Generalized Information Security and Fault Tolerant based on Redundant Residue Number System

Idris Abiodun Aremu
Computer Science Department
School of Technology
Lagos State Polytechnics, Lagos

Kazeem Alagbe Gbolagade
Department of Computer Science
College of ICT
Kwara State University, Malete

ABSTRACT
Residue number systems bestow a first class means for exceptionally long integer arithmetic. Their carry-free operations make parallel implementations feasible. Some applications involving very long integers, such as information security, rely heavily on fast modulo reductions. Information Security is an extensive issue and covers a huge number of crimes. In its simplest form, it is concerned with making sure that curious people cannot read or modify messages anticipated for other recipients, and Fault-tolerant computing is the art and science of building computing systems that continue to operate adequately in the presence of faults. In this paper, a generalized information security and fault tolerant system using Redundant Residue Number System (RRNS) was proposed, the theoretical result show that our proposed scheme is out performed better compared with the state of the art in term of the computation time and space, called Delay and Area respectively and also provides more security to the data.

General Terms
Information Security, Fault Tolerant, Data communication, Sensors Network

Keywords
Residue Number System (RNS), Redundant Residue Number System (RRNS), Mixed-Radix Conversion (MRC), Chinese Remainder Theorem (CRT)

1. INTRODUCTION
Fault tolerance and Information security started as two separate research fields, leading to related but different taxonomy, tactic, and technologies. Information Security is an extensive issue and covers a huge number of crimes. In its simplest form, it is concerned with making sure that curious people cannot read, or modify messages anticipated for other recipients. It is concerned with people trying to access remote services that they are not authorized to use. Information security can be identified by three facets [1] [2]. The concepts can be seen as the objectives with security regarding Information Technology and Information security [3]. The three facets of information security are Confidentiality, Integrity and Availability. Confidentiality is the avoidance of unauthorized disclosure of the information assets; integrity is the prevention of unlawful modification of the information assets, while availability is to give right of entry to information when required. A fault tolerant system possibly will tolerate the following fault types which including-transient, intermittent or permanent hardware faults, software and design errors, operator errors, or externally induced upsets or physical damage [4]. The rest of this paper is organized as follows. Section 2 presents the fault tolerance Section 3 provides an overview of residue number system section 4 presents redundant residue number system Section 5 Discuss the proposed error correction and detention using RRNS. Section 6 demonstrates the application of the proposed scheme in data communication. Section 7 present the performance evaluation and section 8 discussed the conclusions.

2. FAULT TOLERANCE
The integrity of data has tremendous effects on the performance of any data acquisition system. Noise and other disturbances can often degrade the information or data acquired from these systems. Devising a fault-tolerant mechanism in wireless sensor networks is very important due to the construction and deployment characteristics of these low powered sensing devices. Faults can be classified to permanent, intermittent and transient faults according to their duration [5]. Because there are different types of faults also the methods for tolerating them are different. In most cases, a single fault tolerance method is not an optimal solution for all types of faults. This gives rise to the idea of combining a set of fault tolerance methods which together can provide the desired fault tolerance.

3. RESIDUE NUMBER SYSTEM
Residue number system is a technique in which an integer is represented by a set of remainders that are obtained after the modulo division by a set of relatively prime moduli. The process of converting a weighted number system to residue format is called RNS encoding [6]. Consider an arbitrary integer X and a set of v relatively prime integers $(m_1, m_2, \ldots . m_v)$ called moduli with M as the product of all moduli [7]. i.e.

$$M = \prod_{i=1}^{n} m_i$$

Then integer X can be represented as a set of n remainders $(r_1, r_2, \ldots r_n)$ where $r_i = X \bmod m_i$
The dynamic range of the RNS is given by M and the set [0,*M - 1*] gives the legitimate range such that all integers in this range can be represented as residues by this set of moduli[8]. The dynamic range R for negative numbers is given as

$$R = -\frac{M-1}{2}, \frac{M-1}{2} \quad \text{if M is odd}$$

$$R = -\frac{M-1}{2}, \frac{M}{2} - 1 \quad \text{if M is even}$$

Arithmetic operations using RNS has the merit of carry free property. Therefore, in RNS the arithmetic operations performed are mutually independent between residue digits [9]. Let X_1 *and* X_2 be two integers
Xl ● X2⟺$(r_1 * r_2)$ mod mi, i = 1, 2, ... n
(3)

Where • denotes arithmetic addition, subtraction or multiplication and $r_1 and\ r_2$ are residues of X1 and X2 with respect to moduli mi.

