Earthline Journal of Mathematical Sciences
ISSN (Online): 2581-8147
Volume 2, Number 1, 2019, Pages 111-125
https://doi.org/10.34198/ejms.2119.111125

Improved Perceptual Video Encryption Technique using Residue Number System

Salamudeen Alhassan[1], Mohammed Muniru Iddrisu[2] and Mohammed Ibrahim Daabo[3]

[1] Department of Mathematics and ICT, Bagabaga College of Education, Bolgatanga, Ghana; e-mail: salamprog@yahoo.com

[2] Department of Mathematics, University for Development Studies, Navrongo-Campus, Navrongo, Ghana

[3] Department of Computer Science, University for Development Studies, Navrongo-Campus, Navrongo, Ghana

Abstract

In this paper, we propose an enhanced perceptual video encryption technique to speed-up and secure cipher video transmitted across networks using Residue Number System (RNS). The technique proposes a new reverse converter with smaller dynamic range using the moduli set $\{2^n - 1, 2^n, 2^n + 1\}$ that is integrated into our previous work of [2]. After encryption, cipher video is encoded into three residual videos that have smaller pixel values and ideal for transmission across networks. Instead of transmitting the three (3) residual videos, the technique effectively transmits and decodes only two (2) of them back into the original video with same visual quality. Experimental results show that the technique enhances transmission speed and security of cipher video across networks.

1. Introduction

Perceptual video encryption techniques have received overwhelming attention by researchers in recent times leading to the development of varied cryptographic

Received: March 14, 2019; Accepted: April 27, 2019

2010 Mathematics Subject Classification: 68P25, 68U10.

Keywords and phrases: perceptual video encryption, residue number system, cipher video, reverse converter, residual video.

advertisement techniques for video of financial interest [3, 4, 7, 11, 13, 15, 30, 31]. These offer content providers the opportunity to reach more viewers while securing the high quality versions of their videos. Potential consumers can preview the degraded videos before acquiring the high quality ones. However, little has been done by previous techniques to enhance the transmission speed of cipher videos transmitted across networks. Owing to large bit representations, big numbers transmit slower than small ones across network. Small numbers can be achieved with the adoption of RNS where residues of the huge and redundant video data are used. Among many inherent features, RNS offers high computational and transmission speeds. In this proposed technique, RNS is employed to split cipher videos in to three shares (residual videos) that have smaller values. Two of the shares are then transmitted and deciphered at the receiver's end without loss of any information. The shares add extra layer of security and enhance transmission speed to the cipher videos. The rest of the paper is presented as follows; residue number system is presented in Section 2. Section 3 presents detail explanation of the proposed reverse converter while Section 4 presents the proposed integrated crytosystem of the scheme of [2] and RNS. Analysis of results is in Section 5 and finally we conclude in Section 6.

2. Residue Number System

Residue number system is described as a non-weighted number system having numerous benefits in numerical computations. The inherent features in RNS such as the digit-to-digit computations, parallelism, fault tolerance, high computational speed and low power dissipation make it ideal for implementation in fields of communication [9, 10], Digital Signal Processing (DSP) [14, 26, 32], intensive computations such as digital filtering, correlations, convolutions, direct digital frequency synthesis [6], Discrete Fourier Transform (DFT) computations [24], Fast Fourier Transform (FFT) computations, image processing [1, 10, 20, 25, 28] and cryptography [27, 33]. RNS are based on the congruence relation. Two integers x and y are said to be congruent modulo m if m divides exactly the difference of x and y; mathematically [20]

$$x \equiv \mid y \mid_m. \tag{1}$$

If q and r are the quotient and remainder, respectively of the integer division of Y by m that is, $Y = q \cdot m + r$, then, by definition, we have $Y \equiv \mid r \mid_m$. The relationship between r; Y and m is given by [20].

$$r = |Y|_m. \tag{2}$$

RNS is determined by the set $S = m_1, m_2, ..., m_N$ of N positive and pairwise relatively prime moduli where the dynamic range M is the product of the moduli m_i. Thus;

$$M = \prod_{i=1}^{N} m_i. \tag{3}$$

With this, every integer Y in $[0, M-1]$ has a unique representation $(y_1, y_2, ..., y_N)$ in S. The set S and the numbers y_i are respectively called the moduli set and residue of Y modulo m_i [1, 10, 20].

