International Journal of Scientific Research & Engineering Trends
Volume 7, Issue 2, March-April-2021, ISSN (Online): 2395-566X

Systematic Perusal of Volder's Algorithm in Lifescience

Asst. Prof. /HOD Ramya. R, Asst. Prof. Sahaya Reshma. M, Gayathri. R, Parkavi. G, Rakshitha. R
Department of ECE,
K.S.K College of Engineering and Technology, Darasuram,
Thanjavur, Tamil Nadu, India.
Chanmeya.17@gmail.com, Msr.ece33@gmail.com, rakshitharamanathan@gmail.com

***Abstract*- In medical field, ICA plays an important role. This system reduce the power consumption and memory using Modular multiplication. The proposed approach reduce the circuit area in separating the super-Gaussian source signals. Efficient hardware architectures for modular multiplication, modular inversion, unified point addition, and modular multiplication are proposed. In this system aims to design and implement a very large scale integration [VLSI] chip of the extend Infomax ICA algorithm. Further more, the measurement results show the ICA core can be successfully applied to get output within a minutes.**

***Keywords*- Cordic (or) volder's algorithm,radix core modular multiplication ,super-gaussian signal analyzer.**

I. INTRODUCTION

Our life has been largely shaped by the exciting developments of modern electronic technologies, such as pervasive and ubiquitous computing, ambient intelligence, communication, and Internet. Today micro-electronic products are influencing the ways of communication, learning and entertainment. The key driving force for the developments during decades is the VLSI technologies where complex applications are integrated onto single chips. Not only functionally enriched, these products such as mobile phones, notebooks and personal handheld sets are becoming faster, smaller-in-size, larger-in-capacity, lighter-in weight, lower-in-power-consumption. One could favorably think that this trend will persistently continue.

Following this trend, we could integrate more and more complex applications and even systems onto a single chip. However, our current methodologies for VLSI design and integration do not evenly advance due to the big challenges confronted.In early days of VLSI design, signal integrity effects such as interconnect delay, crosstalk, inter-symbol interference, substrate coupling, transmission-line effects, etc. were negligible due to relatively slow clock speed and low integration density. Chip interconnect was reliable and robust.

Today signal and power integrity analysis is as important as timing, area and power analysis. Predominating digital IC designs have been following a globally synchronous design style where a global clock tree is distributed on the chip, and logic blocks function synchronously. However, this style is unlikely to survive with future wire interconnect. The reason is that technology scaling does not treat wire delay and gate delay equally. While gate delay (transistor switching time) has been getting dramatically smaller in proportion to the gate length, wires have slowed down.

II. ICA ARCHITECTURE

Independent component analysis (ICA) is the most popular technique developed to solve the blind source separation (BSS) problem. Under the assumption of signal independence across sources, the task of BSS and ICA is to separate and recover independent source signals from linear or nonlinear mixed sensor observations, in which both sources and the unmixing matrix are unknown. ICA not only decorrelates the signals that are of second-order statistics using a minimum of a priori information but also reduces higher order statistical dependencies between reconstructed signals. This principle has been used in other applications, such as recognition and hyper spectral image analysis.

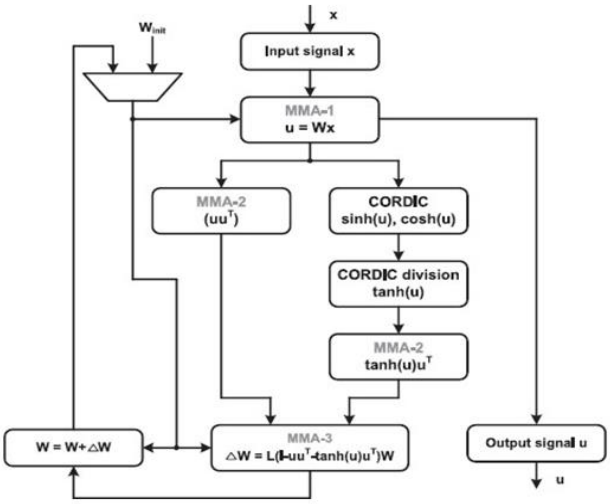


Fig 1. Architecture of ICA.

Many ICA algorithms are slow processes in signal/image processing applications due to the complicated arithmetics as well as the time-consuming iterative computation. VLSI

© 2021 IJSRET

is an ideal algorithm implementation carrier and offers many features such as high processing speed, which is extremely desired in ICA implementations.

The complicated arithmetics of ICA is one of the main barricades in ICA hardware implementation, especially in synthesis procedure. Therefore, hierarchy and modularity techniques in VLSI design are essential for most ICA implementations to overcome the complexity of ICA algorithms.

