Application of Residue Arithmetic in Communication and Signal Processing

by

Pallab Maji
Roll No. # 209EC1109

A Thesis submitted for partial fulfilment for the degree of

Master of Technology

in

Electronics and Communication Engineering

Spcl: Telematics and Signal Processing

Dept. Electronics and Communication Engineering
NATIONAL INSTITUTE OF TECHNOLOGY
Rourkela, Orissa-769008, India

June 2011

Application of Residue Arithmetic in Communication and Signal Processing

by

Pallab Maji
Roll No. # 209EC1109

A Thesis submitted for partial fulfilment for the degree of
Master of Technology
in
Electronics and Communication Engineering
Spcl: Telematics and Signal Processing
Under the Supervision of

Prof. (Dr.) Girija Sankar Rath

Dept. Electronics and Communication Engineering
National Institute of Technology, Rourkela,
Orissa-769008, India

June 2011

Dedicated

to

my niece

Pauli Maji

National Institute of Technology

Rourkela

CERTIFICATE

This is to certify that the thesis entitled, **"Application of Residue Arithmetic in Communication and Signal Processing "** submitted by **Pallab Maji** in partial fulfillment of the requirements for the award of Master of Technology Degree in **Electronics & Communication Engineering** with specialization in **Telematics and Signal Processing** during 2010-2011 at the National Institute of Technology, Rourkela (Deemed University) is an authentic work carried out by him under my supervision and guidance.

To the best of my knowledge, the matter embodied in the thesis has not been submitted to any other University / Institute for the award of any Degree or Diploma.

27.05.2011

Date

Prof. (Dr.) Girija Sankar Rath

Dept. of Electronics & Communication Engg.

National Institute of Technology

Rourkela-769008

Orissa, India

Acknowledgements

This dissertation would not have been possible without the guidance and the help of several individuals who in one way or another contributed and extended their valuable assistance in course of this study.

My utmost gratitude to Prof. Girija Sankar Rath, my dissertation adviser whose sincerity and encouragement I will never forget. Prof. Rath has been my inspiration as I hurdle all the obstacles in the completion this research work and has supported me throughout my project with patience and knowledge whilst allowing me the room to work in my own paradigms.

Sincere thanks to Prof. S. K. Patra, Prof. K. K. Mahapatra, Prof. Samit Ari, Prof. S. K. Das, Prof. S. K. Behera, Prof. S. Meher, Prof. A. K. Sahoo and Prof. Poonam Singh for their constant cooperation and encouragement through out the course.

I also extend my thanks to entire faculty of Dept. of Electronics and Communication Engineering, National Institute of Technology Rourkela, Rourkela who have encouraged me throughout the course of Master's Degree.

I would like to thank all my friends, especially Ashish Agarwal, Kapil Parmar, Sanjay Meena, Sujeet Rai, Vaibhab Raj, Dipanjan Bhadra, Prasun Bhattacharya and Venkatesh S. for their help during the course of this work. I also thank all my classmates for all the thoughtful and mind stimulating discussions we had, which prompted us to think beyond the obvious. I take immense pleasure to thank our seniors namely, Runa Kumari, Yogesh Kumar

Choukiker, Senthilnathan Natarajmani for their endless support in solving queries and advices for betterment of dissertation work. I would also take this opportunity to thank Mr. Prasanta Pradhan, Mr. Bijay Muni, Mr. Ayaskanta Swain and Mr. Jaganath Mohanty for their support during this dissertation.

And finally thanks to my parents, my brother, sister-in-law and Roshni Hazra, whose faith, patience and teaching had always inspired me to walk upright in my life. Without all these beautiful people my world would have been an empty place.

Pallab Maji
pallab.m86@gmail.com

Abstract

Residue Number System (RNS) is a non-weighted number system. In RNS, the arithmetic operations are split into smaller parallel operations which are independent of each other. There is no carry propagation between these operations. Hence devices operating in this principle inherit property of high speed and low power consumption. But this property makes overflow detection is very difficult. Hence the moduli set is chosen such that there is no carry generated. In this thesis, the use of residue number system (RNS) is portrayed in designing solution to various applications of Communication and Signal Processing. RNS finds its application where integer arithmetic is authoritative process, since residue arithmetic operates efficiently on integers. New moduli set selection process, magnitude comparison routine and sign detection methods were limed on the onset of this dissertation.

A good example of integer arithmetic is digital image. The pixels are represented by 8 bit unsigned number. Thus the operations are primarily unsigned and restricted to a small range. Hereby, in this thesis, a novel image encryption technique is depicted. The results show the robustness and timeliness of this technique. This technique is further compared to some of industry standard encryption algorithms for analysis based on robustness, encryption time and various other paradigms.

Filters are signal conditioners. Each filter functions by accepting an input signal, blocking pre-specified frequency components, and passing the original signal minus those components to the output. A lowpass filter allows only low frequency signals (below some specified cutoff) through to its output, so it can be used to eliminate high frequencies. A novel design approach for a low pass

filter based on residue arithmetic was also proposed. Some trite techniques as well as novel approaches were adopted to solve the design challenges. A technique for mapping the data in another space providing the liberty to work with floating numbers with a precision was adopted.

PN sequence generator based on residue arithmetic is also formulated. This algorithm generates a pseudo-noise sequence which further was used to evince a spread spectrum multiuser communication system. The results are compared with trite techniques like Gold and Kasami sequence generators.

Contents

List of Figures

List of Tables

List of Acronyms

RNS	Residue Number System
CRT	Chinese Remainder Theorem
DAC	Digital to Analog Converter
ADC	Analog to Digital Converter
DSP	Digital Signal Processor
CDMA	Code Division Multiple Access
PN	Pseudo Noise
NCRT	New Chinese Remainder Theorem
BER	Bit Error Rate
SS	Spread Spectrum
DS-SS	Direct Sequence Spread Spectrum
SNR	Signal to Noise Ratio

CHAPTER 1

Introduction

1.1 Background

The residue arithmetic basically originated from China in first century A.D. However Chinese mathematician Sun Tzu is given the due credit for giving birth to residue number system (RNS) along with Greek scholar Nichomachus and Hsin-Tai-Wei. Even though this number system is such old, not much work was done before twentieth century. Even the famous Chinese Remainder Theorem (CRT) was proved by Euler in 1734. This number system did not find much practical application until D. H. Lehmer, A. Svoboda and M. Valach designed a hardware based on residue arithmetic to reduce complex calculations in 1955. This triggered a series of research application based on RNS. Major contributions came from M. A. Soderstrand, W. K. Jenkins, W. C. Miller, R. I. Tanaka, B. L. Leon, N. Szabo and others in more than three decades since then. However they basically worked on ROM based devices. They mainly worked on Residue number scaling, RNS to binary converters, binary to RNS converters, error corrections etc. Non-Rom based devices based on RNS were designed with advent of VLSI technologies. This led to work

on special moduli sets [1].

M. A. Soderstrand basically worked on design and implementation DAC, adaptive filters, modulo adders, convolvers and digital filters. He gave implementation design for complex heterodyne tunable filters. G. A. Jullien worked extensively in developing algorithms for selection of efficient moduli for high speed DSP architectures. He gave various algorithms for selection of moduli set of three based on various applications and also proposed modified quadratic RNS. He also worked with W. C. Miller for VLSI implementation of digital filters, adders, convolvers and various DSP architectures based on RNS. They also worked with M. A. Bayoumi to develop systolic array based on RNS for various DSP algorithms. They also proposed the famous look-up table methodology for various RNS based designs [1].

However the availability of inexpensive 16-bit and 32-bit digital signal processors for extensive work on picture encoding, speech encoding and other digital processing algorithms befogged the need of residue arithmetic based processors. However, special purpose processors have been developed for various applications.

During the extensive literature survey the quest for low power designs and high speed computer engines was evident. High speed devices like adder, multipliers, ALU, accumulators were most sought after designs. The 'Break and Process' approach of RNS domain attains the increase in speed of operations with its own limitations which is described later. Nevertheless the applications in which divisions, comparisons, scaling operations are less and can be avoided, typical RNS system works satisfactorily. Thus applications like image encoding and encryption, FIR filter, spread spectrum communication systems can be designed based on Residue Arithmetic. A RNS based system generally operates on integer data. Fig. 1.1 shows a basic signal processor based on RNS.

As we learn from the fig. 1.1, the front end has an analog to digital converter and a binary to RNS converter whose k output words corresponding to k moduli will be processed by the iki parallel processors. At the very end, the k words are converted to binary number and then passed on to digital to analog converter (DAC) to get processed analog output.

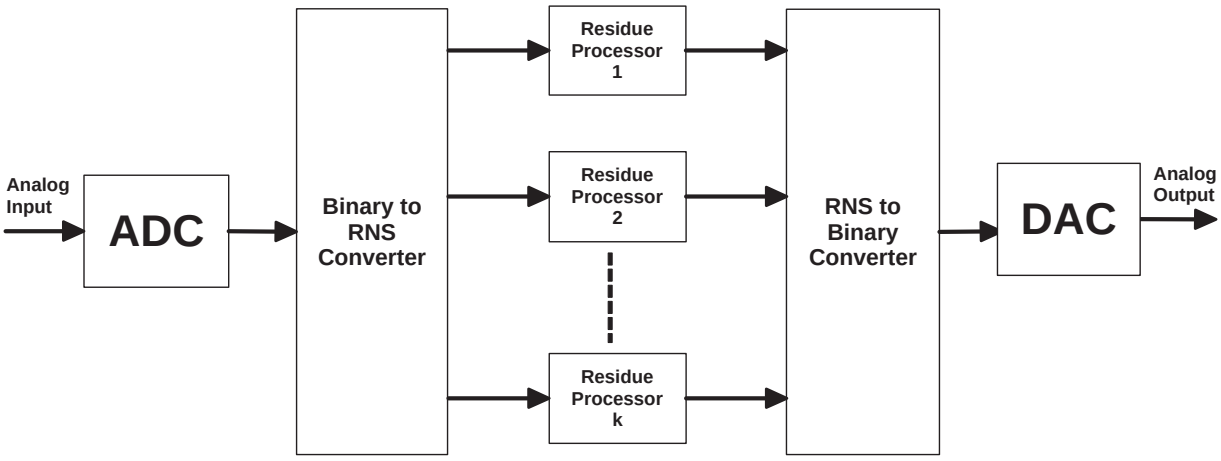


Figure 1.1: Basic RNS Based Signal Processor

1.2 Overview of RNS Applications

As described in section 1.1, RNS is mostly used in VLSI implementation of DSP architecture for achieving low power and high speed. Among the application RNS, implementation of FIR filters, IIR filters, adaptive filters, digital frequency synthesis, two dimensional filters, image encryption and coding are most significant[1].

Most significant research work in the field of RNS was done in forward and reverse conversion. Recent research on reverse converters [2; 3; 4] uses New Chinese Remainder Theorem proposed by Y. Wang[5]. One dimensional[6; 7; 8; 9] and two dimensional Discrete Wavelet Transform architecture[10] based on residue arithmetic made a crucial impact.

RNS had been effectively used in encryption and coding [11; 12]. In field of communication, RNS were introduced in field of CDMA by many researchers. Frequency hopping techniques[13], DS-CDMA[14; 15; 16; 17; 18] and PN sequence correlators[19] based on RNS were proposed and designed.

There were many programmable architectures designed based on residue arithmetic. Griffin and Taylor[20] proposed RNS based RISC architecture as future research area. H. T. Vergos in the year 2001, proposed a 200 MHz RNS core[21]. There were many im-

plementation of fast digital processors based on RNS in literature[22; 23; 24]. J. Ramirez developed a 32-bit SIMD RISC processor fully based on RNS[25].

Thus we find numerous applications of RNS in field of Communication and Signal Processing. In this thesis, some novel techniques have been proposed with reference to some trite techniques present in literature to develop some application of RNS in field of Communication and Signal Processing.

1.3 Motivation

The 'break and process' construct drives the researchers to work with residue arithmetic. This leads to 'carry-free' arithmetic operations. However operations viz. division, comparison, scaling etc. are very difficult since there is no carry propagation. But applications where these operations are not dominant and can be avoided and applications which are limned by integer arithmetic, RNS can be expended. Hereby, these facts are major stimuli to explore the potential of RNS in various fields of Communication and Signal Processing. Basics of residue arithmetic leads to complexity in magnitude calculation, sign detection and incorporation of fractional numbers. These constraints however made the implementation of ideas challenging and research worthy. Therefore the approach to digital FIR filter design was viewed from different perspective.