2.1. *RNS to binary conversion*

Two traditional techniques are widely used for RNS to binary reverse conversion; the Chinese Remainder Theorem (CRT) and the Mixed Radix Conversion (MRC).

2.1.1. *Chinese remainder theorem* (*CRT*)

Consider the moduli set $m_1, m_2, m_3, ..., m_N$ with $\gcd(m_i, m_j) = 1$ for $i \neq j$ and dynamic range $M = \prod_{i=1}^{N} m_i$, the CRT for an integer Y having RNS representation $(x_1, x_2, x_3, ..., x_N)$ is reversed converted as follows;

$$Y = \left| \sum_{i=1}^{N} M_i \left| M_i^{-1} x_i \right|_{m_i} \right|_N, \tag{4}$$

where $M_i = \dfrac{M}{m_i}$ and M_i^{-1} is the multiplicative inverse of M_i with respect to m_i [17, 20, 29].

2.1.2. *The mixed radix conversion* (*MRC*)

Suppose the moduli compose of positive pairwise relative prime integers is being ordered as $m_N > m_{(N-1)} > \cdots > m_1$. A non-negative operand Y in the range of $[0, M-1]$ in mixed radix representation is given by;

$$Y \leftrightarrow \langle \hat{y}_N, \hat{y}_{N-1}, ..., \hat{y}_1 \rangle,$$

where;

$$Y = \hat{y}_N \prod_{i=1}^{N-1} m_i + \hat{y}_{N-1} \prod_{i=1}^{N-2} m_i + \cdots + \hat{y}_2 m_1 + \hat{y}_1 \tag{5}$$

and $0 \leq \hat{y}_i < m_i$ for all i [17, 19, 20]. Apart from the traditional techniques, other researchers have proposed much faster and efficient RNS to binary reverse converter for particular moduli sets [5, 8, 12, 16, 18, 34]. However, most of them are simple modification of the CRT or MRC techniques [21-23].

3. Proposed Technique

In this section, a new reverse converter with smaller dynamic range is proposed using the moduli set $\{2^n - 1, 2^n, 2^n + 1\}$ for fast decoding of cipher video. The quotient technique is used to convert numbers in RNS to their equivalent binary (weighted) number system. The dynamic range adopted for this technique is $[0, m_3 m_2 - 1]$. Thus, two moduli in the moduli set are used in the reverse conversion process while one modulus is made redundant.

3.1. *Proposed reverse converter for dynamic range* $[0, \hat{M} = m_3 m_2 - 1]$

Given the pairwise relative prime moduli set $\{m_1, m_2, m_3\} = \{2^n - 1, 2^n, 2^n + 1\}$ and residue (x_1, x_2, x_3), X can be represented as in the following three different ways;

$$X = m_1 q_1 + x_1, \tag{6}$$

$$X = m_2 q_2 + x_2, \tag{7}$$

$$X = m_3 q_3 + x_3, \tag{8}$$

where q_i, $i = 1, 2, 3$ is the quotient when X is divided by the modulus m_i, $i = 1, 2, 3$. Also, q_2 can be represented as;

$$q_2 = q_3 + d, \tag{9}$$

where $d \in Z$ and $d \geq 0$.

Illustration 1.

