Efficient Image Encryption Scheme Based on the Moduli Set $\{2^n - 1, 2^n, 2^n + 1\}$

[*1]Saheed, Y.K. and [2]Gbolagade, K.A.

[1]Department of Physical Sciences, Al-Hikmah University, Ilorin, Nigeria
[2]Department of Computer Science, Kwara State University, Malete, Nigeria

Received: August 28, 2016; Revised: November 30, 2016; Accepted: December 1, 2016

Abstract

This paper presents an image encryption scheme that utilizes three moduli set. The proposed scheme is based on three moduli set $\{2^n-1, 2^n, 2^n+1\}$, which is efficient, required little hardware, and did not diminish the Residue Number System dynamic range. Also, it promises high speed, reduces area, decreases internal delay conversion from Residue Number System (RNS) to binary. This is because in the reverse converter, the computation of the multiplicative inverse is removed and it achieves low-power very large scale integration implementation for image processing such as digital image filtering. The end results of the RNS image encoder in this new scheme are in small-word length and are arranged in a certain encrypted order. A Residue-Binary converter (decoder) is used to recover the plain image. The proposed scheme is simulated on an image using matrix laboratory tool. An attacker who breaks into network does not know the moduli set and the order of the encrypted bit stream that are computed in parallel. The scheme can be applied to any image formats as against the best known state-of-the-art.

Keywords: Residue number system (RNS), Digital Image, Very Large Scale Integration, Reverse Converter

1.0 Introduction

Data encryption is important to the security and integrity of information to be transmitted through a network [1]. The need for a secured communication is more profound than ever, recognizing the fact that the conduct of almost all our business and personal matters are carried out today by computer networks. Different approaches have been proposed to perform the encryption of an image. The approach presented by Wei *et al* [2] is restricted to joint photographic expert group file format (JPEG), the algorithm used is modified Chinese remainder theorem. In another study, an encryption scheme using Chinese remainder theorem was employed which supports only gray scale image and not suitable for VLSI implementation [1].

Digital image processing has been extensively used in desktop publishing, medical imaging, military target analysis, manufacture automation control, machine vision, geo-physical imaging, graphic arts and multimedia [3]. Most of these applications depend on the availability of compact and inexpensive hardware delivering the required high performance so that very large scale integrated (VLSI) technology is of vital importance for digital image processing [4].

The security of information and digital images has become a major concern for the past few decades due to the rapid advancement in internet and networking technologies [1]. Hence, in an environment where data encryption applications are fast-evolving, an algorithm that offers efficient and low-complexity encryption can provide security for information against intrusion and sophisticated threats that are currently ubiquitous [5]. Moreover, the information that has to be transmitted must be encrypted to reduce the size of the data and increase processing speed. With the increasing use of digital techniques for transmitting and storing images, the fundamental issue of protecting the confidentiality, integrity as well as the authenticity of images has become a major concern. Over the years, various hidden and secret communication techniques aimed at addressing this need, have been proposed [6-9].

***Corresponding Author: Tel: +234(0)8142683364, E-mail: yksaheed@alhikmah.edu.ng**

The VLSI implementation of digital image processing systems requires high-speed and low-power techniques, as well the consideration of a certain measure of security during the transmission. One of the methods of designing high- speed and low-power VLSI digital systems is by using the residue number system (RNS) [4]. The RNS has no carry chain and offers high-speed operations [10,11]. The high-speed gained by the RNS parallelism can then be traded-off for low power consumption [12,13]. In this paper, enhancement of Residue Number System in encryption and decryption of image based on three traditional moduli set with the assistance of New Chinese Remainder Theorem algorithm is addressed.