All digital images are represented by 8 bit unsigned pixel values; this sets perfect platform for the use of RNS in digital image processing. In this thesis, a image processing technique based on RNS is portrayed. Various techniques are present in literature for generation of PN sequences in literature. PN sequences with better autocorrelation and low cross-correlation are of prime interest in spread spectrum communication. Since the sequences are noise like and deals with random generation of series of bits [-1,1] of varied lengths, the scope of RNS based PN sequence was large. These facts, constructs and analyses were impulsive force for the research work done and this dissertation.

1.4 Thesis Organization

Chapter-1 Introduction

Chapter-2 Introduction to Residue Arithmetic

The basics of RNS and the operations of residue arithmetic and its advantages are discussed in this chapter. The famous CRT and NCRT are discussed thoroughly. The proposed problems which were approached in this dissertation are explained in detail.

Chapter-3 Moduli Selection and Mapping

In this chapter, the techniques of generation of co-prime moduli selection based on operating bits of any application are limned. There are two techniques proposed for the same. The concept of utility factor is also given as a standard solution to judge the moduli based on the bit efficiency. The concept of incorporation of fractional numbers with the aid of Homomorphic Mapping is also introduced.

Chapter-4 Application: RNS Based FIR Filter

In this chapter the first application in field of communication and signal processing is depicted. A 32-bit FIR filter based on residue arithmetic is portrayed. Results are compared to the traditional FIR filter and a compendious study is given in the end. The specifications of the filter simulated is mentioned along with the simulation environment.

Chapter-5 Application : RNS Based Image Coding

This chapter presents the basic concept image encryption and coding. A succinct study of the proposed algorithm for image encryption and comparison to industry standard encryption techniques are depicted further. The results of this comparison is tabulated and analysed. The results are compared to the industry standard BLOWFISH encryption technique and the performance analysis based on encryption time, output image quality, correlation between encrypted images with original image, entropy for the same and robustness against channel noise is chalked out in detail.

Chapter-6 Application : RNS Based PN Sequence

This chapter deals with an algorithm to generate a RNS based PN sequence.The generation of the PN sequence is based on the key provided for the secured and authentic transmission along with a set of co-prime numbers generated from the spread factor β. A compendious study comparing the generated sequence with Gold and Kasami sequence is limned further. The results are portrayed there after.

Chapter-7 Conclusion and Scope for Future Work

The overall conclusion of the thesis is presented in this chapter. It also contains some future research topics which need attention and further investigation. Application of RNS to further areas of Communication and Signal Processing are also sighted under this chapter.

CHAPTER 2

Introduction to Residue Arithmetic

Residue number systems are based on the congruence relation, which is defined as follows. Two integers, a and b are said to be congruent modulo m if m divides exactly the difference of a and b; it is common, especially in mathematics tests, to write $a \equiv b(mod\ m_i)$ to denote this. Thus, for example, $10 \equiv 7(mod\ 3)$, $10 \equiv 4(mod\ 3)$, $10 \equiv 1(mod\ 3)$ and $10 \equiv -2(mod\ 3)$. The number m is a modulus or base, and we shall assume that its values exclude unity, which produces only trivial congruences. If q and r are the quotient and remainder, respectively, of the integer division of a by m, that is, $a = q \cdot m + r$ then, by definition, we have $a \equiv r(mod\ m_i)$. The number r is said to be the residue of a with respect to m, and we shall usually denote this by $r = |a|_m$. The set of m smallest values, $0, 1, 2, 3 \cdots m-1$ that the residue may assume is called the set of least positive residues modulo m. Suppose we have a set $\{m_1, m_2 \cdots m_N\}$, of N positive and pairwise relatively prime moduli. Let M be the product of the moduli. Then every number $X < M$ has a unique representation in the residue number system, which is the set of residues $\{|X|_{m_i} : 1 \leq i \leq N\}$. A partial proof of this is as follows[1; 26].

Suppose X_1 and X_2 are two different numbers with the same *residue set*. Then

$|X_1|_{m_i} = |X_2|_{m_i}$ and so $\{|X_1 - X_2|_{m_i} = 0\}$. Therefore X_1 and X_2 is the lcm of m_i. But if the m_i are relatively prime, then their LCM is M, and it must be that X_1 and X_2 is a multiple of M. So it cannot be that $X_1 < M$ and $X_2 < M$. Therefore, the set $\{|X|_{m_i} : 1 \leq i \leq N\}$ is unique and may be taken as the representation of X. The number M is called the dynamic range of the RNS, because the number of numbers that can be represented is M. For unsigned numbers, that range is $[0, M-1]$. Representations in a system in which the moduli are not pairwise relatively prime will not be unique; two or more numbers will have the same representation.

2.1 Basics of Residue Arithmetic

Consider two numbers 43 and 29. Consider a moduli set $P = [3,5,7]$. Then RNS representation of these two numbers are as follows: $43 \rightarrow \{1,3,1\}$
$29 \rightarrow \{2,4,1\}$

2.1.1 Multiplicative Inverse

$$M_i.M_i^{-1} = 1 \ (mod \ p_i) \tag{2.1}$$

where $M_i = \frac{R}{p_i}$. Thus for the above case, $R = 3 \times 5 \times 7 = 105$ and $M_1 = 35$, $M_2 = 21$ and $M_3 = 15$. Hence $M_1^{-1} = 2$, $M_3^{-1} = 1$ and $M_3^{-1} = 1$.

2.1.2 Reverse Conversion

$$\sum_{i=0}^{k} \left| M_i.M_i^{-1} n_i \right|_R \tag{2.2}$$

where R is range p_i is i^{th} number of moduli set P.

Thus for RNS number {1,3,1},

$$|(2 \times 35 \times 1) + (1 \times 21 \times 3) + (1 \times 15 \times 1)|_{105} = |70 \ + \ 63 \ + \ 15|_{105} = |148|_{105} = 43$$

Similarly for {2,4,1} gives 29.

2.1.3 Addition and Multiplication

	43||	1	3	1
+	29||	2	4	1
=	72||	0	2	2

Table 2.1: Addition

	43||	1	3	1
*	29||	2	4	1
=	92||	2	2	1

Table 2.2: Multiplication

Multiplication gives 92 as the result is $|1247|_{105} = 92$

2.2 Advantages

Most important advantage of residue arithmetic over conventional arithmetic is the absence of carry propagation, in the two main operations of addition and multiplication, and the relatively low precisions required ranging to individual prime or co-prime number of the moduli set, which enables LUT implementations in various operations. In practice, these may make residue arithmetic worthwhile, even though in terms of practical applications such arithmetic has little fields over conventional arithmetic to cover. However the concept of 'break and process' can be very useful in places where integer arithmetic is predominant. However, the fields of Communication and Signal Processing are yet to be explored thoroughly for application on RNS[1; 26] .
Basic advantages of residue arithmetic are:

- High Speed
- Low Power
- Superior Fault Tolerance
- Reduction of Computational Load

2.3 Chinese Remainder Theorem

Consider two positive numbers, x (the dividend) and y (the divisor). Then x modulo y (abbreviated as a(mod n)) can be thought of as the remainder, on division of x by y. Now two simultaneous congruences $n = n_1(mod\ m_1)$ and $n = n_2(mod\ m_2)$ are only solvable when $n_1 = n_2(mod\ (gcd(m_1, m_2)))$. The solution is unique when m_1 and m_2 are co-prime and their gcd is 1. The Chinese Remainder Theorem (CRT) may be stated as one of the most important fundamental results in the theory of RNS[1; 26].

Let m_2 and m_2 and y be positive integers which are relatively prime. Let n_2 and n_2 be any two integers. Then there is an integer N such that

$$N \equiv n_1(mod\ m_1) \text{ and } N \equiv n_2(mod\ m_2) \tag{2.3}$$

Moreover, N is uniquely determined modulo $(m_1.m_2)$. An equivalent statement is that if $gcd(m_1, m_2) = 1$ then every pair of residue classes modulo m_1 and m_2 corresponds to a simple residue class modulo $(m_1.m_2)$.

The theorem can be generalized as follows:
Given a set of simultaneous congruences
$n = n_i(mod\ m_i)$, for i = 1 to p and for which m_i are relatively prime. Then the solution to the set of congruences is

$$x = [a_1 \cdot b_1 \frac{M}{m_1}, a_2 \cdot b_2 \frac{M}{m_2} \cdots a_p \cdot b_p \frac{M}{m_p}] \tag{2.4}$$

Where $M = \{m_1, m_2 \cdots m_p\}$, and the b_i are determined from:

$$b_i \frac{M}{m_i} \equiv 1(mod\ m_i) \tag{2.5}$$

2.3.1 Modular Multiplicative Inverse

$$m_1.m_2 = 1(\mathrm{mod} n)$$

$$m_1^{-1} = m_2 \ (\mathrm{mod}\ n) \tag{2.6}$$

The multiplicative inverse of m_1 modulo n exists iff m_1 and n are coprime, i.e,

$$\gcd(m_1,\ n) = 1 \tag{2.7}$$

If the modular multiplicative inverse of m_1 modulo n exists, the operation of division by m_1 modulo n can be defined as multiplying by the inverse, which is in essence the same concept as division in the field of real. The modular multiplicative inverse can be found out using various techniques, one of the most efficient being the Extended Euclidean Algorithm.

2.3.2 Extended Euclidean Algorithm

The Extended Euclidean Algorithm can find the multiplicative inverse of any number a and b in Z when x and y are given and their inverse exists. Assume the following equation[1; 26]:

$$a.x + b.y = \gcd(x, y)$$

However, if the multiplicative inverse of b exists, then gcd(n,b) = 1. So we have now:

$$\Rightarrow a.x + b.y = 1$$

Now we apply modulo operator to both sides. We will have

$$\Rightarrow (a.x + b.y)\ mod\ x = 1$$
$$\Rightarrow (a.x)\ mod\ x + (b.y)\ mod\ x = 1$$
$$\Rightarrow 0 + (b.y)\ mod\ x = 1$$

$$\Rightarrow b^{-1} \equiv y\ (mod\ x) \tag{2.8}$$

This means that y is the multiplicative inverse of b in Z.

2.4 Limitations and Constraints in Residue Arithmetic

On completion of extensive literature survey the following problem statements were defined:

- Magnitude Calculation
- Sign Detection
- Overflow Detection and Correction

2.4.1 Magnitude Calculation

Chinese Remainder Theorem (CRT) can be used to convert to the weighted number system of any given number and then can be compared with the other one. However this technique is very time consuming as well as increases computational load. Hereby, the approximate CRT method is used to compare magnitude. The theorem[26] is as follow:

$$N = \{n_1, n_2 \cdots n_p\} = \left\langle \sum_{i=0}^{k-1} M_i \langle a_i \cdot n_i \rangle_{m_i} \right\rangle_M$$

$$\frac{N}{M} = \frac{\{n_1, n_2 \cdots n_p\}}{M} = \left\langle \sum_{i=0}^{k-1} \frac{M_i}{M} \langle a_i \cdot n_i \rangle_{m_i} \right\rangle_1$$

$$\frac{N}{M} = \frac{\{n_1, n_2 \cdots n_p\}}{M} = \left\langle \sum_{i=0}^{k-1} m_i^{-1} \langle a_i \cdot n_i \rangle_{m_i} \right\rangle_1 \tag{2.9}$$

All values of $(\frac{N}{M})$ are in [0, 1]. These values are stored in the look up table and the magnitude of each number is calculated to get a magnitude representation.

2.4.2 Sign Detection

For sign detection a trite technique was used. In this a sign bit was introduced as 32^{nd} bit. This results in a signed bit representation of a number. Operating on floating numbers is a difficult task in residue arithmetic. Hence we convert the floating point number to an integer in a range $\pm Z$. The mapping is done such that the operating range $Z < R$. If the floating point number $\pm A$ is in range, and $A < Z$, then

$$P_{sn} = \frac{Z}{A} \tag{2.10}$$

$$X = \frac{x}{P_{sn}} \tag{2.11}$$

where P_{sn} is precision which decides the incorporation of digits after decimal points.

2.4.3 Overflow Detection

The dynamic range of 18 bits is supposed to be adequate for most practical situation as the bound of 18 bits is the worst outcome possible [27]. Now during the homomorphic mapping if we can keep the operating range Z is taken around 2^{18}, and the coefficients are mapped over range of 2^{14}, then scope for overflow is drastically limited.

