FUZZY PERFORMANCE ANALYSIS OF NTT BASED CONVOLUTION USING RECONFIGURABLE DEVICE

[1]Dr.N.Anitha, [2]V.Lambodharan, [3]P.Arunkumar
[1]Assistant Professor, [2]Assistant Professor, [3]Assistant Professor
[1]Department of Mathematics,
[1] Periyar University, P.G Extension Centre , Dharmapuri, India

Abstract : This paper presents the convolution operation based on the Number Theoretic Transfom for two n=8 input sequences. The convolution of two n-point sequences using Fast Fourier Transform exhibits design complexity leading to high power consumption. The Number Theoretic Transform utilizes the matrix of modulus values to evaluate the convolution. The Number Theoretic Transform is as an integer transform which makes the design comparatively simple. The convolution based Number Theoretic Transform is developed using the Very High Speed Integrated Circuit Hardware Description language. Also the real time implementation of the proposed method is validated by the Xilinx Spartan FPGA family devices. The performance analysis of power, speed and area are evaluated and compared with 3A DSP FPGA and Virtex 6 FPGA devices.

IndexTerms **- Convolution, Number Theoretic Transform, VHDL, Xilinx Spartan FPGA.**

I. INTRODUCTION

The convolution is a mathematical operation between two functions to generate the third function. Depending on the type of signal, the convolution can be classified as discrete and analog. The discrete convolution is used more predominantly compared to the analog convolution due to high precision, high performance and easy debugging. The convolution is classified as linear and circular convolution depending on the periodicity of the signal. Gradually; the circular convolution got evolved for its faster operation. The circular convolution uses finite number of inputs in operations. The convolution could be performed by several methods like sectioned convolution, graphical convolution, fast louder transform and vedic multiplication algorithm[1].

Modern day applications such as signal and image processing, acoustics, electrical engineering demand faster convolution algorithm. By making use of Fast Fourier Transform (FFT), the convolution is converted to ordinary multiplication of the input sequence. As the FFT includes complexity in the design and high power consumption, the Number Theoretic Transform (NTT) is utilized.

The Number Theoretic Transform (NTT) is a finite integer convolution algorithm. In NTT, the complex FFT algorithms with the twiddle factors are replaced with the modulus operation. The NTT can be effectively used in the lossless medical image transmission by water marking approach [2]. The NTT's effectiveness has been proven in the images lossless transmission and in convolution fast calculation [3] The NTT combined with lattice based cryptosystems performs cyclic, mega cyclic and convolutions in encrypted domain[4].NTT algorithm are improvised for the float value transforms for Fourier, Hartley, Sine and Cosine signals [5]

This paper proposes the design of convolution based on NTT algorithm using the VHDL coding. The VHDL coding of the FFT based convolution is time consuming in design and occupies more number of multipliers and adders. By utilizing the NTT algorithm, the VHDL design is simple and thus easily downloadable in the FPGAs. The FPGA more advantages than other digital controllers in high speed operation, low power consumption, parallel processing and reconfigurable design. The convolution neural network based on FPGA is effectively used in image identification [6].The FPGA accelerator for the 3D convolution design aides to avoid the loading repetition of the processing feature maps[7]. The performance of deep convolution neural network is 1.9 to 250 times faster by utilizing FPGA device[2][8].

The real time implementation of the convolution based on NTT algorithms evaluated by using the FPGA devices namely Xilinx Spartan 3A DSP FPGA and Xilinx Virtex 6 FPGA. The next section discuss on the convolution based NTT algorithm preceded by the FPGA based design flow of the proposed method.

II. THE PROPOSED CONVOLUTION METHOD

The convolution of two sequences of length N = 8 is performed using the NTT algorithm. The NTT algorithm uses the modulus function for the evaluation of the FFT. The procedure for the NTT algorithm is as follows.

i. The order of the sequence (n) for the FFT is specifies as non-negative integer.

ii. The modulus M is chosen such that every value of the input sequence is within range of 0 to M.

iii. The formula for the working module in the NTT algorithm is given by

N = kn+1 (1) Where k is an integer > 1, n is the order of the sequence.

