorithm for a highly modular and parallel architecture*, IEEE Transactions on Circuits and Systems- II, **60**, 5, 2013, p. 282-286.

[9] Chiper D.F., Ungureanu P., *Novel VLSI Algorithm and Architecture with Good Quantization Properties for a High-Throughput Area Efficient Systolic Array Implementation of DCT*, EURASIP Journal on Advances in Signal Processing, 2011.

[10] Xie J., Meher P.K., He J., *Hardware efficient realization of prime-length DCT based on distributed arithmetic*, IEEE Trans. On Computers, **62**, 6, 2013, p. 1170-1178.

[11] Chiper D.F., *A VLSI Algorithm for a Systolic Array VLSI Implementation of Type IV DST Based on A Pseudo-Band Correlation Structure*, Proc. of Int. IEEE Symp. on Circuits and Systems, ISSCS 2011, Iasi, 2011.

[12] Chiper D.F., *A New VLSI algorithm and Architecture for the hardware implementation of type IV discrete cosine transform using a pseudo-band correlation structure,* Central European Journal of Computer Science, **1**, 2, 2011, p. 90-97.

[13] Chiper D.F., Cracan A., Burdia D., *A New Systolic Array Algorithm and Architecture for the VLSI Implementation of IDST Based on a Pseudo-Band Correlation Structure*, Advances in Electrican and Computer Engineering, **1**, January 2017.

[14] Sullivan G. J., Meeting Report for 26th VCEG Meeting, ITU-T SG16/Q6 document VCEG-Z01, Apr. 2005.

[15] Chiper D.F., Cotorobai L.T., *A Low Complexity Algorithm for the VLSI Implementation of DST based on Band-Correlation Structures*, Proc. of Int. IEEE Symp. on Circuits and Systems, ISSCS 2019, Iasi, 2019.

[16] Chiper D.F., Cotorobai L.T., *A New Approach for a Unified Architecture for Type IV DCT/DST with an Efficient Incorporation of Obfuscation Technique,* Electronics, **10**, 14, **2021**.

[17] Chiper D.F., Cotorobai L.T., *A Low Complexity Algorithm for the VLSI Implementation of DST based on Band-Correlation Structures*, Proc. of Int. IEEE Symp. on Circuits and Systems, ISSCS 2019, Iasi, 2019.