Consider $n = 3,\ \{m_1, m_2, m_3\} = \{7, 8, 9\},\ \hat{M} = 72$ and using Equations (7) and (8)

For $X = 17$,

$$17 = 8(2) + 1 = 9(1) + 8$$

$$\Rightarrow 2 = 1 + 1, \text{ where } d = 1$$

For $X = 32$,

$$32 = 8(4) + 0 = 9(3) + 5$$

$$\Rightarrow 4 = 3 + 1, \text{ where } d = 1$$

For $X = 63$,

$$63 = 8(7) + 7 = 9(7) + 0$$

$$\Rightarrow 7 = 7 + 0, \text{ where } d = 0.$$

Hence, $q_2 = q_3 + d$.

Thus Equation (8) becomes;

$$X = m_2 q_3 + m_2 d + x_2. \tag{10}$$

From Equation (9);

$$q_3 = \frac{(X - x_3)}{m_3}$$

and substituting gives;

$$X = m_2\left(\frac{(X - x_3)}{m_3}\right) + m_2 d + x_2$$

$$Xm_3 = Xm_2 - m_2 x_3 + m_3 m_2 d + m_3 x_2,$$

$$X = \frac{m_3 m_2 d + m_3 x_2 - m_2 x_3}{m_3 - m_2}$$

but $(m_3 - m_2) = 1$, hence;

$$X = m_3 m_2 d + m_3 x_2 - m_2 x_3.$$

Eliminate the term in d by taking both sides modulo $\hat{M}$

$$| X |_{\hat{M}} = | m_3 m_2 d + m_3 x_2 - m_2 x_3 |_{\hat{M}}$$

$$X = | m_3 x_2 - m_2 x_3 |_{\hat{M}}. \tag{11}$$

3.2. *Hardware implementation*

The binary representations of the respective residues are as follows:

$$x_{1,\,(n-1)}\, x_{1,(n-2)} \cdots x_{1,1} x_{1,0}, \tag{12}$$

$$x_{2,\,(n-1)}\, x_{2,(n-2)} \cdots x_{2,1} x_{2,0}, \tag{13}$$

$$x_{3,\,n}\, x_{3,n-1} \cdots x_{3,1} x_{3,0}. \tag{14}$$

Equation (11) can be simplified as

$$\begin{aligned} X &= | \tau_1 + \tau_2 |_{2^n(2^n+1)} \\ &= | \tau_{1,(2n-1)}\, \tau_{1,(2n-2)} \cdots \tau_{1,1} \tau_{1,0} + \tau_{2,(2n-1)}\, \tau_{2,(2n-2)} \cdots \tau_{2,1} \tau_{2,0} |_{2^n(2^n+1)} \\ &= X_{2n-1} X_{2n-2} \cdots X_1 X_0, \end{aligned} \tag{15}$$

where

$$\begin{aligned} \tau_1 &= 2^n x_2 + x_2 \\ &= x_{2,(n-1)}\, x_{2,(n-2)} \cdots x_{2,1} x_{2,0} \overbrace{00\cdots00}^{(n-bits)} + x_{2,(n-1)}\, x_{2,(n-2)} \cdots x_{2,1} x_{2,0} \\ &= x_{2,(n-1)}\, x_{2,(n-2)} \cdots x_{2,1} x_{2,0} \bowtie x_{2,(n-1)}\, x_{2,(n-2)} \cdots x_{2,1} x_{2,0} \\ &= \tau_{1,(2n-1)}\, \tau_{1,(2n-2)} \cdots \tau_{1,1} \tau_{1,0} \end{aligned} \tag{16}$$

and,

$$\begin{aligned} \tau_2 &= |- 2^n x_3 |_{2^n(2^n+1)} \\ &= | \bar{x}_{3,n}\, \bar{x}_{3,(n-1)} \cdots \bar{x}_{3,1} \bar{x}_{3,0} \overbrace{(11\cdots11)}^{(n-bits)} |_{2^n(2^n+1)} \\ &= \tau_{2,(2n-1)}\, \tau_{2,(2n-2)} \cdots \tau_{2,1} \tau_{2,0} \end{aligned} \tag{17}$$