2.5 Summary

The constraints defined in section 2.4 and the approach obtained to avoid them is enforced throughout in all applications mentioned in this thesis. The basics of all the application and the way residue arithmetic is involved in all the chapters discussed further is summarized in this chapter. The basics of residue arithmetic and the operations like multiplication and addition are approached in 'break and process' methodology. This reduces complexity and computational load and processes things faster. However the undiscovered part of RNS is the power of its wide range as specified by the moduli set. This system has a non-linear distribution of numbers. Two number cannot be compared

just viewing them. Computation has to be done to analyse them. This concept can be used in various application. Image encryption as in chapter 5 uses this fundamental of RNS for encryption. Further the concept has been used in PN sequence generation.

CHAPTER 3

Moduli Selection and Mapping

3.1 Introduction

If we consider any prime number, then there exists at least one primitive root $r \leq p-1$, such that the set $\left\{\left|r^i\right|_p : i = 0, 1, 2 \ldots p-2\right\}$ is set of all possible non-zero residues with respect to p. 5 and 7 are examples of primitive root. Consider $r = 3$ and $p = 5$. Then

$$\left\{\left|3^0\right|_5 = 1, \left|3^1\right|_5 = 3, \left|3^2\right|_5 = 4, \left|3^3\right|_5 = 2\right\}$$

. Thus we get $\{1, 3, 4, 2\}$ where all possible non-zero residues w.r.t. 5 are present [26].

For any digital application moduli set should be chosen such that representation is efficient, unique and the difference between the moduli be as small as possible to increase the dynamic range[26], thus improving the utility factor. Utility factor is mentioned in section 3.4. In this thesis all applications uses either of the selection of moduli set as following two proposed methods:

- Consecutive Moduli Selection

- Exponential Moduli Selection

3.2 Consecutive Moduli Selection

Theorem: Let $\{N_1, N_2, N_3 \ldots N_k\}$ be a set of k consecutive co-prime numbers. Let these numbers be expressed as

$$N_i = N_1 - m_{i-1} \tag{3.1}$$

for i=1,2,3 ... k, where $m_{i-1} > m_{i-2} > m_{i-3} > \ldots m_{i-k} > 0$. Let N_{k+1} be another number that can be added to the set of co-prime numbers, i.e. $N_{k+1} = N_1 - m_k$ then N_{k+1} will be co-prime if $\gcd(N_i, m_k - m_{i-1}) = 1$, for i=1,2,3 ... k.

Proof

For N_{k+1} to be co-prime to every other numbers in the set $\{N_1, N_2, N_3 \ldots N_k\}$,

$$\gcd(N_i, N_{k+1}) = 1$$

$$\Rightarrow \gcd(N_{k+1}, N_i - N_{k+1}) = 1$$

$$\Rightarrow \gcd(N_{k+1}, m_i - m_{i-1}) = 1 \tag{3.2}$$

In order to improve dynamic range of RNS with high bit efficiency, N_1 must be selected as 2^{m-1} which will be a m bit number. Then by the above method one can generate the set of co-prime numbers and use them as moduli set for RNS. The figure represents the bit pattern obtained for consecutive moduli.

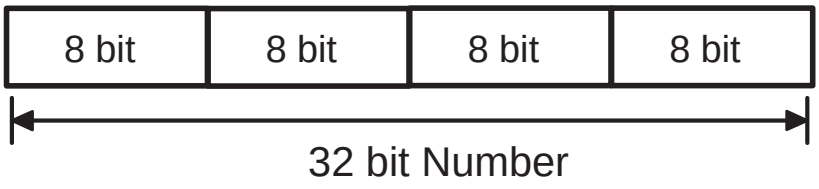


Figure 3.1: Bit Distribution of Residue Number with Consecutive Moduli

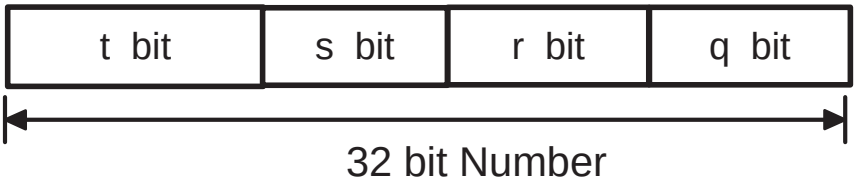


Figure 3.2: Bit Distribution of Residue Number with Exponential Moduli

3.3 Exponential Moduli Selection

Figure 3.2 shows the bit distribution in exponential moduli system. In figure 3.2, $t = 32-(s+r+q)$. Consider a set of number P such that

$$p_i = 2^{n-k} - 1 \tag{3.3}$$

where $k = \{k \, \epsilon \, \mathbb{N} : \forall \; k, \; \gcd(2^{n-k}, P) \; is \; 1\}$.

3.4 Utility Factor

Consider set $P = \{p_1, p_2 \ldots p_n\}$ of n co-prime numbers of x bits each. Hence every number will be represented in $n.x$ bits. Thus if we have to represent any number into k bits system, then

$$x = \frac{k}{n} \tag{3.4}$$

where,

$$p_i < 2^x \tag{3.5}$$

Hence, n and k should be chosen such that $|b|_n = 0$. Eg. A 32bit number can be represented in the RNS as four 8-bit numbers with a range 0 to P_{i-1}.
The numbers which cannot be represented by this scheme of representation,

$$e = 2^k - \prod_{i=0}^{n-1} p_i \tag{3.6}$$

Thus Utility factor will be:

$$U_f = 1 - \frac{e}{2^k} \tag{3.7}$$

Example

Choose co-prime numbers with b=32 and n=4, i.e., close to 2^8 (= 256), gives us P = {255, 254, 253, 251} and P = {31, 127, 511, 2047} when consecutive moduli selection and exponential moduli selection is used respectively. Since there cannot be any other combination of co-prime numbers close to 2^8, hence this is the most bit efficient moduli set with widest dynamic range possible in range of 8 bit numbers. The dynamic range R is hence:

$$R = \prod_{i=0}^{n-1} p_i \tag{3.8}$$

Now calculating R as in eq 3.8, $R_{Con} = 4113089310$ and $R_{Exp} = 4118168929$. In literature there are standard moduli set for medium dynamic ranges (less than 22 bits), three moduli set $2n, 2n$Âś1, and for large dynamic range (greater than 22 bits), general moduli set in form $2^{n_1}, 2^{n_1}+1, 2^{n_2}\pm 1 \ldots 2^{n_i}\pm 1$ with length greater than three are more efficient [27; 28; 29]. But this moduli set shows a better bit utilization. The dynamic range of 18 bits is supposed to be adequate for most practical situation as the bound of 18 bits is the worst outcome possible [27]. Hereby the dynamic range R is a huge margin to avoid overflow. The calculated

$$U_{f_{con}} = 0.95765 \text{ and } U_{f_{exp}} = 0.95884$$

. The higher the utility factor better is the moduli set in term of bit utilization.

3.5 Homomorphic Mapping

The next step is to map the number i.e. to convert the floating point numbers to integers. The operating range is suitably taken such that no overflow occurs. Mapping is a special correspondence between the members (elements) of two fields. Two homomorphic systems have the same basic structure. Their elements and operations appear different; results on one system often apply as well to the other system [30]. Operating on floating numbers is a difficult task in residue arithmetic. Hence we convert the floating point number to an integer in a range $\pm Z$. The mapping is done such that the operating range $Z < R$.

Precisely if,

$$Z \leq R$$

then overflow of any operation can be easily avoided. If the floating point number x is in range $\pm A \text{and} A < Z$, then

$$P_{sn} = \frac{Z}{A}$$

Now, mapped output is:

$$X = \frac{x}{A} \tag{3.9}$$

In this mapping the range $\pm A$ has predominant effect on the precision with which the technique can handle the floating point numbers. As value of A increases the precision decreases and the floating point numbers accuracy deteriorates.

3.6 Summary

Through out this thesis, the moduli selection and homomorphic mapping is used in various applications. The techniques are novel and hereby the new method of comparing moduli based on bit representation is unique and has been bit-efficient in every applications depicted further in this thesis.

CHAPTER 4

Application : RNS Based FIR Filter

Residue number system (RNS) is generally an integer number system as described in chapter 2. The foremost canonical reason for implementation of filter in residue arithmetic is the inherent property of carry-free addition, subtraction and multiplication. As a result we add, subtract and multiply in unison regardless to the numbers. Hereby, devices operating in this principle are fast and ingest low power. However, principal limitation of Residue Number System is the slow and complex nature for arithmetic operations viz. division, comparison, sign detection and overflow detection and rejection. In this paper we have described some novel approaches to grapple with the limitations of comparison, sign detection and averting overflow. The selection of moduli in RNS is most important in attaining to solutions of problems as described earlier. Accordingly, a set of moduli is selected. Further in this paper we have used this set of moduli to successfully depict a design approach for 32-bit lowpass finite impulse response (FIR) filter. A transposed form of FIR filter is preferred always when larger filters are used. For an 8-tap, 16 bit FIR filter the device utilization and performance obtained are almost identical for both direct form as well as transposed form . But when large filters are deployed across

multiple devices, the traditional approach provides a lethargic response as the input to output latency is reduced [31]. This filter architecture allows parallel processing of the input signal thereby, sample rate is increased. RNS arithmetic is carry free and each modulo arithmetic operation is independent to each other. This causes overflow detection to be indocile. In literature there is no approach to detect overflow during any operation. However, if a moduli set is chosen such that the range of the moduli set limits the magnitude of any practical signal, overflow can be significantly obviated.

4.1 FIR Filter Basics

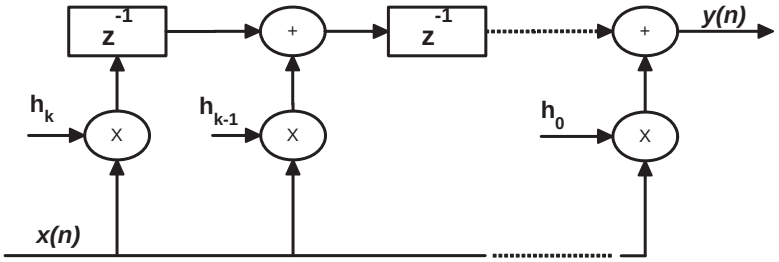


Figure 4.1: FIR Filter Direct Form Transpose

The input to a digital filter is usually a sequence of numbers obtained from sampling an analog signal. The FIR filter may be represented by a block diagram of the type shown in the figure 4.1. The z^{-1} block represents a unit delay. If the input is x(n), then the output of the delay element is x(n-1), which is the value of x(n) one time-period before now, or, put simply, the previous input. Similarly, x(n-2) simply means the value of the input two sampling periods before now. The Filter shown in the figure 4.1 may be represented by a difference equation.

$$y(n) = a_0 x(n) + a_1 x(n-1) + a_2 x(n-2) \ldots a_n x(0) \tag{4.1}$$

The number of branches in the filter is known as the taps of the filter. The filter can be described in terms of its impulse response, which is a series of weighted impulses. With the impulse response, it is easy to compute the output of the filter simply by multiplying

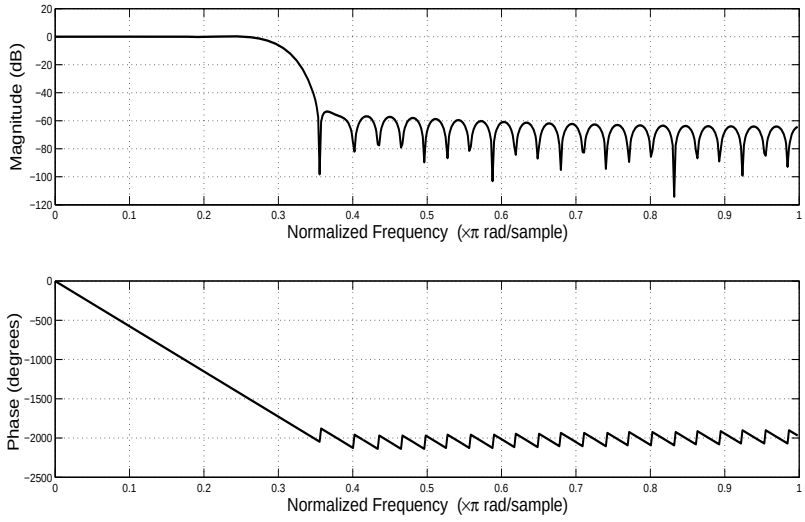


Figure 4.2: Frequency Response of FIR Filter with cutoff frequency 0.3π

the impulse response and the input train of sampled pulses present at the desired time. We may use the idea of delay elements to rewrite the difference equation and so obtain the transfer function. Since z-1 stands for a delay element we have