III. PROPOSED SYSTEM

The ICA algorithm becomes important in the field of the Digital Signal Processing (DSP), Image Processing, and Biomedical Signal Analysis, such as a lectroencephalogram (EEG), Electrocorticography (ECOG), Magnetoencephalograp hy (MEG), and Electrocardiogram (ECG) analyses. Memory plays a crucial role in designing embedded systems. Embedded systems are constrained by the available memory.A larger memory can accommodate more and large applications but increases cost, area, as well as energy requirements

1. Modular Multiplication Algorithm:
Modular multiplication hardware algorithms for a large modulus are suitable to be implemented in compact hardware. Much effort has been devoted to developing specialized hardware for computing fast modular multiplication and modular inversion separately. Many algorithms have been proposed in the literature for computing modular multiplication. Most of them use redundant number systems and perform a high-radix modular multiplication or use Residue Number System (RNS). For modular division, however, there are only a few algorithms and these are based on the Euclidean algorithm for computing GCD. Radix-4 algorithm for modular multiplication for a large modulus suitable for VLSI implementation can be used. We have accelerated

Montgomery multiplication algorithm as a radix-4 algorithm.

2. Cordic/Voldes's Process:
Coordinate Rotation DIgital Computer (CORDIC) algorithm was first developed by Jack E. Volder in 1959. CORDIC algorithm is extremely useful in efficient and effective implementation of DSP systems. This algorithm allows implementation of trigonometric functions like sine, cosine, magnitude and phase with great precision by using just simple shift and adding operations. Although the same functions can be implemented using multipliers, variable shift registers or Multiply Accumulator (MAC) units, but CORDIC can implement these functions efficiently while saving enough silicon area which is considered to be primary design criteria in VLSI technology. This paper designs first order complex DPLL using CORDIC which functions as a FSK demodulator. In digital PLL, an adjustable local sine wave generator and phase detector is required. The sine and cosine terms can be calculated using polynomial approximation, e.g. Taylor series.

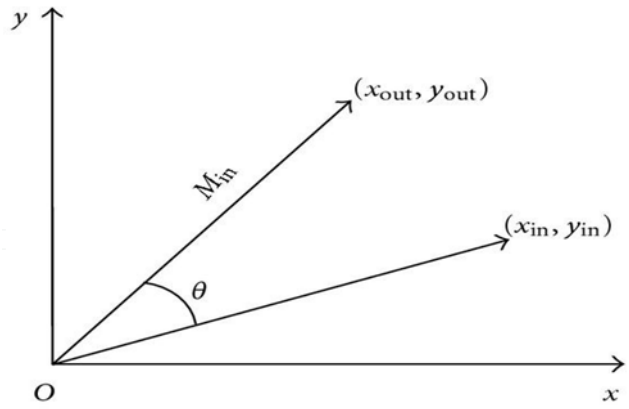


Fig 2.Two dimensional vector rotation

The coordinate rotational digital computer (CORDIC) algorithm is an iterative algorithm. It uses simple shifts and adds operations. It consists of two shift registers and three adder–subtractor along with some special Here, the rotational vector p0 [x0 y0] is rotated through an angle θ in order to obtain a rotated vector pn [xn yn].

$$x_{out} = x_{in}\cos\theta - y_{in}\sin\theta,$$
$$y_{out} = x_{in}\sin\theta + y_{in}\cos\theta \quad \textbf{(1)}$$

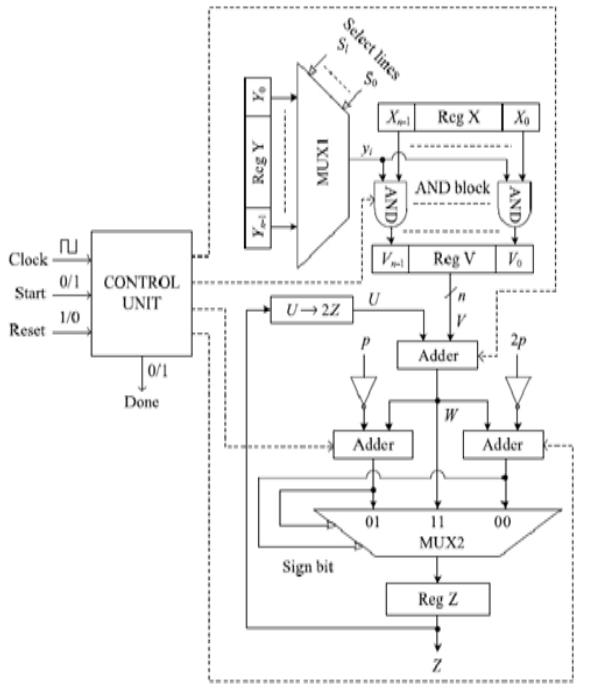
where (xin, yin) indicates the initial coordinates of the vector and (xout, yout) gives the final coordinates of the vector.