The binary number system, decimal and hexadecimal traditional numbers are linear and are highly reliant on the order of the digits. In all these systems, each bit position is associated with a weight and these weights are derived from the same base (radix). For example, in binary number system, the base is 2 and the weights are (2^0, 2^1, 2^2 ...) and in decimal number system, the base is 10 and the weights are (10^0, 10^1, 10^2 ...). Residue number system helps to increase the speed of arithmetic operations like addition, subtraction and multiplication when compared to traditional number systems [10]. Residue number system (RNS) is a non-weighted, non positional number system which can be represented by specifying its base. Unlike Decimal or Binary Number System, it does not have a single fixed radix. The bases of RNS are represented by an n-turple of integers $\{m_1, m_2, \ldots\ldots, m_n\}$ where each of these bases is called a modulus. Thus, in RNS any given integer is represented by a set of residues which are obtained by modulo dividing the integer with moduli set [10].

The moduli are usually relatively prime to each other. So large calculations can be decomposed into a series of smaller parallel calculations and thus RNS can be used for application in the field of digital computer arithmetic.

4. REDUNDANT RESIDUE NUMBER SYSTEM

Redundant Residue Number System (RRNS) is achieved by adding some redundancy to the RNS.

RRNS helps in both error correction and error detection. By adding (u - w) redundant moduli ($m_{w+1}, m_{w+2}, \ldots\ldots m_w$) to the v information moduli ($m_1, m_2, \ldots\ m_w$), a RRNS (u, w) code can be generated. This process is called RRNS encoding. Thus an integer X is represented in the RRNS form as

X= $\{r_1, r_2 \ldots\ldots r_w, r_{w+1} \ldots\ldots r_u\}$ (4)

Where ($m_1, m_2 \ldots\ldots m_w$) are called information moduli and ($m_{w+1}, m_{w+2} \ldots\ldots m_w$) are called redundant moduli[5]. Similarly ($r_1, r_2 \ldots\ldots r_w$) are called information residues and ($r_{w+1}, r_{w+2} \ldots r_w$) are called redundant residues. M_r denotes the product of redundant moduli. In RRNS, the legitimate range is defined as [0, M] and illegitimate range indicating overflow, where residues are obtained using redundant moduli, is [M, M, M_r].

RRNS can be used for error detection and error correction, self checking in digital computers [10]. Thus it helps in the design of general purpose systems, which are capable of sensing and rectifying their own transmission and processing errors [10] .

The use of RRNS for error detection and correction has many advantages over the conventional error codes. The arithmetic operations like addition, subtraction and multiplication are carrying free in RNS. This implies that the error due to these operations or due to noise does not propagate from one residue digit to other. They remain confined to the original residues [10]. Another important advantage of RNS arithmetic operation is lack of ordered significance among residue digits. Therefore, an integer can be recovered from its residues even after discarding some of the redundant residues, provided that the retained residue digits should be correct [11]. This has resulted in the development of a number of error detection and error correction algorithms.

The decoding of Redundant Residue Number System is commonly carried out using Chinese Remainder Theorem (CRT) [10][11][12][13]. Implementation of CRT decoder at the receiver results in a computational complexity of order 0(n3), where n is the number of non redundant moduli [11]. An alternate scheme called Mixed Radix Conversion (MRC) can be used which yields a low complexity of O (n) [14] [15]. The algorithm used in this paper uses both CRT and MRC techniques at the decoder for comparison.