Note: The N value generated using this formula should be a prime number using the Dirichlet's Theorem.

iv. For the n-point DFT, the primitive nth root of unity. This is compensated in the NTT algorithm by using Euler's Theorem defined as

$\omega = g^k \bmod N$ (2)

Where g is the generator

The value of the generator "g" is selected by using following conditions:

a) The value of g is assumed to be say a.

b) The prime number N is considered as N-1 and factorise as two product values say x and y.

c) Now the generator "a" is found bychecking for the following

- $a^{N-1} \bmod M=1$ (3)
- $a^x \bmod M \neq 1$ and $a^y \bmod M \neq 1$ (4)

v. After finalising with the values of N, M and a; the convolution based on NNT algorithm is evaluated

vi. The two n sequences are fed in through the 8X8 matrices. The 8X8 matrices of the NTT algorithm is given below

$$\begin{pmatrix} (W_8^0)^0 & \cdots & (W_8^0)^7 \\ \vdots & \ddots & \vdots \\ (W_8^7)^0 & \cdots & (W_8^7)^7 \end{pmatrix}$$

vii. The FFT manipulated values are multiplied for the evaluation of the 8 point values which is again fed the IFFT based NTT algorithm using the following 8X8 matrices as shown below

$$\begin{pmatrix} (W_8^0)^{-0} & \cdots & (W_8^0)^{-7} \\ \vdots & \ddots & \vdots \\ (W_8^7)^{-0} & \cdots & (W_8^7)^{-7} \end{pmatrix}$$

vii. The convoluted output of the 8 point input sequences are acquired.

viii. The block diagram for the proposed NTT method is shown in Fig.1

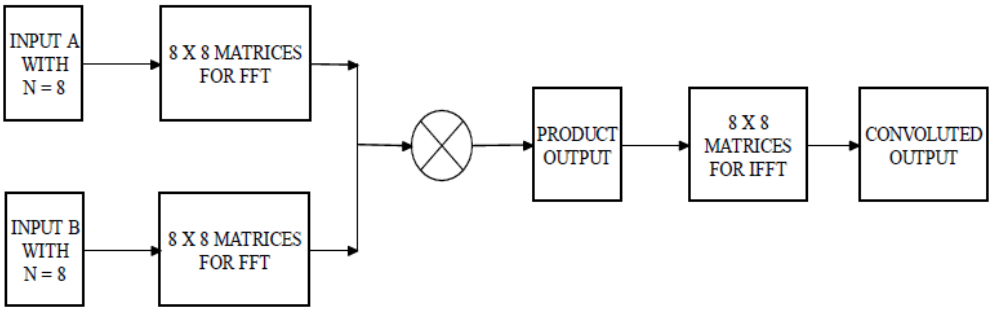

Fig.1: Block diagram of the Number Theoretic Transform with sequence n=8

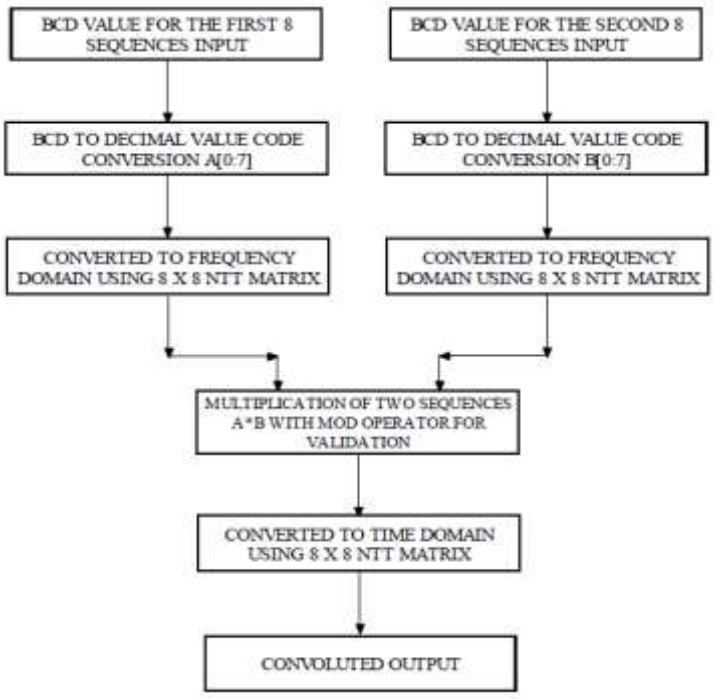

Fig. 2: FPGA Design flow of the propose convolution method

The FPGA design flow of the proposed method is depicted in Fig.2.The inputs are fed in the BCD format, as the inputs could be assigned to the IO pins in real time FPGA implementation. The BCD of the two 8 sequences are converted into the integer values using the BCD to decimal code converter. The two 8 integer values are converted to frequency domain equivalence by using the 8X8 NTT matrices. The NTT matrix is framed considering the modulus function as equivalent to the twiddle factors of the FFT

algorithm. The two frequency converted 8 sequences are multiplied and operated with the mod operator to make sure that the value is not greater than the value of modulus value M. The product obtained has to be converted back to time domain using INTT matrix. The INTT is performed on the obtained 8 integer value using the 8X8 NNT inverse matrices multiplied with the n-1 mod M to yield the desired output. The VHDL code of the proposed convolution method involves the structure style of modelling.