2.0 Materials and Methods

A residue number system is defined in terms of a relatively-prime moduli set $\{P_1, P_2, \ldots\ldots, P_n\}$ that is $\gcd(P_i, P_j) = 1$ for $i \neq j$. A weighted binary number X can be represented as $X=(x_1, x_2, \ldots, x_n)$, where

$$x_i = X \bmod P_i = /X/_{pi}\ , \ 0 \leq x_i < P_i \qquad (1)$$

Such a representation is unique for any integer X in the range [0, M-1], where $M=P_1\ P_2 \ldots P_n$ is the dynamic range of the moduli set {P1, P2… Pn} [14]. Addition, subtraction and multiplication on residues can be performed in parallel without carry propagation. Hence, by converting the arithmetic of large numbers to a set of the parallel arithmetic of smaller numbers, RNS representation yields significant speed up. Binary to residue conversion is very simple and can be implemented with modular adders [15]. When binary to residue conversion of the needed operands had finished, arithmetic operations on RNS numbers are performed in parallel without carry-propagation between residue digits. Hence, RNS leads to carry-free, parallel and high-speed arithmetic. It should be noted that each modulo of the moduli set has its own arithmetic processor which consists of a modulo adder, a modulo subtractor and a modulo multiplier. In order to use the result of arithmetic operations in outside of RNS, the resulted RNS number must be converted into its equivalent weighted binary number. The algorithms of residue to binary conversion are mainly based on CRT, MRC and New CRTs [16]. The CRT is defined as follows according to the study of Mi [17].

Given a moduli set $\{m_1, m_2, m_3, \ldots, m_n\}$ with $\gcd(m_i, m_j) = 1$ for $i \neq j$ and dynamic range $M = \prod_{i=1}^{n} m_i$, then by the CRT an integer X whose RNS representation is $(x_1, x_2, x_3 \ldots x_n)$ can be converted from its residue form as

$$X = \left|\sum_{i=1} n M_i \left| M^{-1} y_i \right|_{mi} \right|_m , \qquad (2)$$

Where $M_i = m/m_i$ and M_i^{-1} is the multiplicative inverse of M_i with respect to m_i.

The CRT requires a modulo M (large-valued) operation, which is not very efficient. Recently, some new general alternative conversion algorithms, the new Chinese remainder theorems (New CRT-I, II and III) have been proposed [18].

2.1 New Chinese Remainder Theorem-I (New CRT-I)

Given the residue number $(x_1, x_2, \ldots . x_n)$, the corresponding decimal number X can be computed by $X = x_1 + P_1 |k_1 (x_2 - x_1) + k_2 P_2 (x_3 - x_2) + \ldots . + k_{(n-1)} P_2 \ldots P_{n-1} (x_n - x_{n-1})|_{p3 \ldots pn-1p}$

Where $k_1 P_1 = 1 \bmod P_2 \ldots P_n$, $k_2 P_1 P_2 = 1 \bmod P_3 \ldots P_n, \ldots, k_{(n-1)} P_1 \ldots P_{n-1} = 1 \bmod P_n$

Based on the new CRT-I, the following proposition for n=3 are available.

Proposition 1 [18]:

For a three moduli set (P_1, P_2, P_3), the binary number $X = (x_1, x_2, x_3)$ can be calculated as

$$X = x_1 + |k_1 (x_2 - x_1) + k_2 P_2 (x_3 - x_2)|_{p2p3} P_1 \qquad (3)$$

Where $k_1 P_1 = 1 \bmod P_2 P_3$ and $k_2 P_1 P_2 = 1 \bmod P_3$

Based on New Chinese Remainder Theorem, efficient residue-to-binary conversion algorithm have been proposed and the design of several efficient residue-to-binary converter technique [19,20]. The proposed image decoder residue-to-binary converter can be very efficiently designed using VLSI technology.

Thus, the proposed encoder part, the moduli set is selected according to this proposed method. For example, for the [0,255] range png image data, the moduli set {7,8,9} for the encoder design can be selected. Thus, the encoder consists of three 3-bit channels of RNS image processors. The B/R converters and the three RNS image processors are based on the three low-cost moduli {7,8,9} and can be efficiently implemented using VLSI technology.