Theorem 1

RRNS (u - w, v) code has a detection capability of (u - w - v) errors and an error correction capability of (u - w - v) /2 [16]. The code rate of a redundant residue number system can be defined as

$$kb = \frac{kb}{\sum_{i=1}^{u} kb} \qquad (5)$$

where kb = $\lfloor log_2 m_r \rfloor$ and $k_{bj} = \lfloor log_2 m_j \rfloor$, where m_j, (j = 1,2 ... u) are the moduli. By varying the number of redundant bits that are transmitted, the code rate and error correction capability are varied. Redundancy is added to the information/data, therefore the code rate decreases and error correction property is improved. In RNS, the number of non-zero elements in a vector is defined as its hamming weight. Let X_i and X_j are two code vectors, then hamming distance d (X_i, X_j) is defined as the number of bits in which two code vectors Xi and X_j differ. Minimum distance, d is the minimum of hamming distances

d = min (d (x_i, x_j); $x_i \neq X_j$). (6)

Theorem 2

The minimum hamming distance d of an RRNS (u, w)-code is defined as d = u - w + 1, provided ($m_1 < m_2 \ldots\ldots < m_w < m_{w+1} < \cdots < m_u$)

Theorem 3

For a redundant residue number system, the error detecting capability, c = d - 1 and the error correcting capability [17],

t = $\left\lfloor {}^{d-1}/_{2} \right\rfloor$ 2 where $\lfloor a \rfloor$ is the largest integer smaller than a. Thus RRNS (u, w) code can detect up to u - w residue digits and can correct up to t = $\left\lfloor {}^{u-w}/_{2} \right\rfloor$ residue digits. This means that single error and multiple error correction algorithms can be developed by suitably selecting u and w.

5. PROPOSED ERROR DETECTION AND CORRECTION USING RRNS

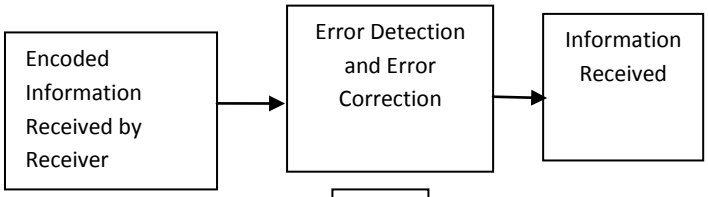

Fig 1

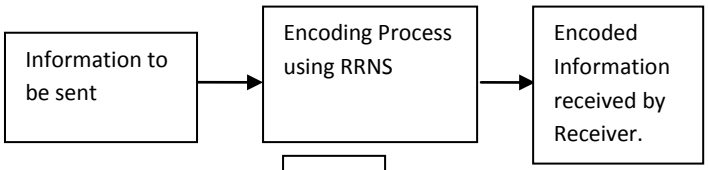

Fig 2

The Information Encoding and Decoding Process of the proposed

DATA CONVERSION

Given the moduli set $\{m_1, m_2, \ldots, m_n\}$ and $\{m_{n+1}, m_{n+2}, \ldots, m_m\}$ with residue representation

$\{x_1, x_2, \dots, x_n\}$ and $\{x_{n+1}, x_{n+2}, \dots, x_m\}$ for the information and redundant data sets respectively. The decimal equivalent is given as:

$$X = \left| \sum_{i=1}^{n} M_i |M^{-1}|_{m_i} x_i \right|_M$$

Such that

$$M = \prod_{i=1}^{n} m_i$$

$$M_i = \frac{M}{m_i}$$

M^{-1} Is the multiplicative inverse of M_i with respect tom_i?

Theorem 1:

Given the moduli set $2^{2n} - 1, 2^{2n}\ and\ 2^{2n} + 1$ are relatively co-prime numbers.