III. RESULTS AND DISCUSSION

In this work, the inputs values for the two input sequences are verified with three different combinations. The prime number 673 is fixed as the modulus value 'M'. The generator value is assumed as W=326. The first set of two inputs say x={4,1,4,2,1,3,5,6} and y={6,1,8,0,3,3,9,8} assigned to the proposed convolution based NTT algorithm gives the result of convolution of (x*y)={123,120,106,92,139,144,140,124}.

The second set of two inputs are assigned as x={4,3,2,1,0,0,0,0} and y={8,7,6,5,0,0,0,0} to given the convoluted result as {32,52,61,60,34,16,5,0}. Similarly for the third set of two inputs x={1,1,2,2,3,3,4,4} and y={5,5,6,6,7,7,8,8}, the convoluted output is given as {126,132,134,136,134,132,126,120}.

Fig.3 shows the simulated output for the three different input sets using the proposed convolution based on NTT algorithm using the ModelSim software. The real time implementation of the proposed method is performed using the Xilinx Spartan family devices like 3A DSP FPGA and Virtex 6 FPGA. The RTL view with the detailed schematic of the propose method in depicted in the Fig.4.

The area analysis of the proposed method using Xilinx Spartan 3A DSP and Virtex 6 FPGA are presented in Table 1&2 respectively. The area utilization of the proposed method is low for the Virtex 6 FPGA.

The performance of the power holds good for the Xilinx Spartan 3A DSP FPGA as proven by comparing the Tables 3 & 4. The timing analysis of the proposed method using the FPGA is presented in Table 5.

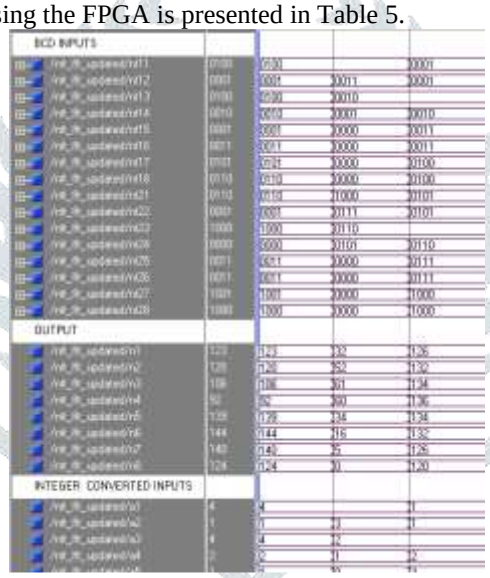

Fig. 3: Simulation output of the NTT algorithm using the MODELSIM software

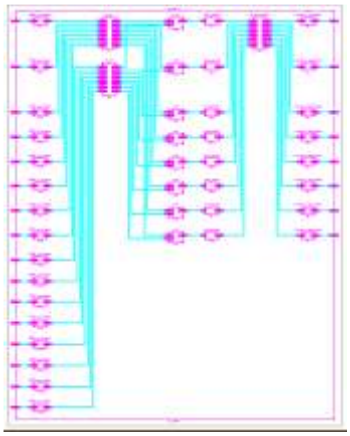

Fig. 4: RTL view with detailed schematic view of the proposed convolution based on NTT algorithm using the Xilinx Spartan FPGA device

Table 1 Device Utilization chart of the propose method using the Xilinx Spartan 3A DSP FPGA

Device Utilization Summary			
Logic Utilization	**Used**	**Available**	**Utilization**
Number of Slice Latches	64	33,280	1%
Number of 4 input LUTs	1,806	33,280	5%
Number of occupied Slices	1,080	16,640	6%
Number of Slices containing only related logic	1,080	1,080	100%
Total Number of 4 input LUTs	1,900	33,280	5%
Number used as logic	1,806		
Number used as a route-thru	94		
Number of bonded IOBs	320	519	61%
Number of DSP48As	40	84	47%
Average Fanout of Non-Clock Nets	1.86		

Table 2 Device Utilization chart of the propose method using the Xilinx Virtex 6 FPGA