2.2 Proposed Image Encryption and Decryption Technique

The image coding scheme consists of two parts: the encoding and decoding parts, based on the moduli set $\{2^n-1, 2^n, 2^n+1\}$. The encoder is built by a Binary-to-Residue converter, which requires an RNS image processor of small word length. The decoder is a Residue-to- Binary converters used to retrieve the encrypted bit stream according to the moduli set chosen.

2.3 Encoding and Decoding Process

The proposed designed system is divided into two main categories. The first category deals with the encoding that is mainly carried out by the encoder (Binary-to-residue converter). The other category is the decoding, which is implemented by the decoder Residue-to-Binary converter.

Category A: Encoding Part

1. The original digital image is read as a binary or decimal value.
2. The digital image data are encrypted into bitstream in a certain order according to the moduli set.
3. The encrypted bitstream is processed by the RNS image processor; hence the resulting image is encrypted.
   The proposed encoder is shown in Fig. 1.

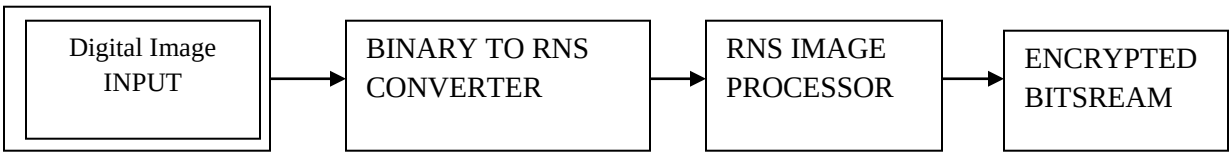

Fig. 1: Proposed Encoding Scheme

Category B: Decoding Part

1. The encrypted digital image is received and recognized each residue number.
2. Decode the encrypted bitstream back to binary.
   The proposed decoder is illustrated in Fig. 2.

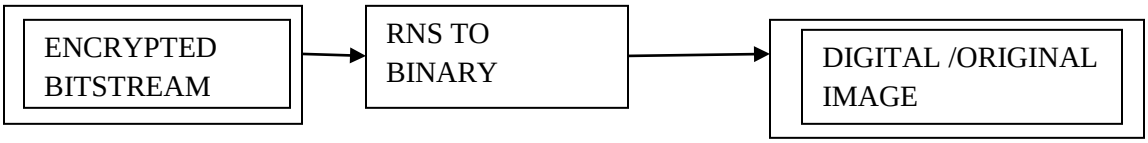

Fig. 2: Proposed Decoding Scheme

3.0 Results and Data Analysis

3.1 Security of the Proposed Image Scheme

Compared to the binary image coding, the proposed RNS image processing scheme has an encoder and a decoder, which is modeled based on the operation of a three moduli set $\{2^n-1, 2^n, 2^n+1\}$. The end results of the RNS image encoder in this new scheme are of small word length and are arranged into a certain encrypted bit stream in a certain order. An eavesdropper who breaks into the network does not know the moduli set and the order of the encrypted bit stream that are computed in parallel.

The decoder is a Residue-to-Binary converter to recover the encrypted bit stream in the corresponding order back to the processed image data. The proposed method achieves high-speed and low-power VLSI implementation for image processing such as digital image transform and digital image filtering. The design of the scheme is based on the residue to binary converter [19,20].

3.2 Comparison of Results

The approach presented in this paper is compared to the RNS image coding scheme according to Ammar *et al* [1]**.** The proposed scheme is more efficient for VLSI implementation. As illustrated in Table 1, the proposed scheme RNS algorithm is New Chinese Remainder Theorem, while the RNS image coding scheme [1] is based on traditional Chinese remainder theorem which requires a modulo-M (large valued) operation and it is not efficient for the implementation.