3. Modular Multiplication System:
A modular multiplier is an indispensable part of an ICA processor. The area utilization and the maximum achievable frequency of the processor entirely depend on its adopted modular multiplier. It is a major challenge in prime field ICA to develop a low-area modular multiplier without compromising the speed. Hence, optimizing modular multiplication algorithm is a crucial demand. Since the interleaved array has the good feature of resource reused, we only need to design a single unique processing element for performing the matrix multiplication computations. Therefore, the total numbers of multipliers and adders can be saved efficiently.The hardware architecture that operates iterative bitwise multiplication followed by modular reduction operations. The bitwise multiplication is started from the most significant bit (MSB) of the multiplier Y and moved towards the least significant bit (LSB) of it. The accumulator Z is doubled and computed as U at the

© 2021 IJSRET

beginning of each iteration. A total of n+1 clock cycles are required to complete this multiplication process.A major drawback of this design is that it always spends n +1 clock cycles to accomplish single modular multiplication even if the multiplier Y is of less than n bits in size. The multiplier Y is bitwise multiplied with the multiplicand X and the partial product yiX is stored in register V (Reg V). The *h* bit of Y is selected by multiplexer MUX1 and the multiplication yiX is performed by n number of 2- input AND gates. U is added to V and the addition is reduced to modulo p in every iteration.The modular reduction is performed by subtracting the prime number p and 2p from W.Multiplexer MUX2 is used to store one of the three outputs W; W -p; and W -2p into register Z (Reg Z). The basic idea of interleaved modular multiplication is multiply by 2 and add operations followed by modular reduction in a repeated manner.

The modular multiplication of the multiplicand X and the multiplier Y over GF(p) is given bythe general expression. Many algorithms have been proposed in the literature for computing modular multiplication. Most of them use redundant number systems and perform a high-radix modular multiplication or use Residue Number System (RNS).



$$Z = X \cdot Y \bmod p$$
$$= y_0 \cdot (2^0 X) + y_1 \cdot (2^1 X) + \ldots + y_n \cdot (2^n X) \bmod p$$
$$= \sum_{i=0}^{n-1} y_i \cdot (2^i X) \bmod p,$$

where p is a prime number, X and Y are two integers such that $X, Y \in [1, p-1]$, and n is the length of the integers.

Fig 3.Proposed Modular multiplication system

This principle has been used in other applications, such as recognition and hyper spectral image analysis. Many ICA algorithms are slow processes in signal/image processing applications due to the complicated arithmetics as well as the time-consuming iterative computation. VLSI is an ideal algorithm implementation carrier and offers many features such as high processing speed, which is extremely desired in ICA implementations.

4. Software Requirements Simulation:

Xilinx ISE (Integrated Synthesis Environment) is a software tool produced by Xilinx for synthesis and analysis of HDL designs, enabling the developer to synthesize ("compile") their designs, perform timing analysis, examine RTL diagrams, simulate a design's reaction to differrent stimuli, and configure the target device with the programmer.Xilinx ISE is a design environment for FPGA products from Xilinx, and is tightly-coupled to the architecture of such chips, and cannot be used with FPGA products from other vendors.

The Xilinx ISE is primarily used for circuit synthesis and design, while ISIM or the ModelSim logic simulator is used for system-level testing. Other components shipped with the Xilinx ISE include the Embedded Development Kit (EDK), a Software Development Kit (SDK) and ChipScope Pro.Since 2012, Xilinx ISE has been discontinued in favor of

Vivado Design Suite, that serves the same roles as ISE with additional features for system on a chip development. Xilinx released the last version of ISE in October 2013, and states that "ISE has moved into the sustaining phase of its product life cycle, and there are no more planned ISE releases.

ModelSim or ISIM may be used to perform the following types of simulations:

- Logical verification, to ensure the module produces expected results
- Behavioral verification, to verify logical and timing issues
- Post-place & route simulation, to verify behavior after placement of the module within the reconfigurable logic of the FPGA

5. Field Programmable Gate Array:

A field-programmable gate array (FPGA) is an integrated circuit designed to be configured by a customer or a designer after manufacturing–hence the term "field-programmable". The FPGA configuration is generally specified using a hardware description language (HDL), similar to that used for an application-specific application for integrated circuit (ASIC).

Circuit diagrams were previously used to specify the configuration, but this is increasingly rare due to the advent of electronic design automation tools.

© 2021 IJSRET

FPGAs contain an array of programmable logic blocks, and a hierarchy of "reconfigurable interconnects" that allow the blocks to be "wired together", like many logic gates that can be inter- wired in different configurations. Logic blocks can be configured to perform complex combinational functions, that or merely simple logic gates like AND and XOR.

Fig 4. Stratix IV FPGA from Altera

In most FPGAs, logic blocks also include memory elements, which may be simple flip-flops or more complete blocks of memory. Many FPGAs can be reprogrammed to implement different logic functions, allowing flexible reconfigurable computing as performed in computer software.