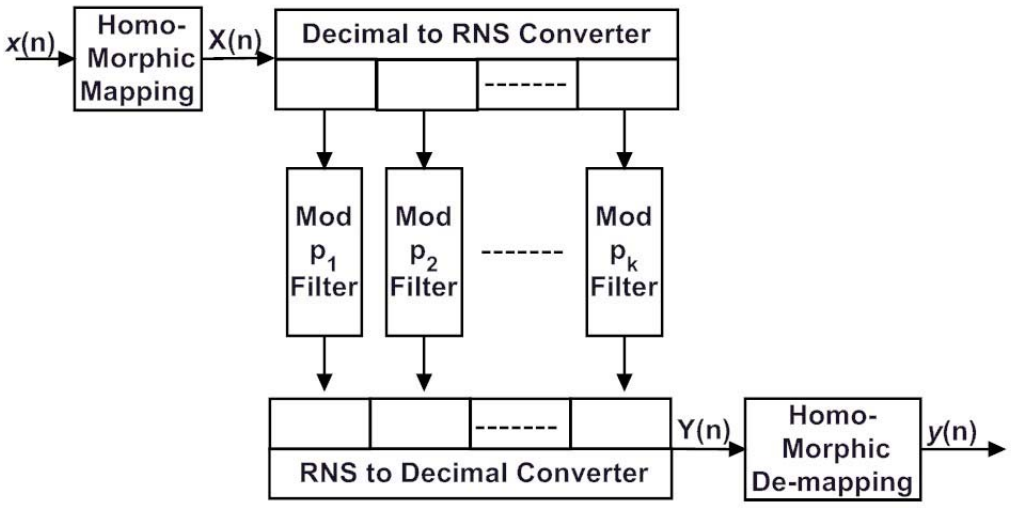
$$y(n) = \sum_{k=0}^{N-1} h(k)x(n-k) \tag{4.2}$$

where $n = 0, 1 \ldots N-1$. Now the coefficients h_k determine the characteristic of the fir filter viz. low pass, high pass, band pass, band reject etc. There are several techniques to determine the coefficients. The filter coefficients are determined using a Hamming-window based, linear-phase filter with normalized cutoff frequency 0.3π rads. By default the filter is normalized so that the magnitude response of the filter at the center frequency of the pass band is 0 dB. Thus the frequency response of the filter is as in figure 4.2; the frequency response of the lowpass fir filter with normalized cutoff frequency 0.3π rads/sec. Matlab function 'fir1' uses the window method of FIR filter design. If w(n) denotes a window, where $1 \leq n \leq N$, and the impulse response of the ideal filter is h(n), where h(n) is the inverse Fourier transform of the ideal frequency response, then the

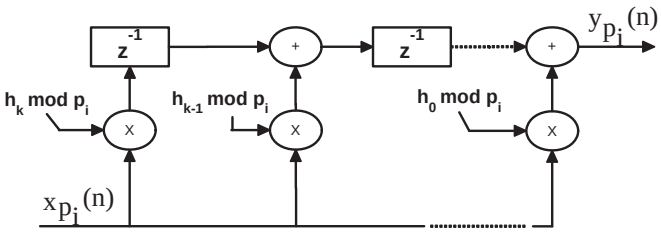
windowed digital filter coefficients are given by following equation.

$$b(n) = w(n).h(n) \tag{4.3}$$

4.2 Proposed Filter Architecture



(a) Architecture



(b) Mod p_i Filter

Figure 4.3: Architecture of the proposed RNS based FIR filter

The figure 4.3 shows the proposed architecture of the FIR filter based on residue arithmetic. The moduli selection as discussed in chapter 3 is the basic and foremost

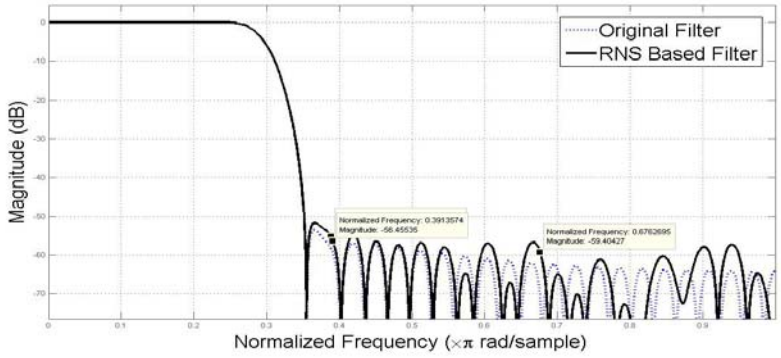
step of this process. The next step is to map the number i.e. to convert the floating point numbers to integers. The operating range is suitably taken such that no overflow occurs. Mapping is a special correspondence between the members (elements) of two fields. Two homomorphic systems have the same basic structure. Their elements and operations appear different; results on one system often apply as well to the other system [30]. Operating on floating numbers is a difficult task in residue arithmetic. Hence we convert the floating point number to an integer in a range $\pm Z$. The mapping is done such that the operating range $Z < R$. Thereafter the filter process goes on as in the figure. The architecture is a 32 bit filter architecture. However, the processing of RNS conversion adds a 33_{rd} sign bit. The introduction of magnitude comparison technique for the addition operation caused a reduction in time consumption. The multipliers used for this filter is based on the IDEA cryptosystem using a recursive multiplication approach [32]. This reduces the time as the time drastically. The performance analysis of the proposed RNS based FIR filter is as portrayed further.

4.3 Filter Specification and Design

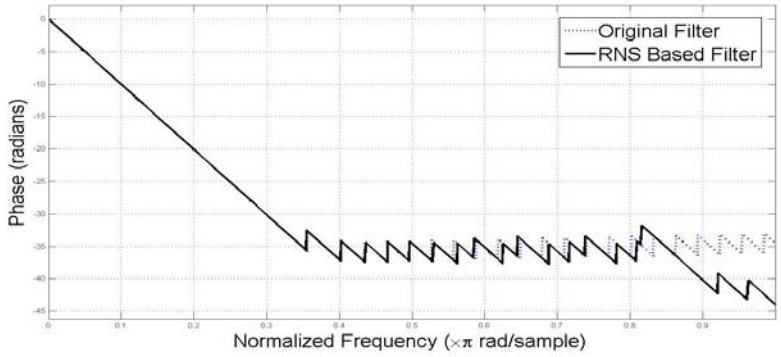
The coefficients of the filter decide the nature of the filter. There are several techniques available in literature that generates the coefficients of a filter for a particular behaviour. In RNS, since operations are split into smaller parallel operations which are independent of each other, there exists n number of filters operating simultaneously. This provides very high speed architecture. Figure 4.3 show the proposed RNS based filter. The residue numbers and converted back by the Chinese remainder theorem based reverse conversion method [26]. The performance analysis is with respect to the traditional FIR filter implementation technique as done in many papers present in the literature [26; 28; 29; 33; 34]. However, the simulation was done in matlab and no hardware implementation was done.

4.4 Results

4.4.1 Simulation



(a) Magnitude Response



(b) Phase Response

Figure 4.4: Comparison of Frequency Response of Proposed RNS Filter with Traditional Filter

The filter coefficients are determined using a Hamming-window based linear-phase 64 tap lowpass FIR filter with normalized cutoff frequency 0.3 rads. By default the filter is normalized so that the magnitude response of the filter at the center frequency of the pass band is 0 dB. The filter is designed in Matlab ver. 7.9.0. This simulation depicts the effects of this design approach on the filter. The magnitude response is compared

with the original response to find out the error as in figure 4.4(a). The phase response figure 4.4(b) is linear over the filter pass band, but it loses its piecewise linearity after the cut-off region, unlike the original FIR filter. However, this does not affect the filter performance.

4.4.2 Performance Analysis

The filter generated with RNS moduli set of P=[31,127,511,2047] and provides the maximum range R = 4118168929 possible. Hereby the filter can operate between these ranges and provides better bit efficiency than existing RNS based filters. The poles zero diagram, in figure 7, of the RNS based filter shows the filter stability. The pole zero plot is generally used to analyze the stability of the system, in this case the designed filter. The poles and the zeros of the RNS filter designed are almost same as the general FIR filter. The stability of the designed filter is not affected at all by the proposed design methodology as suggested by the figure 4.5 and 4.6.

```
 % Original FIR Filter
      % ------------------------------

Discrete-Time FIR Filter (real)
-------------------------------
Filter Structure  : Direct-Form FIR Transposed
Filter Length     : 65
Stable            : Yes
Linear Phase      : Yes (Type 1)

Implementation Cost
Number of Multipliers : 65
Number of Adders      : 64
Number of States      : 64
MultPerInputSample    : 65
AddPerInputSample     : 64

      % ------------------------------
 % RNS Based FIR Filter
      % ------------------------------

Discrete-Time FIR Filter (real)
-------------------------------
Filter Structure  : Direct-Form FIR Transposed
Filter Length     : 65
Stable            : Yes
Linear Phase      : Yes (Type 1)

Implementation Cost
Number of Multipliers : 59
Number of Adders      : 58
Number of States      : 64
MultPerInputSample    : 59
AddPerInputSample     : 58
```

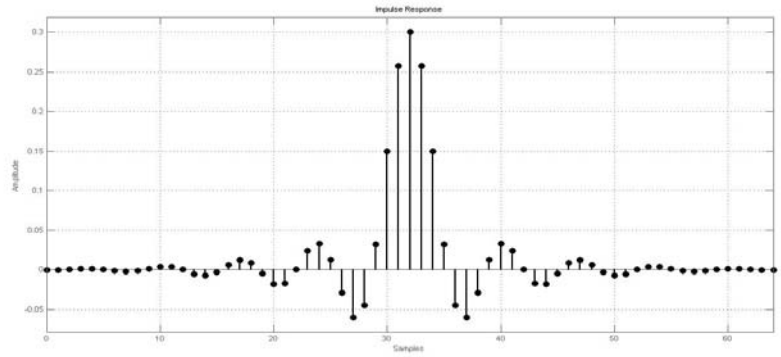
Figure 4.5: Performance Analysis between Traditional and RNS Based FIR Filter Implementation Techniques

The performance analysis is done with respect to the generic traditional FIR filter [33; 34; 35]. However the phase response shows deviation as because there are few data as well as coefficients those are truncated to their higher value during the homomorphic mapping and RNS conversion. This creates an error which propagates through the filter to its output. The detailed report of the comparison drawn between the designed filter after simulation and the traditional FIR filter is shown in figure 4.5 .

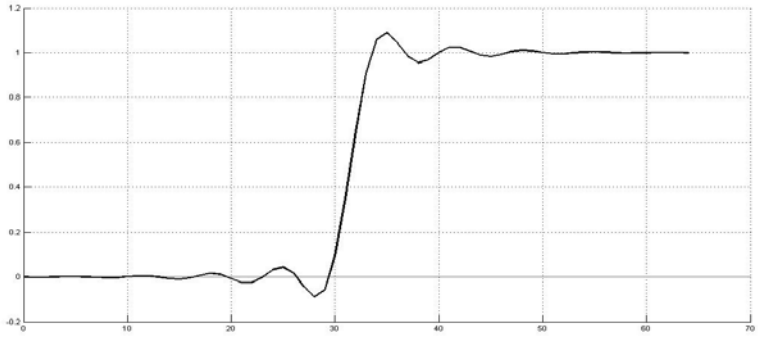
4.5 Summary

The magnitude response and the pole zero plot analyses the filter designed with the coefficients obtained from hamming window technique and implemented on residue arithmetic with a homomorphic mapping. The results are satisfactory with the moduli set proposed.

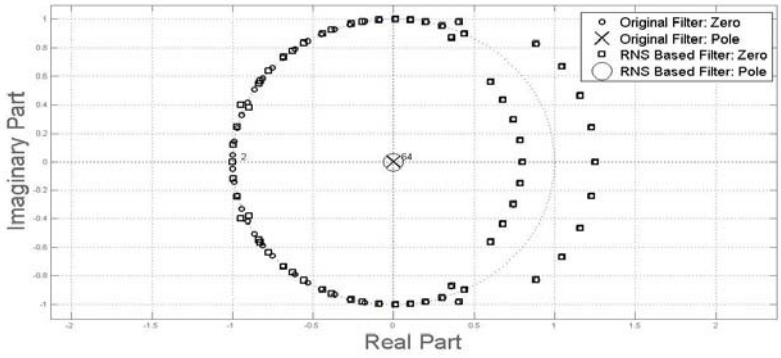
The RNS based filter design can produce very high speed FIR filter. A FIR filter based on the residue number system is exhibited and the filter performance is analysed extensively. The new proposed lowpass FIR filter operates over a high range and the homomorphic mapping provide the incorporation of fractional part of the signal with a calculated precision. Hereby the bit efficiency of the residue number based FIR filter is concluded to have a satisfactory performance. However, the major problem with the RNS based filter is the detection of overflow. If the overflow detection can be done without any use of lookup tables unlike many methods cited in literature viz. [36; 37], then these filters can be optimized to be highly accurate filter which will inherit the property of high speed and low power consumption.