In addition, the proposed scheme moduli selection method and Residue to Binary converter design is efficient because it requires no explicit use of modulo operation. This gives our approach added advantage in terms of both area and delay. Furthermore, the approach proposed is suitable for all types of image formats and encrypts the whole image.

Fig. 3 is the image that is encoded by the proposed scheme. An attacker who breaks into a network does not know the moduli set and the order of the encrypted bit stream that are computed in parallel. Fig. 4 presents the histogram of the input image that is input to the encoder. Fig. 5 is the output image to the decoder while Fig. 6 is the histogram of the output image that is output to the decoder. RNS serves three goals in this paper namely to increase the speed of transmission, reduce the area of image data and increase the security level of transmission through computer networks.

Table 1: Comparison of the RNS Encryption Scheme

Schemes	**The range of Encryption**	**Image coding component**	**VLSI Implementation**	**Image formats**	**RNS Algorithm**
Ammar *et al* (2001)	Part of the image	Several in both encoding and decoding part	Not suitable	Grayscale image	CRT
Wei *et al* (2004)	Whole picture	Both encoding and decoding.	Suitable	Jpeg	Modified CRT
Proposed scheme	Whole picture	Both encoding and decoding	Suitable	All image formats	NCRT

Fig. 3: Input image to the encoder

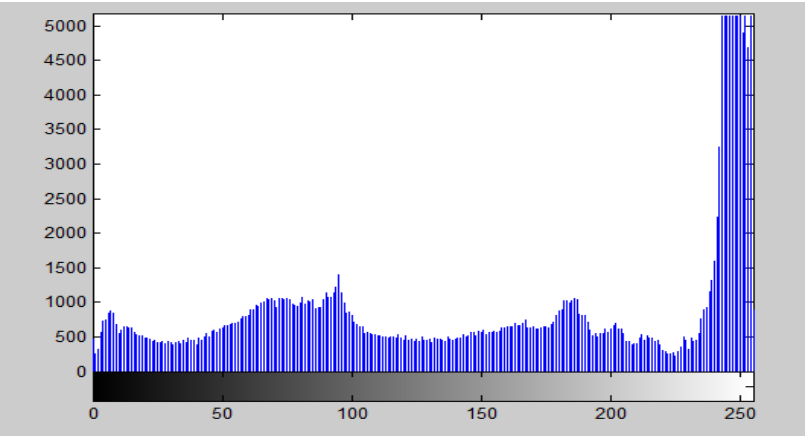

Fig. 4: Histogram of the input image showing the distribution of the image pixels

Fig. 5: Output image of the decoder

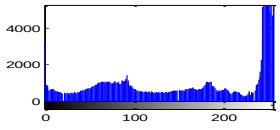

Fig. 6: Histogram of the output image showing the distribution of the image pixels

4.0 Discussion

In this study, the researchers investigated the application of RNS in digital image processing and proposed an encryption scheme that is based on moduli set $\{2^n -1, 2^n, 2^n +1\}$ that offers high speed, reduce area and low power VLSI implementation for secure image processing. The end results of the RNS image encoder in this new scheme are in small word length and are arranged in an encrypted order. A third party who breaks into the network does not know the moduli set. Further, the proposed scheme is based on New Chinese remainder theorem algorithm which is more efficient than earlier approaches in

terms of VLSI implementation and image format. The design of encoder, decoder for the image was carried out using MATLAB tool. The results of the MATLAB simulation in histogram and the inherent features of residue number system validate the security ability of the proposed scheme. Image encryption using the residue number system concept is presented in this paper, the traditional moduli set is employed which required little hardware.

References

[1] Ammar, A., Al Kabbany A., Youssef M. and Emam A. (2001). A Secure image coding scheme using Residue Number System, In: Proceedings of the 18th National Radio science conference, Egypt, pp. 339- 405.

[2] Wei, W., Swamy, M.N.S. and Ahmad, M.O. (2004). RNS Application for Digital Image Processing, In: Proceedings of the 4th IEEE International Workshop on System-on-Chip for Real-time Applications.