Proof:

From the Euclidean theorem, we have $\gcd(a, b) = \gcd(b, |a|_b)$ therefore

$\gcd(2^{2n} - 1, 2^{2n}) = \gcd(2^{2n} - 1, |2^{2n}|_{2^{2n}-1}) =$
$\gcd \gcd(2^{2n} - 1,1) = 1$. Similarly, $\gcd(2^{2n} - 1, 2^{2n} + 1) =$
$\gcd(2^{2n} - 1, |2^{2n} + 1|_{2^{2n}-1}) = \gcd(2^{2n} - 1,2) = 1$ and
$\gcd(2^{2n}, 2^{2n} + 1) = \gcd(2^{2n} - 1, |2^{2n} + 1|_{2^{2n}}) =$
$\gcd(2^{2n}, 1) = 1$.

Theorem 4:

Given the information moduli set $2^{2n} - 1, 2^{2n}\ and\ 2^{2n} + 1$ such that $m_1 = 2^{2n} - 1, m_2 = 2^{2n}\ and\ m_3 = 2^{2n} + 1$, the following condition is true:

$$|(m_2 m_3)^{-1}|_{m_1} = 2^{2n-1}$$
$$|(m_1 m_3)^{-1}|_{m_2} = -1$$
$$|(m_1 m_2)^{-1}|_{m_3} = -2^{2n-1}$$

Theorem 5:

Given the moduli set$\{2^{2n} - 1, 2^{2n}\ and\ 2^{2n} + 1\}$, the RNS number (x_1, x_2, x_3) can be converted to conventional number X as follows:

$$X = m_2 \left\lfloor \frac{X}{m_2} \right\rfloor + x_2$$

$$\left\lfloor \frac{X}{m_2} \right\rfloor = |2^{2n-1} m_3 x_1 - m_2 x_2 - 2^{2n-1} m_1 x_3|_{m_1 m_3}$$

Proof:

It has been demonstrated in [18].

INFORMATION ECODING ALGORITHM

Step 1:
Input the information to be sent

Step 2:
Input the both the Information and Redundant Moduli set

Step 3:
Encode the Information using both Information and Redundant moduli set to have both information and redundant residue digits

Step 4:
Send the encoded information to the receiver

Step 5:
Stop

ERROR DETECTION ALGORITHM

Step 1:
Input the received information

Step 2:
Decode the information using the adopted Chinese Remainder Theorem

Step 3:
Use the redundant moduli set to do consistency checking via Forward Conversion Technique

Step 4: **Report if there is error otherwise goto Step 5**

Step 5: **Stop.**

ERROR CORRECTION ALGORITHM

Step 1: **Input the erroneous information**

Step 2: **Determine which channel is faulty**

Step 3: **Use Based Extension via Redundant Moduli set to correct the error**

Step 4: **Restored the correct information**

Step 5: Stop.

6. APPLICATION OF THE PROPOSED SCHEME TO DATA COMMUNICATION

Given the moduli set $\{m_1, m_2, \dots\dots, m_n\}$ and $\{m_{n+1}, m_{n+2}, \dots\dots, m_m\}$ with residue representation $\{x_1, x_2, \dots\dots, x_n\}$ and $\{x_{n+1}, x_{n+2}, \dots\dots, x_m\}$ for the information and redundant data sets respectively. The information moduli set are use to encode information and redundant moduli set are use to detect and correct error.

Given the information moduli set $2^{2n} - 1, 2^{2n}\ and\ 2^{2n} + 1$ such that $m_1 = 2^{2n} - 1, m_2 = 2^{2n}\ and\ m_3 = 2^{2n} + 1$. Assuming $n = 2$ then$m_1 = 15, m_2 = 16\ and\ m_3 = 17$.

Given the redundant modulus $2^{2n+1} - 1\ and\ 2^{2n-1} + 1$ such that $m_4 = 2^{2n+1} - 1\ and\ m_5 = 2^{2n-1} - 1$. Assuming $n = 2$ then $m_4 = 31\ and\ m_5 = 7$.