(a) Impulse Response



(b) Step Responce



(c) Pole-Zero Plot

Figure 4.6: Performance and Stability of the RNS based FIR Filter

CHAPTER 5

Application : RNS Based Image Encryption

5.1 Overview to Image Encryption

Since image is an important and trite form of information, secured and authentic transmission is crucial and requisite. Many applications are based on confidential and authentic transmission over unsecured and noisy channel. Thus protection of data, in this case image, from foreign attacks and external channel noise is of prime interest. The basic requirement of encryption is to assure confidentiality, integrity and availability [38]. There are many security mechanism like encipherment, authentic exchange, traffic padding, notarization, digital signature and many more. However, single mechanism for encryption of data is not optimal. Multiple mechanisms are applied together on a data to encrypt is before transmission. An authentic transmission may be achieved by combining , digital signature and authentication exchange [38]. However, this increases computational complexity and are very difficult to encrypt data in real-time online transmission. Hence cryptography, a part of encipherment, was explored to achieve encoding data with a key where the extraction of this key by unauthorised user becomes practically impossi-

ble. If a key take substantially a large amount of time to decipher a key for the extraction of the data, the data is said to be well encrypted. Numerous techniques are developed and present in literature which claims better encryption of any image. However very few viewed the transmission channel noise as a threat to loss of data. Robustness of any encryption technique to channel noise is also of prime importance. In this chapter a robust encryption technique is proposed.

5.2 Introduction

The major security goals for which image, needs to be encoded and encrypted before transmission through a channel are confidentiality, integrity and availability[38]. These are serious issues with respect to data security and transmission and has been challenging for researchers to develop secured encoding techniques. There have been multiple proposed techniques in literature [39; 40; 41; 42; 43; 44; 45]. However there is no specific absolutely reliable technique. In this chapter a novel, secured and low computational image coding scheme based on residue arithmetic is adduced. Basics of residue arithmetic is explained in chapter 2. The concept of 'break and process is again expended to operate on the data in parallel such that the computational load is minimum as well as shared. Moreover the number system works effectively with integer arithmetic. The proposed technique has very low. The robustness and performance of this scheme under adverse channel conditions is exemplified further. This technique was found to be robust and a detailed analysis is given further in results. Standard encryption techniques like Blowfish encryption techniques are compared to the proposed technique for performance analysis.

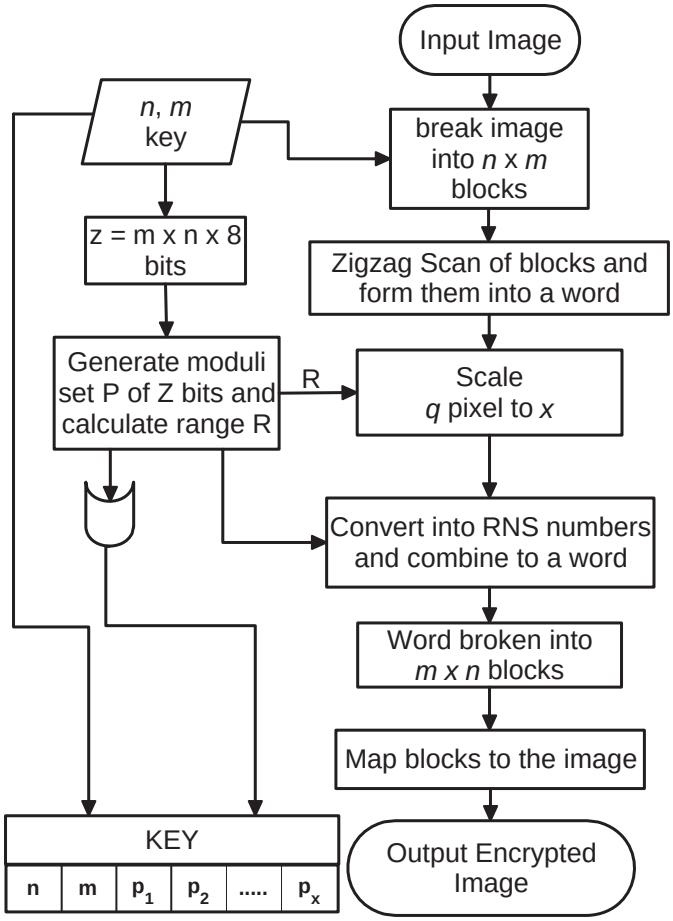


Figure 5.1: Flowchart of RNS Based Encryption Technique

5.3 Proposed Algorithm

5.3.1 Encryption

As in the flowchart described in figure 5.1, we find there are two parts of the key used in this encryption technique. The first part is used to break the image into (m x n) blocks. The second part of the key holds Z bit moduli set. The algorithm for the same is as follows:

Step I: Input image and block size m and n.

Step II: Break image into m x n blocks and Zigzag Scan the intermediate blocks.

Step III: $Z = m$ x n x 8 bits. Generate a moduli set P, where $P = \{p_1, p_2 \ldots p_k\}$ corresponding to Z bits.

Step IV: Convert the intermediate zigzag scanned block into one word and scale to avoid overflow.

$$q = \left\lfloor \frac{2^z}{R} \cdot X \right\rfloor \tag{5.1}$$

Step V: Use the set P to convert the word into RNS.

Step VI: Regroup the RNS number to form a word and further break them into m x n blocks.

Step VII: Map the encrypted block to image.

5.3.2 Decryption

As in the flowchart described in figure 5.2, we find there are two parts of the key used in this decryption technique as in encryption. The first part is used to break the image into (m x n) blocks. The second part of the key holds Z bit moduli set. The algorithm for the decryption of the encrypted image is as follows:

Step I: Input encrypted image and key.

Step II: The first two numbers of the key represents m and n block size. The next part represents the moduli set P.

Step III: Break encrypted image into m x n blocks and the intermediate blocks are converted to one word.

Step IV: Bit length pf every p_i is calculated and the word is then broken according to the bit length into separate numbers.

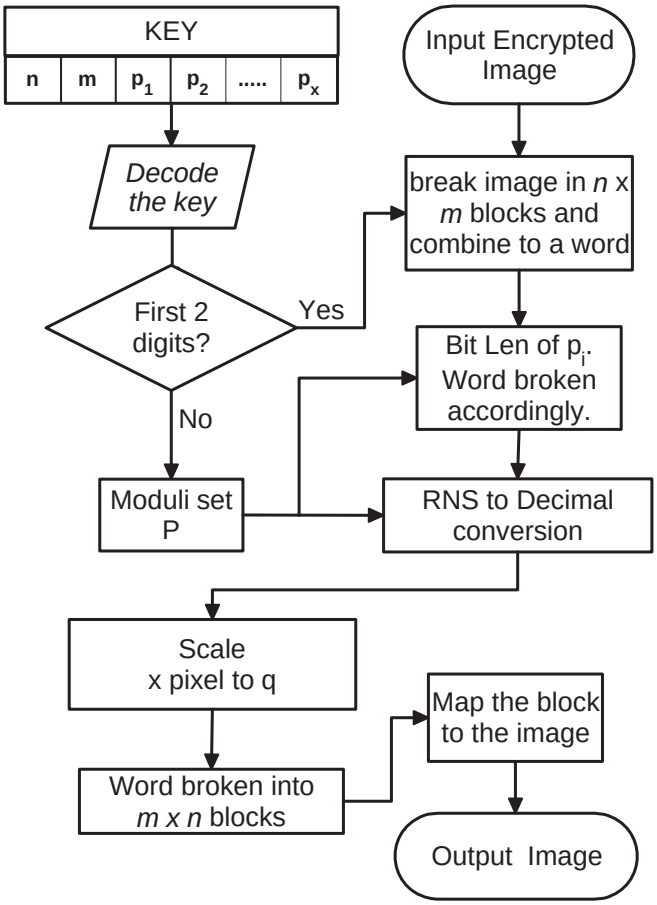


Figure 5.2: Flowchart of RNS Based Decryption Technique

Step V: Convert these RNS numbers to decimal or binary and scale accordingly.

$$X = \left\lfloor \frac{2^z}{R} \cdot q \right\rfloor \tag{5.2}$$

Step VI: Decimal or binary number is further broken into m x n blocks.

Step VII: Zigzag inverse the blocks and map them to form the image.

5.4 Standard Algorithm

Blowfish is a symmetric block cipher designed by Bruce Schneier in 1993 and is commercially used in large number of encryption products. It is also used in internet widely for secured data transmission. It designed based on DES and Fiestel Network structure. It has 64 bit block size and key length varying from 1 to 448 bits. Blowfish is open source and free license [46]. Twofish is recently discovered encryption algorithm and is preferred over Blowfish in many ways. It is also a symmetric key block cipher with block size of 128 bits and key length 128, 192 or 256 bits. It is derived from Blowfish and hence follows Fiestel Network structure [45; 47]. Threefish is another very new concept of encipherment published in 2008. In this algorithm, key size is always same as block size. Block sizes are 256, 512 or 1024; hence the key sizes are selected respectively. 266 and 512 block sizes uses 72 rounds. However, 1024 block size uses 80 rounds. Threefish algorithm takes 6.1 cycles per byte on core 2 processor.

5.5 Results

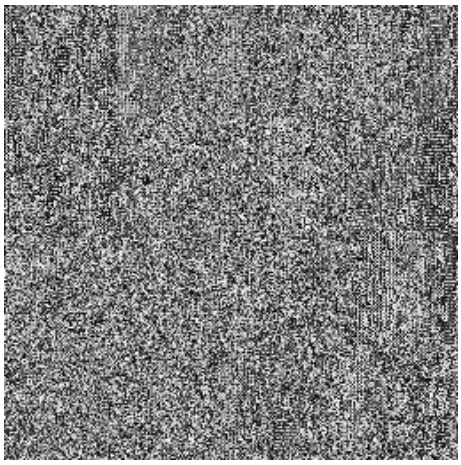
The proposed algorithm was simulated in Matlab in Core 2 duo 2.33 Ghz processor. Lena image of 256x256 as in figure 5.3(a) was used for simulation. The encrypted image is shown in figure 5.3(b).

The encrypted image figure 5.3(b) in was transmitted through an AWGN channel and the output image was analysed for error. The bit error plot is given in figure 5.4. The transmitted image at 8db, 10db, 12db and 15db is shown in figure 5.5. These noisy images are denoised by simple median filter and the output is shown in figure 5.6.

5.5.1 PSNR Analysis

Peak signal-to-noise ratio (PSNR) has traditionally been used in analog systems as a trusty quality metric. Due to its low complexity, PSNR is used widely for analysis of quality image and video processing metric for evaluating algorithms for de-noising, encryption and compression methods and is considered to be a reference benchmark for

(a) Original image



(b) RNS Encrypted Image

Figure 5.3: RNS Based Encryption

developing perceptual image or video procesing [48]. However, correlation of PSNR subjective to equality have been shown to perform below average [49].

MSE is defined as follows [50]:

$$MSE = \frac{1}{MN} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} \left[O_{img}(i,j) - A_{img}(i,j) \right]^2 \tag{5.3}$$

PSNR is hereby defined as [50]:

$$PSNR = 10\ log_{10} \left(\frac{MaxVal^2}{MSE} \right) \tag{5.4}$$

where MaxVal is maximum pixel value possible in the image. Table 5.1 gives the PNSR performance for the proposed algorithm when applied on the image in figure 5.3(a) and AWGN channel SNR from 1 to 20db.