[3] Konstantinides, K. and Bhaskaran, V. (1992). Monolithic architectures for image processing and compression. IEEE Computer Graphics and Applications, Vol.12, No.6, pp. 75-86.

[4] Pirsch, P. and Stolberg, H.J. (1998). VLSI implementations of image and video multimedia processing systems. IEEE Transaction on Circuits and Systems for Video Technology, Vol. 8, No. 7, pp. 878-891.

[5] Weyori, B.A. Amponsah P.N. and Yeboah, P.K. (2012). Modeling a Secured Digital Image Encryption Scheme Using a Three Moduli Set. Global Journal of Computer Science and Technology Interdisciplinary, Vol. 2, No. 10, pp. 6-13.

[6] Alhassan, S. and Gbolagade, K.A. (2013). Enhance of the Security of a Digital Image using the Moduli Set $\{2^n-1, 2^n, 2^n+1\}$. International Journal of Advanced Research in Computer Engineering and Technology, Vol. 2, No. 7, pp. 2223-2229.

[7] Linhua, Z., Xiaofeng, L. and Xuebing, W. (2005). An image encryption approach based on chaotic maps. Chaos, Solitons and Fractals, Vol. 24, pp. 759–765.

[8] Mazleena, S., Subariah, I. and Ismail, F.I. (2003). Image Encryption Algorithm Based on Chaotic Mapping. Journal Teknologi, Vol. 39, No.1, pp. 1-12.

[9] Minati, M., Priyadarsini, M., Adhikary, M.C. and Sunit, K. (2012). Image Encryption Using Fibonacci-Lucas Transformation. International Journal on Cryptography and Information Security, Vol. 2, No. 3, pp.131-141.

[10] Soderstrand, M.A., Jenkins, W.K., Jullien, G.A. and Taylor, F.J. (1986). Residue Number System Arithmetic: Modern Applications in Digital Signal Processing. New York: IEEE Press.

[11] Parhami, B. (2000). Computer Arithmetic: Algorithms and Hardware Designs. Oxford: Oxford University Press.

[12] Freking, W.L. and Parhi, K.K. (1998). Low-power FIR digital filters using residue arithmetic, In Proceedings of the IEEE International Symposium on Circuits and Systems, Vol. 1, pp.739-743.

[13] Bhardwaj, M. and Blaram, A. (1998). Low-power signal processing architectures using residue arithmetic, In: Proceedings IEEE International Symposium on Circuits and Systems, pp. 3017-3120.

[14] Jenkins W.K. and Leon, B.J. (1977). The use of residue number systems in the design of finite impulse response digital filters. IEEE Trans. Circuits System, Vol. 24, pp. 191–201.

[15] Guan, B. and Jones, E.V. (1988). Fast conversion between binary and residue numbers. Electronics Letters, Vol. 24, No. 19, pp. 1195–1197.

[16] Molahosseini, A.S. and Navi, K. (2007). New Arithmetic Residue to Binary Converters. International Journal of Computer Sciences and Engineering Systems**,** Vol.1, No.4, pp. 291-295.

[17] Mi, L. (2004). Arithmetic and Logic in Computer Systems. John Wiley & Sons, Inc., Hoboken, New Jersey.

[18] Wang, Y. (1998). New Chinese Remainder Theorem, In: Proceedings of Asilomar Conference, USA.

[19] Wei, W., Swamy, M.N.S., Ahmad, M.O. and Yuke, W. (YEAR). A study of residue-to-binary converters for three-moduli sets. IEEE Trans. On Circuits and Systems I, Vol. 50, No.2, pp. 235-243.

[20] Wei, W., Swamy M.N.S., Ahmad, M.O. and Yuke, W. (2000). A high-speed residue-to-binary converter for three-moduli RNS and a scheme of its VLSI implementation. IEEE Trans. on Circuits and Systems II, Vol. 47, No.12, pp. 1576-1581.