Fig 5.Spartan FPGA from Xilinx

IV. CONCLUSION

This paper presented a VLSI implementation of ICA algorithm with modular multiplication approach. In the proposed ICA chip, a modular multiplication approach operates large dimension matrix multiplications and the CORDIC engine is employed to execute hyperbolic functions and division operation so the ICA algorithm can be effectively and efficiently realized.

Both the numerical experimental and the measured results demonstrated that the proposed ICA chip achieved a low-area, high-speed, and low-power design. The mixed medical signals can be successfully separated into independent source signals through the proposed ICA chip with over 95% factor of similarity for each reconstructed source signal

REFERENCE

[1] Jinnan Ding; Shuguo Li, 2020, “A Low-Latency and Low-Cost Montgomery Modular Multiplier Based on NLP Multiplication”, IEEE Transactions on Circuits and Systems II: Express Briefs, Vol: 67, No: 7, pp: 1319 – 1323.

[2] Jinnan Ding; Shuguo Li, 2018, “A Modular Multiplier Implemented With Truncated Multiplication”, IEEE Transactions on Circuits and Systems II: Express Briefs, Vol: 65, No: 11, pp: 1713 – 1717.

[3] Ling-Yu Yeh; Po-Jen Chen;Chen-Chun Pai; Tsung-Te Liu, 2020, “An Energy-Efficient Dual- Field Elliptic Curve Cryptography Processor for Internet of Things Applications”, IEEE Transactions on Circuits and Systems II: Express Briefs, Vol: 67, No: 9, pp: 1614 – 1618.

[4] Zhe Liu; Johann Großschädl; Zhi Hu; Kimmo Järvinen; Husen Wang; Ingrid Verbauwhede, 2017, “Elliptic Curve Cryptography with Efficiently Computable Endomorphisms and Its Hardware Implementations for the Internet of Things”, IEEE Transactions on Computers, Vol: 66, No: 5, pp: 773 –

[5] Bing Li; Bingjie Lei; Yunlong Zhang; Shaochong Lei, 2019, “A Novel and High-Performance Modular Square Scheme for Cryptography Over GF”, IEEE Transactions on Circuits and Systems II: Express Briefs, Vol: 66, No: 4, pp: 647 – 651.

[6] Gabriel Gallin; Arnaud Tisserand, 2019, “Generation of Finely-Pipelined GF(PP) Multipliers for Flexible Curve Based Cryptography on FPGAs”, IEEE Transactions on Computer, Vol: 68, No: 11, pp: 1612 – 1622.

[7] Jinlin Zhu; Zhiqiang Ge; Zhihuan Song, 2017, “Non-Gaussian Industrial Process Monitoring With Probabilistic Independent Component Analysis”, IEEE Transactions on Automation Science and Engineering, Vol: 14, No: 2, pp: 1309 – 1319.

[8] Weiqiang Liu; Liangyu Qian; Chenghua Wang; Honglan Jiang; Jie Han; Fabrizio Lombardi, 2017,

© 2021 IJSRET

"Design of Approximate Radix-4 Booth Multipliers for Error-Tolerant Computing", IEEE Transactions on Computers, Vol: 66, No: 8, pp: 1435 – 1441.

[9] Duncan J. M. Moss;David Boland; Philip H. W. Leong, 2019, "A Two-Speed, Radix-4, Serial–Parallel Multiplier", IEEE Transactions on Very Large Scale Integration (VLSI) Systems, Vol: 27, No: 4, pp: 769 – 777.

[10] Shuning Zhang; Wei Xie; Hang Zhu; Huichang Zhao, 2017, "Combined Eigenvector Analysis and Independent Component Analysis For Multi-Component Periodic Interferences Suppression In PRCPM-PD Detection System", IEEE Access, Vol: 5, pp: 12552 – 12562.

[11] Yun Feng; Han-Xiong Li, 2020, "Dynamic Spatial-Independent-Component-Analysis-BasedAbnormality Localization for Distributed Parameter Systems", IEEE Transactions on Industrial Informatics, Vol: 16, No: 5, pp: 2929 – 2936.

[12] Gopal Raut; Shubham Rai; Santosh Kumar Vishvakarma; Akash Kumar, 2021, "RECON: Resource-Efficient CORDIC-Based Neuron Architecture", IEEE Open Journal of Circuits and Systems, Vol: 2, pp: 170 – 181.

[13] Ching-Iang Li; Gwo-Dong Chen; Tze-Yun Sung; Huai-Fang Tsai, 2019, "Design and Implementation of Smart Multi-Touch Interface Using Special Purpose CORDIC Processor", IEEE Transactions on Consumer Electronics, Vol: 65, No: 4, pp: 516 – 525.

© 2021 IJSRET