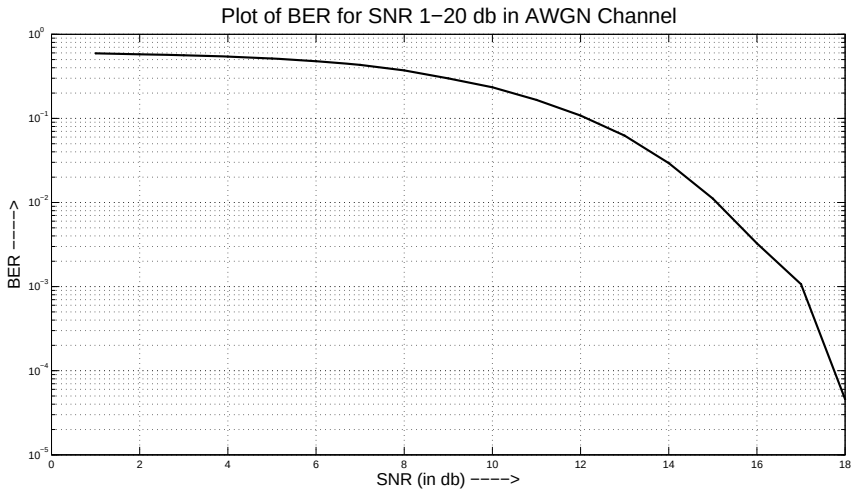


Figure 5.4: BER plot of RNS based encryption technique

5.5.2 Median Filter

The median filter is a non-linear digital filter. It is just like a mean filter. It is a spatial filter and is mostly used to reduce noise in image. Median filter looks at the surrounding neighbours to decide whether or not its is representative of its surroundings. The median of those values are calculated and then replaced. Median filter is also a smoothing technique hence the sharpness of the output image is marginally lost. The received images are denoised by passing through a median filter. Hence the denoised images are seemed to lose the sharpness as evident in figure 5.6

5.5.3 Comparision with Blowfish Encryption

As mentioned in section 5.4, Blowfish is an encryption technique and is widely used commercially. Thus the proposed technique is compared to it with respect to

- Bit Error Rate
- Encryption time
- Correlation and Entropy

(a) Recieved Image at 8db SNR (b) Recieved Image at 10db SNR

(c) Recieved Image at 12db SNR (d) Recieved Image at 15db SNR

Figure 5.5: RNS Based Encryption

5.5.4 Bit Error Rate

The figure 5.7 shows the BER plot of two encryption technique. The plot of Blowfish is better than the proposed technique. However both starts to be noise immune from 18db.

5.5.5 Encryption Time

The encryption time for the proposed algorithm is less then that of Blowfish encryption as depicted in table 5.2.

MSE	SNR	PSNR
8.524×10^3	1	8.8242
	2	8.9268
	3	9.0649
	4	9.2745
	5	9.4465
	6	9.9002
	7	10.4117
	8	11.0685
	9	12.0293
	10	13.1042
	11	14.8547
	12	16.6835
	13	19.2325
	14	22.2243
	15	26.0141
	16	30.9006
	17	37.4252
	18	47.5283
	19	Inf
	20	Inf

Table 5.1: PSNR Analysis

5.5.6 Correlation and Entropy

Correlation is defined as:

$$r = \frac{\sum_m \sum_n (I_{mn} - \bar{I})(J_{mn} - \bar{J})}{\sqrt{(\sum_m \sum_n (I_{mn} - \bar{I})^2)(\sum_m \sum_n (J_{mn} - \bar{J})^2)}} \tag{5.5}$$

where I and J are two images and $\bar{I}$ and $\bar{J}$ are mean of those images respectively.

Entropy is again defined as [51]

$$E_n = -\sum_{i=0}^{M-1} P_k \ log_2 (P_k) \tag{5.6}$$

(a) Denoised Image at 8db SNR

(b) Denoised Image at 10db SNR

(c) Denoised Image at 12db SNR

(d) Denoised Image at 15db SNR

Figure 5.6: Denoised Images Received At Various SNR

The encrypted images in both techniques are correlated to the original image to calculate pixel to pixel relation. The correlation is found for the proposed algorithm is less then that of Blowfish encryption as depicted in table 5.3.

5.6 Summary

Thus we find that the proposed algorithm of RNS based image encryption is not as robust as Blowfish, however the fact that is of interest is the encryption time. The encryption time is appreciably less compared to Blowfish. Further research can be done to improve

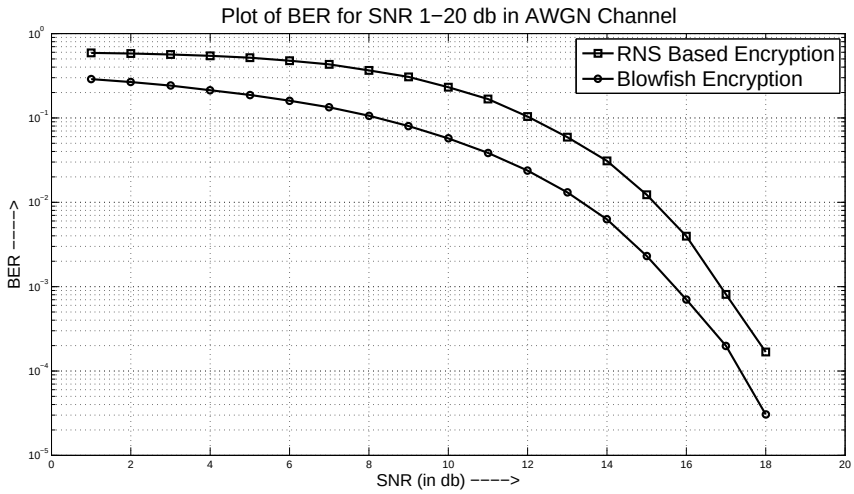


Figure 5.7: BER Plot of RNS Based Encryption and Blowfish Ecryption

Tr. No.	RNS Encryption (in sec.)	Blowfish (in sec.)
1	0.14314	0.18736
2	0.14269	0.18964
3	0.14363	0.18767
4	0.14632	0.18811
5	0.14364	0.18722
Avg.	0.14389	0.1880

Table 5.2: Encryption time

the quality of the output image.

Perf. Factors	RNS Encryption	Blowfish
Correlation	.0066	0.0089
Entropy	7.9874	7.9971

Table 5.3: Correlation and Entropy Calculation

CHAPTER 6

Application : RNS Based PN Sequence

Before beginning with spread spectrum system, we focus on to concept of spectrum. Every system that modulates or transmits a signal has two basic cardinals, namely the frequency at which the signal is centred and bandwidth of the signal when modulated. Spectrum gives the range of a signal; in communication and signal processing, the range of the signal is spoken in terms of frequencies covered by the signal. Thus by spectrum of a signal we mean frequency spectrum. The difference between the maximum frequency and minimum frequency of the signal in view is called bandwidth of the signal. As mentioned in chapter 4, any signal in time domain can also be presented in frequency domain and vice versa by various transform techniques. In spread spectrum we therefore just spread the spectrum i.e. a signal covering one or narrow band of frequencies are spread over a large band of frequencies, quite large in fact than frequency required to transmit signal consummately, hence converting a small bandwidth to a very large bandwidth.

6.1 Introduction to Spread Spectrum Communication

The basis of spread spectrum technology is expressed Shannon in terms of channel capacity:

$$C = \omega \ log_2\left(1 + \frac{S}{N}\right) \tag{6.1}$$

where

C is capacity in bps

ω is bandwidth in Hz

S is signal power

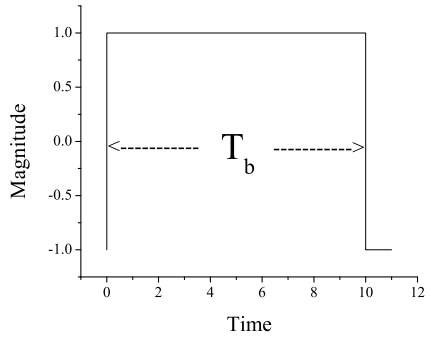
N is noise power

Equation 6.1. limns the competency of a channel to transmit information devoid of any error compared to SNR in the channel and bandwidth used to transmit the information [52]. The bit duration is T_b as in figure 6.1(a). The bit duration of the PN sequence is T_c as in fig. 6.1(b) and is called as chip period. Now when the bit is multiplied to the PN sequence, the output is in fig. 6.1(c) which also has a bit duration of T_c. Since $T_b >> T_c$, the frequency of the transmitted bit becomes very large compared to the signal. This is called Direct Sequence Spread Spectrum (DS-SS). Frequency hopping is also a concept widely used in spread spectrum communication. However this chapter only deals with DS-SS as frequency hopping is out of scope.

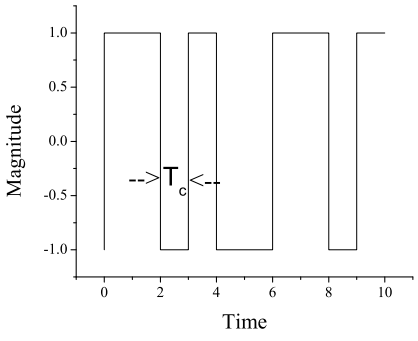
DS-SS is primarily used in CDMA for multiple access. The structure of the spread DS-CDMA is portrayed in figure 6.2. This is similar to MA-ACSK scheme except the fact that the spreading sequences used in the system are vectors generated based on residue arithmetic.The transmitter generates N no. of RNS based orthogonal PN sequences for N users. The details of the proposed RNS based PN sequence generator and comparison to standard DS-CDMA techniques are chalked out in the rest of the chapter.

6.2 Proposed PN Sequence Algorithm

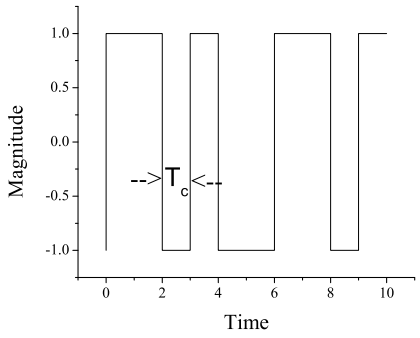
The proposed PN sequence is generated based on residue arithmetic. There is a key input to the generator along with the spread factor β. The figure 6.3 shows the block diagram



(a) Bit to Transmit



(b) PN Sequence



(c) Transmitted Symbol

Figure 6.1: Direct Sequence Spread Spectrum Bit Pattern

of the PN sequence generated. As depicted in the chapter 3, moduli set are selected either by consecutive method or exponential method. The input k in figure also known as spread factor β is responsible for the no. of moduli to be generated. The bits of moduli set should be same as that of k. The keys in separate phase are selected such that the orthogonality of the output vector holds. The generated numbers in RNS are concatenated and converted into binary sequence of 1 and 0. This sequence is passed through the NRZ encoder to make a PN sequence of -1 and 1. This RNS based PN sequence generator is then used in DS-CDMA.

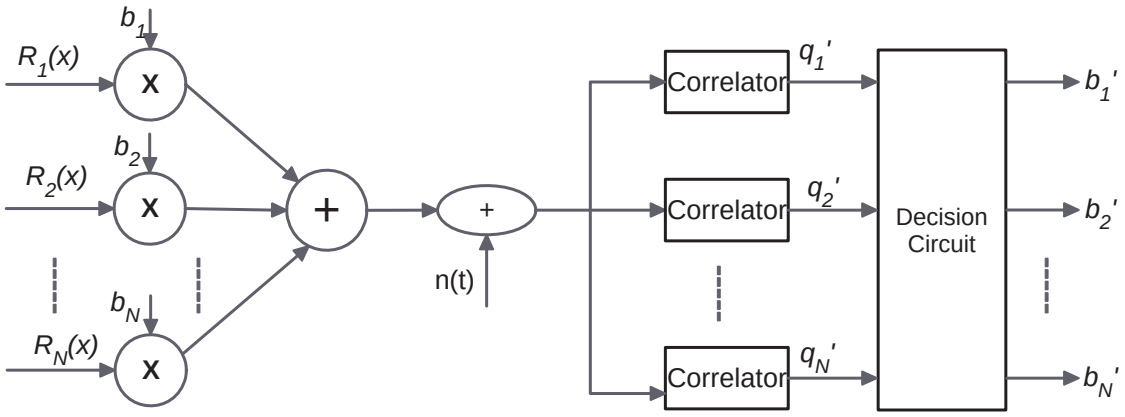


Figure 6.2: Direct Sequence CDMA Technique

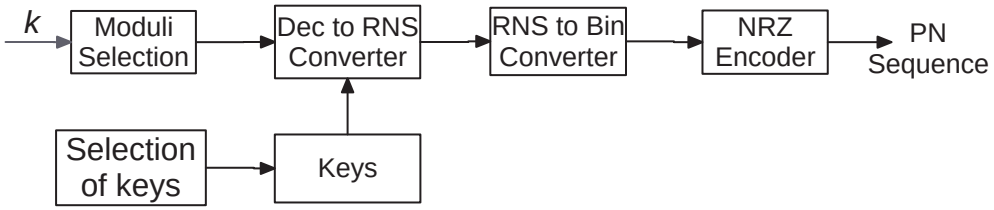


Figure 6.3: RNS Based PN Sequence Generator

6.3 Standard PN Sequences

In this chapter, performance of the RNS based PN sequence is compared to Gold Code sequence and Kasami Code sequence. Gold Sequence was proposed by Robert Gold. These are constructed by EXOR-ing two m-sequences of the same length with each other. Thus, for a Gold sequence of length $m = 2^l - 1$, one uses two LFSR, each of length $m = 2^l - 1$. Choosing LFSRs appropriately, Gold sequences give better cross-correlation properties than maximum length LSFR sequences [53; 54]. Kasami sequences are binary sequences of length 2^N where N is an even integer. Kasami sequences have good cross-correlation values and approaches close the Welch lower bound. Kasami sequences commonly have two classes, namely the small set and the large set. The process of generating a Kasami sequence starts by generating a maximum length sequence x(n), where $n = 1, 2 \ldots 2^N - 1$. Maximum length sequences are periodic sequences so a(n) is repeated periodically for

N larger than $2^N - 1$. Henceforth another sequence $x(n) = y(q.n)$ is generated where $q = 2^{\frac{N}{2}} + 1$. Kasami sequences are formed by adding x(n) and a time shifted version of y(n)modulo two. All sequences generated by different time shifts of y(n) plus the x(n) and y(n) sequence constitute the Kasami sequence. This set has $2^{\frac{N}{2}}$ different sequences.