Consider an integer $X = 125$ which is encoded in to Redundant Residue Number System using both information and redundant moduli set (16, 17, 15, 31, 7) where the information moduli are (16, 17, 15) and redundant moduli set are (31, 7) respectively. The RRNS representation of $X = 125$ is$(13, 6, 5, 1, 6)$. Assuming that x_1 is changed to 5 from 13. Then the information received is$(5, 6, 5, 1, 6)$. The decoding is done using the adopted Chinese remainder theorem [18]. We have.

$$X^r = m_1 \left\lfloor \frac{X^r}{m_1} \right\rfloor + x_1$$

Where

$$\left\lfloor \frac{X^r}{m_1} \right\rfloor = |-m_1 x_1 - 2^{2n-1} m_3 x_2 + 2^{2n-1} m_2 x_3|_{m_2 m_3}$$

From the information received above $n = 2,\ m_1 = 15, x_1 = 5, m_3 = 17, x_2 = 5, m_2 = 16\ and\ x_3 = 6$. Then

$$\left\lfloor \frac{X^r}{m_1} \right\rfloor = |-16 \times 5 - 8 \times 15 \times 6 + 8 \times 17 \times 5|_{17 \times 15}$$

$$\left\lfloor \frac{X^r}{m_1} \right\rfloor = |-80 - 720 + 680|_{255}$$

$$\left\lfloor \frac{X^r}{m_1} \right\rfloor = |175 + 45 + 170|_{255} \left\lfloor \frac{X^r}{m_1} \right\rfloor = |390|_{255}$$

$$\left\lfloor \frac{X^r}{m_1} \right\rfloor = 135$$

And

$$X^r = m_1 \left\lfloor \frac{X^r}{m_1} \right\rfloor + x_1$$
$$X^r = 16 \times 135 + 5$$
$$X^r = 2165$$

Now to perform consistency checking, we have

$$x_4 = |X^r|_{m_4} = 1 = |2165|_{31} : No$$
$$x_5 = |X^r|_{m_5} = 6 = |2165|_7 : No$$

The error is reported.

Then we performed the error correction using substitution method we proposed, we have

$$(x_1, x_3 x_4)_{RNS(m_1, m_3, m_4)} = (5,5,1)_{RNS(16/15/31)} = 3845$$

$$(x_2, x_3x_4)_{RNS(m_2,m_3,m_4)} = (6,5,1)_{RNS(17/15/31)} = 125$$
$$(x_1, x_2x_4)_{RNS(m_1,m_2,m_4)} = (5,6,1)_{RNS(16/17/31)} = 125$$

Table 1: Information encoding at receiver site with respect to redundant moduli set.

Moduli Set	x_1	x_3	x_4	Decimal Equivalent
16	5	5	1	3845
15				
31				
Moduli Set	x_2	x_3	x_4	Decimal Equivalent
17	6	5	1	125
15				
31				
Moduli Set	x_1	x_2	x_4	Decimal Equivalent
16	5	6	1	3845
17				
31				

In the above table we performed consistency checking using m_4 and m_5 we have

For Channel 1

$$x_4 = |3845|_{m_4} = 1 = |3845|_{31}: Yes$$
$$x_4 = |3845|_{m_4} = 6 = |3845|_{7}: No$$

For Channel 2

$$x_4 = |125|_{m_4} = 1 = |125|_{31}: Yes$$
$$x_4 = |125|_{m_5} = 6 = |125|_{7}: Yes$$

For Channel 3

$$x_4 = |125|_{m_4} = 1 = |125|_{31}: Yes$$
$$x_4 = |125|_{m_5} = 6 = |125|_{7}: Yes$$

Therefore, we concluded that there is error in channel 1.

To restored the faulty channel we have

$$x_1 = |125|_{m_1} = |125|_{16} = 13$$

Therefore the corrected information from the receiver site is $(13,6,5)_{RNS(16/17/15)}$.

7. PERFORMANCE EVALUATION

This paper, proposed a new error detection and correction approach that is based on redundant residue number system. This approach results in faster encoding and decoding procedures and has following advantages over the following existed works.