Device Utilization Summary			
Slice Logic Utilization	**Used**	**Available**	**Utilization**
Number of Slice Registers	190	301,440	1%
Number of Slice LUTs	1,691	150,720	1%
Number of occupied Slices	630	37,680	1%
Number of LUT Flip Flop pairs used	1,691		
Number with an unused Flip Flop	1,501	1,691	88%
Number with an unused LUT	0	1,691	0%
Number of fully used LUT-FF pairs	190	1,691	11%
Number of unique control sets	64		
Number of slice register sites lost to control set restrictions	448	301,440	1%
Number of bonded IOBs	320	600	53%
Number of DSP48E1s	36	768	4%
Average Fanout of Non-Clock Nets	2.29		

Table 3 Power Analysis of the proposed method using the Xilinx Spartan 3A DSP FPGA

Table 4 Power Analysis of the proposed method using the Xilinx Virtex 6 FPGA

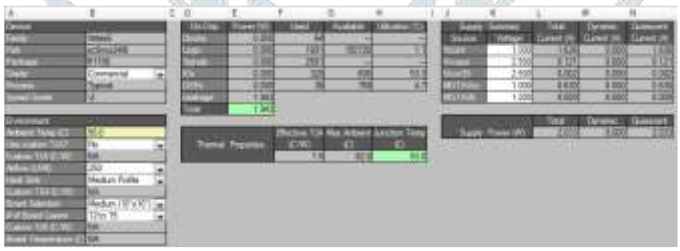

Table 5 Timing Analysis of the proposed method using the Xilinx FPGA devices

Methods	SPARTAN 3A DSP	VIRTEX 6
Max Delay	2.852ns	1.214ns
Number of paths	10	8
Number of destination ports	4	1
Memory Utilized	306696 KB	350460 KB
Total Real Time to MAP	6 sec	13sec
Total Real Time to PAR	1 min 10 sec	1 min 35 sec

IV. CONCLUSIONS

The design of convolution based NTT is developed and executed using the VHDL coding. The real time validation using the FPGA for the proposed method seems to be satisfactory. The power and area hold good for the Xilinx Spartan 3A DSP FPGA. The Xilinx Virtex 6 FPGA proves to be fast in operation with the maximum delay of 1.214ns. The extension of this work could be performed with the floating point multiplication using NTT algorithm.

REFERENCES

[1] R. Nagaraju, T. Chandra Prakash, A. Venkateshwarlu, "A Novel High Speed Convolution and De-convolutionAlgorithm Implementation Based on Ancient Indian Vedic Mathematics", International Journal of VLSI systems and Communication systems, vol.3, no.4, July 2015, pp: 514-517.
[2]RaghidMorcel, MazenEzzeddine, HaithamAkkary, "FPGA-Based Accelerator for Deep Convolutional Neural Networks for the SPARK Environment", 2016 IEEE International Conference on Smart Cloud (SmartCloud), Nov 2016, DOI: 10.1109/SmartCloud.2016.31.
[3]LamriLaouamer, "Towards a robust and fully reversible image watermarking framework based on number theoretic transform", International Journal of Signal and Imaging Systems Engineering, vol.10, no.4, April 2017, pp.169 - 177
[4]Alberto Pedrouzo-Ulloa, Juan Ram´onTroncoso-Pastoriza, and Fernando Pérez-González, "Number Theoretic Transforms for SecureSignal Processing" , IEEE Transactions on Information Forensics And Security, vol. 12, no. 5, May 2017, pp: 1125-1140.
[5]Paulo Hugo E. S. Lima, Juliano B. Lima and Ricardo M. Campello de Souza, "Fractional Fourier, Hartley, Cosine and Sine Number-Theoretic Transforms Based on Matrix Functions", Circuits, Systems, and Signal Processing, vol.36, no.7, July 2017, pp 2893–2916.
[6]CongyiLyu, Haoyao Chen, Xin Jiang, Peng Liand Yunhui Liu, "Real-time object tracking system basedon field-programmable gate arrayand convolution neural network", International Journal of AdvancedRobotic Systems,Special Issue,Feb 2017, pp:1–14.
[7] Hai Wang, Mengjun Shao, Yan Liu, and Wei Zhao, "Enhanced Efficiency 3D Convolution Based on Optimal FPGA Accelerator", IEEE Access, vol.5, April 2017, pp: 6909-6916
[8]Mohammad Motamedi ,Philipp Gysel, and VenkateshAkella"Design space exploration of FPGA-based Deep Convolutional Neural Networks",Design Automation Conference (ASP-DAC), 2016 21st Asia and South Pacific, Mar 2016, DOI: 10.1109/ASPDAC.2016.7428073.