6.4 Results

Pn Seq	PN_1	PN_2	PN_3	PN_4	PN_5	PN_6
PN_1	1	0.0691	0.0020	0.0796	0	0.1463
PN_2	0.0691	1	0.0544	-0.0866	0.1411	0.0713
PN_3	0.0020	0.0544	1	0.0023	-0.0157	-0.0577
PN_4	0.0796	-0.0866	0.0023	1	0.1459	-0.2050
PN_5	0	0.1411	-0.0157	0.1459	1	-0.0314
PN_6	0.1463	0.0713	-0.0577	-0.2050	-0.0314	1

Table 6.1: Correlation Matrix for PN sequence with $\beta = 128$

The table 6.1 represents correlation matrix of six RNS based PN sequences generated from key matrix Q=[1536958 1536965 1235688 4321531 2315312 2447683]. The spread factor $\beta = 128$ and hence the generated moduli set P=[255 254 253 251 247 241 239 233 229 227 223 217 211 199 197 193].

The figure 6.5 shows the BER performance of the proposed sequence over a AWGN channel.

6.5 Performance Comparison

The figure 6.6 shows the comparison between the performance of Gold sequence, Kasami sequence and RNS based PN sequence over a AWGN channel based on BER. The plots shows the nature of the PN sequences with increase in user. As the user increases the proposed PN sequence is not affected as much as Gold and Kasami Sequence. All the simulations are done for spread factor $\beta = 128$.

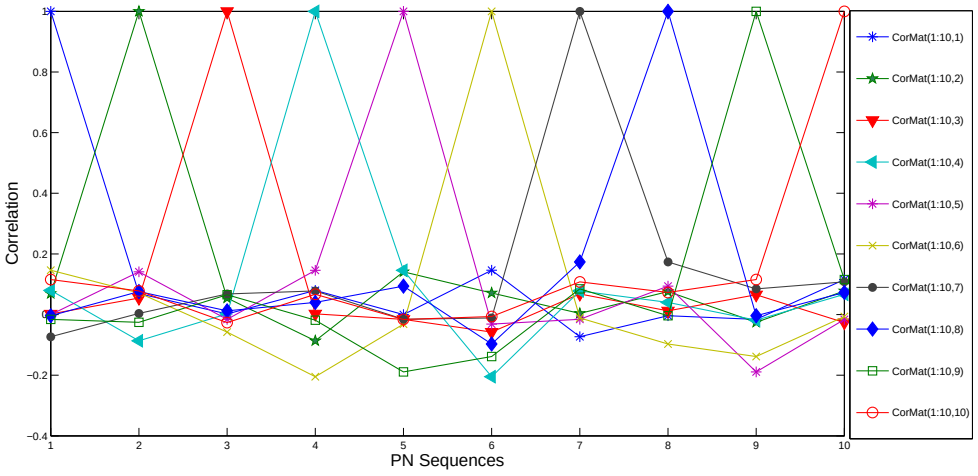
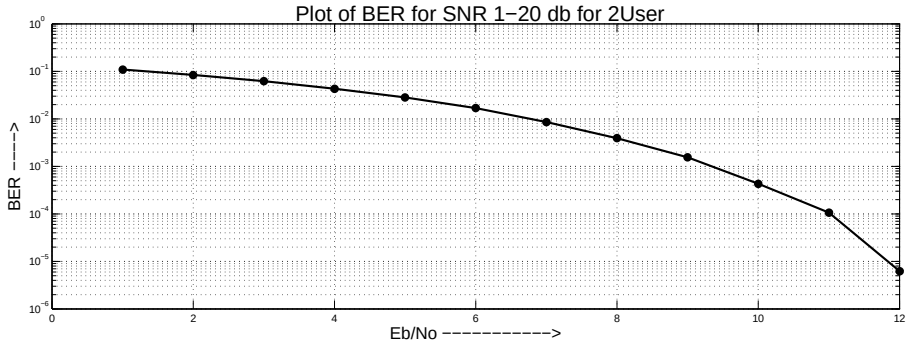


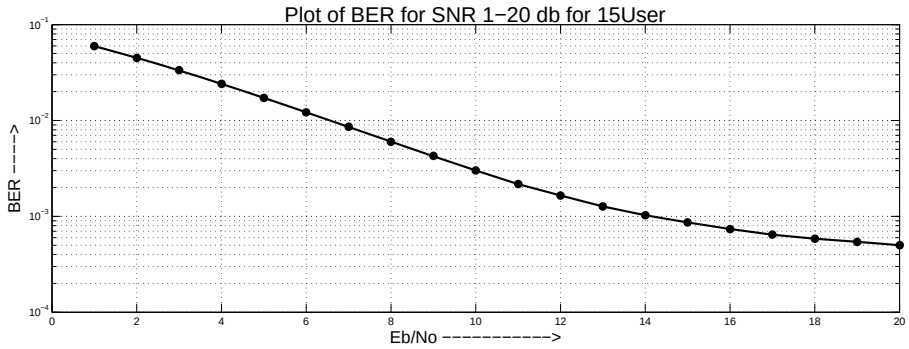
Figure 6.4: Correlation Matrix for 10 sequence generated by RNS based PN generator

6.6 Summary

The proposed PN sequence based on RNS has a low computational complexity and has a very high dynamic key range. Hence, the secured and authentic transmission is possible. The performance based on BER provides adequate data about the robustness of the technique.

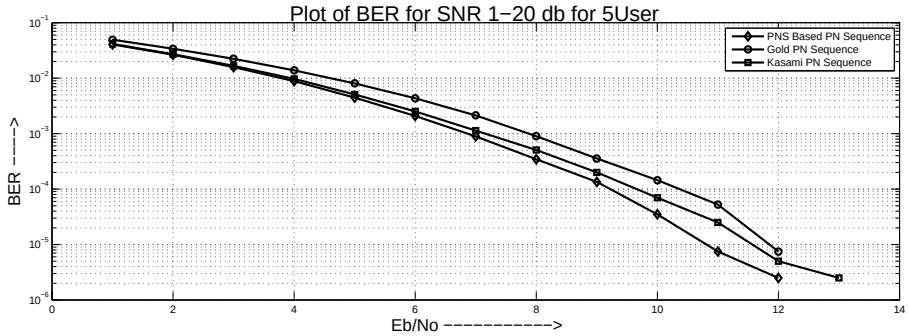


(a) 2 User

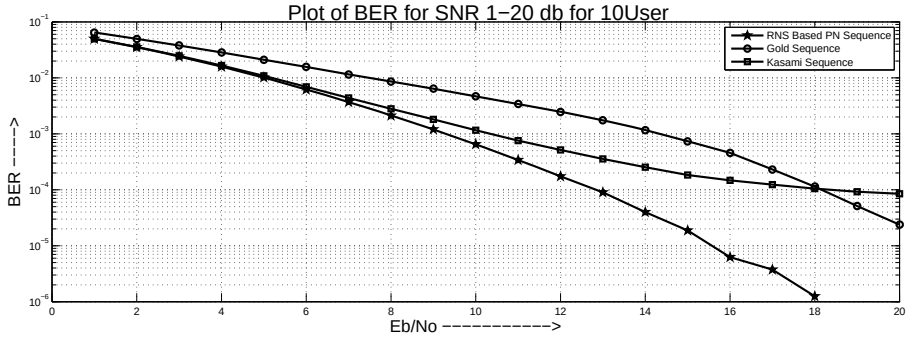


(b) 15 User

Figure 6.5: BER plot for RNS based PN sequence for 2 and 15 User



(a) 5 User



(b) 10 User

Figure 6.6: BER plot for Gold, Kasami and RNS based PN sequence for 5 and 10 Users

CHAPTER 7

Conclusion

7.1 Conclusion

In this thesis, focus was on exploring the potential of Residue Arithmetic in the field of Communication and Signal Processing. The most important aspect of Residue Number System, 'break and process', was widely used in this dissertation. Apart from that, large dynamic range and the non-linearity in the number system was put to its use in generating PN sequence and image encryption. This chapter further describes summary of the thesis, work done, contributions and scope of future work.

Major contribution was generating moduli set by consecutive and exponential method. The approach made mor with bit efficiency of a particular application be it a digital FIR filter, image encryption or PN sequence based on utility factor.

The introduction of homomorphic mapping for incorporation of fractional numbers with a precision and by large avoiding overflow was another contribution to literature. Further a design approach for RNS based FIR filter was discussed and the performance analysis shows credibility of the system designed. The introduction of RNS on image en-

cryption was not new. However the idea of grouping of image pixels and combine them together finally to convert them to RNS and represent the same pixels was a novel idea. The application of RNS to develop a PN sequence and generate the orthogonal sequence such that the performance is good, was another major contribution. Sequence generated by this technique, produces good performance as it was shown in the performance analysis of chapter 6.

7.2 Scope for Future Work

- VLSI implementation of the propose RNS based FIR filter architecture
- Developing results obtained image encryption such that the performance level is better than existing algorithm keep the encryption time constant if not improved.
- The performance of the proposed PN sequence in fading channel can be analysed and necessary amendments can be done to improve performance.
- RNS can be introduced in other applications of Communication and Signal Processing like adaptive filtering, neural networks etc.
- RISC processors based on RNS can be developed as lots of research is going on around the globe.

Appendix A: Image Encryption Simulation Parameters

The results of the simulation in section 5.5 shows the performance of the RNS based novel encryption technique and a performance analysis with Blowfish encryption technique. The simulation uses:

Parameters	Values
Block Size for Zigzag Scan	4
Block Size for Encryption	4
Key Length	32
Moduli set (P)	Consecutive moduli set selection

Appendix B: Spread Spectrum

The RNS based PN sequence generator used to limn the DS-SS communication system in section 6.4 for generation of several PN sequences uses a PIN that is used by the user. Hence the simulation results in this section shows results for 15 different users at the maximum as in figures 6.5 and 6.6. Hence 15 different user uses 15 different PIN (Personal Identification Number). The simulation uses the following PIN for generation of PN sequences. The PIN can be in range of R as in equation 3.8.