1. It is a generalized based. That's the choice of moduli selected can works for any kinds of dynamic range because n is the determinant factor of the system.
2. The existing works as suggested algorithm for single error detection and correction with magnitude index, whereas the proposed approach is general for multiples channel errors.
3. The choice of moduli selected provides a very effective and efficient encoding and decoding process for detecting and correcting errors.

8. CONCLUSION

In this paper, we proposed a single error detection and correction using RRNS, our scheme provide information security in term of the information encoding using Redundant Residue Number System, and also maintain the information integrity because is capable of detecting and correct error at the cost of transmission. Our proposed scheme is performed better compared with state of the art because we adopted a very large dynamic range moduli set proposed [18] and very effective and efficient reverse converter proposed in [18].

However, RNS coding are good for fast computation and arithmetic operation, which help in Digital Signal Processor (DSP). An attempt may be advantageous to simplify the encoding as well as decoding.

9. REFERENCES

[1] Gollmann, Dieter(2010). Computer security Wiley Interdisciplinary Reviews: Computational Statistics, 544-554

[2] Harris, S. (2002). *Mike Meyers' Cissp Certification Passport with Cdrom*. Osborne/McGraw-Hill.

[3] Jonsson, E. (1996). *A quantitative approach to computer security from a dependability perspective*. Chalmers University of Technology,.

[4] Meshram, A. D., Sambare, A. S., & Zade, S. D. (2013). Fault tolerance model for reliable cloud computing. *International Journal on Recent and Innovation Trends in Computing and Communication*, *1*(7), 600-603.

[5] Constantinescu, C. (2003). Trends and challenges in VLSI circuit reliability. *IEEE micro*, *23*(4), 14-19.

[6] Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). Wireless sensor networks: a survey. *Computer networks*, *38*(4), 393-422.

[7] Gbolagade, K. A. (2010). Effective reverse conversion in residue number system processors.

[8] Younes, D., & Steffan, P. (2012, December). A comparative study on different moduli sets in residue number system. In *Computer Systems and Industrial Informatics (ICCSII), 2012 International Conference on* (pp. 1-6). IEEE.

[9] James, J., & Pe, A. (2015, July). Error correction based on redundant Residue Number System. In *Electronics, Computing and Communication Technologies (CONECCT), 2015 IEEE International Conference on* (pp. 1-5). IEEE.

[10] Yau, S. S., & Liu, Y. C. (1973). Error correction in redundant residue number systems. *IEEE Transactions on Computers*, *100*(1), 5-11.

[11] Sengupta, Avik, Dalin Zhu, and Balasubramaniam Natarajan (2012). On the performance of redundant residue number system codes assisted STBC design Computing, Networking and Communications (ICNC), International Conference on. IEEE,.

[12] Krishna, H., & Sun, J. D. (1993). On theory and fast algorithms for error correction in residue number system product codes. *IEEE Transactions on Computers*, *42*(7), 840-853.

[13] Siewobr, Hillary, Kazeem A. Gbolagade, and Sorin Cotofana (2014). An efficient residue-to-binary converter for the new moduli set {2 n/2±1, 2 2n+1, 2 n+ 1}.International Symposium on Integrated Circuits (ISIC). IEEE,.

[14] Amusa, K., & Nwoye, E. (2012). Novel algorithm for decoding redundant residue number systems (RRNS) codes. *integers*, *1*, 7.

[15] Krishna, H., Lin, K. Y., & Sun, J. D. (1992). A coding theory approach to error control in redundant residue

number systems. I. Theory and single error correction. *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*, *39*(1), 8-17.

[16] Bagri, D. S., Statman, J. I., & Gatti, M. S. (2007). Proposed array-based deep space network for NASA. *Proceedings of the IEEE*, *95*(10), 1916-1922.

[17] Tay, T. F., & Chang, C. H. (2016). A non-iterative multiple residue digit error detection and correction algorithm in RRNS. *IEEE transactions on computers*, *65*(2), 396-408.

[18] Bankas, E. K., & Gbolagade, K. A. (2013). A New Efficient FPGA Design of Residue-To-Binary Converter. *International Journal of VLSI Design & Communication Systems*, *4*(6), 1.