P=[255 254 253 251 247 241 239 233 229 227 223 217 211 199 197 193]

The Gold and Kasami Sequence is generated by polynomial as below (as per Matlab simulation):
poly1 = [10 6 5 0] and
poly2 = [10 4 2 0]

User	PIN
User 1	1536958
User 2	1536965
User 3	1235688
User 4	4321531
User 5	2315312
User 6	2447683
User 7	1010157
User 8	3051173
User 9	2002007
User 10	1003765
User 11	1065895
User 12	2056586
User 13	3256581
User 14	2325652
User 15	0252145

Bibliography

[1] *Residue number systems: algorithms and architectures*. Kluwer Academic Publisher, 2002. 2, 3, 7, 9, 10, 11

[2] T. Stouraitis and V. Paliouras, "Considering the alternatives in low-power design," in *IEEE Electron Devices Society IEEE Lasers and Electro-Optics Society*. 3

[3] C.-L. Wang, "New bit-serial vlsi implementation of rns fir digital filters," in *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*. 3

[4] A. Skavantzos and Y. Wang, "The applications of the new chinese remainder theorems for three moduli sets," in *IEEE Pacific Rim Conference on Communications, Computers and Signal Processing, 1999*. 3

[5] Y. Wang, "New chinese remainder theorems," in *Conference Record of the Thirty-Second Asilomar Conference on Signals, Systems and Computers, 1998*. 3

[6] P. . M.-B. U. . T. F. . G. A. . L. A. Ramirez, J. ; Fernandez, "Index-based rns dwt architectures for custom ic designs," in *IEEE Workshop on Signal Processing Systems, 2001*. 3

[7] ——, "Implementation of canonical and retimed rns architecture for orthogonal 1-d dwt over fpl devices," in *Conference Record of the 34th Asilomar Conf. on SSC*. 3

[8] A. A. Author, B. B. Author, and C. Author, "Title of article," *Title of Journal*, vol. 10, no. 2, pp. 49–53, 2005. 3

[9] G. A. B. U. T.-F. F. P. L. A. Rama■rez, J., "Design of rns-based distributed arithmetic dwt filterbanks," vol. 2, 2001, pp. 1193–1196, cited By (since 1996) 2. 3

[10] Y. Liu and E. M. Lai, "Design and implementation of an rns-based 2-d dwt processor," *IEEE Transactions on Consumer Electronics*, vol. 50, no. 1, pp. 376–385, 2004, cited By (since 1996): 8. [Online]. Available: www.scopus.com 3

[11] J. . Bajard and L. Imbert, "A full rns implementation of rsa," *IEEE Transactions on Computers*, vol. 53, no. 6, pp. 769–774, 2004, cited By (since 1996): 43. [Online]. Available: www.scopus.com 3

[12] D. M. Schinianakis, A. P. Kakarountas, and T. Stouraitis, "A new approach to elliptic curve cryptography: An rns architecture," in *Proceedings of the Mediterranean Electro-technical Conference - MELECON*, vol. 2006, 2006, pp. 1241–1245, cited By (since 1996): 1. [Online]. Available: www.scopus.com 3

[13] A. S. Madhukumar and F. Chin, "Residue number system-based multicarrier cdma system for high-speed broadband wireless access," *IEEE Transactions on Broadcasting*, vol. 48, no. 1, pp. 46–52, 2002, cited By (since 1996): 5. [Online]. Available: www.scopus.com 3

[14] ——, "Design and performance of residue number system based multicarrier cdma in frequency-selective rayleigh fading channels," in *Conference Record of the Asilomar Conference on Signals, Systems and Computers*, vol. 2, 2000, pp. 884–888. [Online]. Available: www.scopus.com 3

[15] L. Yang and L. Hanzo, "Performance of residue number system based ds-cdma over multipath fading channels using orthogonal sequences," *European Transactions on*

Telecommunications, vol. 9, no. 6, pp. 525–535, 1998, cited By (since 1996): 14. [Online]. Available: www.scopus.com 3

[16] L.-L. Yang and L. Hanzo, "Residue number system based multiple code ds-cdma systems," *IEEE VTS 50th Vehicular Technology Conference, VTC 1999-Fall*, vol. 2, pp. 1450–1454, 1999, cited By (since 1996): 3. [Online]. Available: www.scopus.com 3

[17] D. Zhu and B. Natarajan, "Residue number system arithmetic assisted coded frequencyhopped ofdma," *EURASIP Journal on Wireless Communications and Networking*, vol. Article ID 263695, 2009. 3

[18] ——, "Residue number system arithmetic inspired hopping pilot pattern design for cellular downlink ofdma," in *2010 Wireless Telecommunications Symposium, WTS 2010*, 2010. [Online]. Available: www.scopus.com 3

[19] C. T. Clarke and T. Srikanthan, "Residue arithmetic techniques for hardware reduction in pseudo-random sequence correlators," in *Conference Record - Asilomar Conference on Signals, Systems and Computers*, vol. 2, 2004, pp. 1864–1867. [Online]. Available: www.scopus.com 3

[20] M. F. Griffin and F. J. Taylor, "Residue number system reduced instruction set computer (risc) concept," in *ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing - Proceedings*, vol. 4, 1989, pp. 2581–2584, cited By (since 1996): 1. [Online]. Available: www.scopus.com 3

[21] H.T.Vergos, "A 200-mhz rns core," *European Conference on Circuit Theory and Design*, pp. II/249–252, August 2001. 3

[22] C. H. Huang, D. G. Peterson, H. E. Rauch, J. W. Teague, and D. F. Fraser, "Implementation of a fast digital processor using the residue number system." *IEEE transactions on circuits and systems*, vol. CAS-28, no. 1, pp. 32–38, 1981, cited By (since 1996): 1. [Online]. Available: www.scopus.com 4

[23] R. Chaves and L. Sousa, "Rdsp: a risc dsp based on residue number system," *IEEE Proceedings. Euromicro Symposium on Digital Object Identifier*, pp. 128 – 135, September 2003. 4

[24] A. Skavantzos, "Efficient residue to weighted converter for a new residue number system," in *Proceedings of the IEEE Great Lakes Symposium on VLSI*, 1998, pp. 185–191, cited By (since 1996): 10. [Online]. Available: www.scopus.com 4

[25] J. Ramírez, A. García, S. López-Buedo, and A. Lloris, "Rns-enabled digital signal processor design," *Electronics Letters*, vol. 38, no. 6, pp. 266–268, 2002, cited By (since 1996): 30. [Online]. Available: www.scopus.com 4

[26] A. Omondi and B. Premkumar, *Residue Number System: Theory and Implementation*. Imperial College Press, 2007, vol. 2. 7, 9, 10, 11, 15, 24

[27] N. Stamenkoviťc, "Digital fir filter architecture based on the residue number system," *ELEC. ENERG. vol. 22, no. 1, April , 125-140*, vol. 22, no. 1, pp. 125–140, April 2009. 13, 18

[28] W. Wang, M. N. S. Swamy, and M. O. Ahmad, "Moduli selection in rns for efficient vlsi implementation," in *Proceedings - IEEE International Symposium on Circuits and Systems*, vol. 4, 2003, pp. IV512–IV515, cited By (since 1996): 6. [Online]. Available: www.scopus.com 18, 24

[29] R. Conway and J. Nelson, "Improved rns fir filter architectures," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 51, no. 1, pp. 26–28, 2004, cited By (since 1996): 24. [Online]. Available: www.scopus.com 18, 24

[30] K. A. Fuatai, *Concepts of Mapping*. Springer, 2009, vol. DOI 10.1007/978-0-387-89194-1. 19, 24

[31] A. M. Vikram Pasham and K. Chapman, *Transposed for FIR Filter*, v1.2 ed., Xilinx, October 2001. 21

[32] M. Bahrami and B. Sadeghiyan, "Efficient modulo 2n+1 multiplication schemes for idea," in *Proceedings - IEEE International Symposium on Circuits and Systems*, vol. 4, 2000, pp. IV–653–IV–656, cited By (since 1996): 2. [Online]. Available: www.scopus.com 24

[33] W. K. Jenkins and B. J. Leon, "Use of residue number systems in the design of finite impulse response digital filters." *IEEE Trans Circuits Syst*, vol. CAS-24, no. 4, pp. 191–201, 1977, cited By (since 1996): 37. [Online]. Available: www.scopus.com 24, 27

[34] F. Pourbigharaz and H. M. Yassine, "A signed-digit architecture for residue to binary transformation," *IEEE Transactions on Computers*, vol. 46, no. 10, pp. 1146–1150, 1997, cited By (since 1996): 16. [Online]. Available: www.scopus.com 24, 27

[35] T. K. Shahana, R. K. James, B. R. Jose, K. Poulose Jacob, and S. Sasi, "Performance analysis of fir digital filter design: Rns versus traditional," in *ISCIT 2007 - 2007 International Symposium on Communications and Information Technologies Proceedings*, 2007, pp. 1–5. [Online]. Available: www.scopus.com 27

[36] M. Askarzadeh, M. Hosseinzadeh, and K. Navi, "A new approach to overflow detection in moduli set 2n-3, 2 n-1, 2n+1, 2n+3," in *2009 International Conference on Computer and Electrical Engineering, ICCEE 2009*, vol. 1, 2009, pp. 439–442. [Online]. Available: www.scopus.com 27

[37] R. C. Debnath, D. A. Pucknell, and D. A. Pucknell, "On multiplicative overflow detection in residue number system." *Electronics Letters*, vol. 14, no. 5, pp. 129–130, 1978. [Online]. Available: www.scopus.com 27

[38] B. A. Forouzan, *Cryptography and Network Security*, special indian ed. Tata McGraw-Hill, 2008. 29, 30

[39] N. Bourbakis and C. Alexopoulos, "Picture data encryption using scan patterns,"

Pattern Recognition, vol. 25, no. 6, pp. 567–581, 1992, cited By (since 1996): 109. [Online]. Available: www.scopus.com 30

[40] H. K. Chang and J. Liu, "A linear quadtree compression scheme for image encryption," *Signal Processing: Image Communication*, vol. 10, no. 4, pp. 279–290, 1997, cited By (since 1996): 42. [Online]. Available: www.scopus.com 30

[41] C. Chang, M. Hwang, and T. Chen, "A new encryption algorithm for image cryptosystems," *Journal of Systems and Software*, vol. 58, no. 2, pp. 83–91, 2001, cited By (since 1996): 70. [Online]. Available: www.scopus.com 30

[42] H. Cheng, "Partial encryption of compressed images and videos," *IEEE Transactions on Signal Processing*, vol. 48, no. 8, pp. 2439–2451, 2000, cited By (since 1996): 179. [Online]. Available: www.scopus.com 30

[43] H. M. A. K. D. S. A. Elminaam and M. M. Hadhoud, "Evaluating the performance of symmetric encryption algorithms," *International Journal of Network Security*, vol. 10, no. 3, pp. 213–219, 2010. 30

[44] N. E. Fishawy and O. M. A. Zaid, "Quality of encryption measurement of bitmap images with rc6, mrc6, and rijndael block cipher algorithms," *International Journal of Network Security*, vol. 5, no. 3, pp. 241–251, 2007. 30

[45] S. Moriai and Y. L. Yin, "Cryptanalysis of twofish(ii)," *Technical Report of IEICE*, 2000. 30, 34

[46] B. Schneier, "Description of a new variable-length key, 64-bit block cipher (blowfish)," *Springer LNCS*, vol. 809, pp. 191–204, 1994. 34

[47] N. Ferguson, "Impossible differentials in twofish," 1999. 34

[48] Q. Huynh-Thu and M. Ghanbari, "Scope of validity of psnr in image/video quality assessment," *Electronics Letters*, vol. 44, no. 13, pp. 800–801, 2008, cited By (since 1996): 31. [Online]. Available: www.scopus.com 35

[49] B. Girod, *What's wrong with mean-squared error? in Digital images and human vision*. MIT Press Cambridge, 1993. 35

[50] D. Salomon, *Data Compression The Complete Reference*, 4th ed. Springer, 2007. 35

[51] R. W. Gonzalez, R.C., *Digital Image Processing Using MATLAB*, 2nd ed., A. Dworkin, Ed. New Jersey, Prentice Hall, 2003. 38

[52] R. C. Dixon, *Spread Spectrum System with Commercial Application*, 3rd ed. Wiley-Interscience, 1994. 43

[53] R. Gold, "Optimal binary sequences for spread spectrum multiplexing," *IEEE Transactions on Information Theory*, vol. 13, pp. 619–621, 1967. 45

[54] S. Haykin, *Communication Systems*, 4th ed. John Wiley and Sons, 2004. 45

Publications

7.1 Journal

1. Pallab Maji and GS Rath," Design of Low Pass FIR Filter based on Residue Arithmetic", International Journal of Science and Technology (IJSAT),2011.(In Press)

7.2 Conference

1. Pallab Maji and G. S. Rath," A Novel Design Approach for Low Pass Finite Impulse Response Filter Based on Residue Number System", IEEE 3rd ICECT, Kanyakumari, India, 2011.

2. Pallab Maji and G. S. Rath," Bit Efficient Finite Impulse Response Filter based on Residue Arithmetic", ICSSA-11, Gujarat, India, 2011.