3.3. *Hardware realization*

The hardware of the proposed scheme applicable to values of $n \leq 4$, can be realized with a simple modulo carry propagate adder (MCPA) and an inverter. Equation (16) is a concatenation of bits, which would not require any hardware resource for that operation. Equation (17) would only require a bit inverter, which is not expensive and at the same time, does not impose undue delay on the scheme. It is only in Equation (15) that an MCPA of length 2*n*-bits would be required to add the results of (16) and (17). Thus, the hardware resources in this regard are 2*n*-bits wide whiles the delay imposed by such an adder is 4*n*-bits. The delay for an inverter is usually unity; therefore, the total delay that would be imposed on the scheme is $(4n+1)$-bits. The block diagram for the reverse conversion is shown in Figure 1.

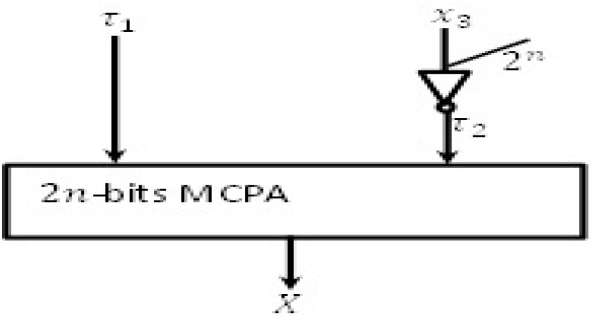

Figure 1. Block diagram for the reverse conversion.

4. RNS Integration with Proposed Video Cryptosystem

4.1. *Enhanced encryption algorithm*

The proposed enhancement to the encryption algorithm of [2] is obtained by modifying the last step to include the RNS encoder. This is presented as;

- Input video file *V*, number of iteration *I*, block size *blkSize*, angle of rotation θ, unit-anti-diagonal matrix *K* and the number of bits *n*.
- Encrypt video frames as follows:
  - Compute point of rotation and extract block of pixels (V_{P_b}) using rotation matrix (*A*).

- Multiply block of pixels (V_b) by unit anti-diagonal matrix (K) to obtain cipher frame $(V_{be} = V_{P_b} \times K)$.
- Add cipher frame to cipher video $(V_E + = V_{be})$.

- Compute the moduli set $\{2^n - 1, 2^n, 2^n + 1\}$ using n.
- Compute the residual videos $x2$ and $x3$ from V_E modulus 2^n and $2^n + 1$, respectively.
- Transmit cipher videos $x2$ and $x3$.

4.2. ***Enhanced decryption algorithm***

The proposed enhancement to the decryption algorithm of [2] is obtained by modifying the initial steps to include the RNS decoder. The proposed enhancement is presented as;

- Input cipher videos $x2$ and $x3$, number of iteration I, block size *blkSize*, angle of rotation θ, anti-diagonal matrix K and the number of bits n.
- Compute the moduli set $\{2^n - 1, 2^n, 2^n + 1\}$ using n.
- Decrypt cipher frames as follows:
  - Decode $x2$ and $x3$ back into cipher frames V_E using equation (11).
  - Compute point of rotation and extract block of pixels V_{E_b} using rotation matrix (A).
  - Multiply block of pixels V_{E_b} by unit anti-diagonal matrix (K) to obtain plain frame $V_{bp} = V_{E_b} \times K$.
  - Add plain frame to plain video $V + = V_{bp}$.
- Transmit cipher video V.

In Figure 2, the forward and proposed reverse converters for the moduli set $\{2^n - 1, 2^n, 2^n + 1\}$ are fitted after the encryption algorithm and before the decryption algorithm respectively. Pixels values of encrypted video are passed through the forward

converter which yields two residues (x_2, x_3) corresponding to the moduli $\{2^n\}$ and $\{2^n + 1\}$. Continuous bitstream of the residues are transmitted through the transmission channel in fixed length code words. At the receivers' end, the fixed length code words are transformed back to continuous form and the proposed reverse converter is applied to recover the cipher video. The original video is then recovered from the cipher video by applying the decryption algorithm sub-block.

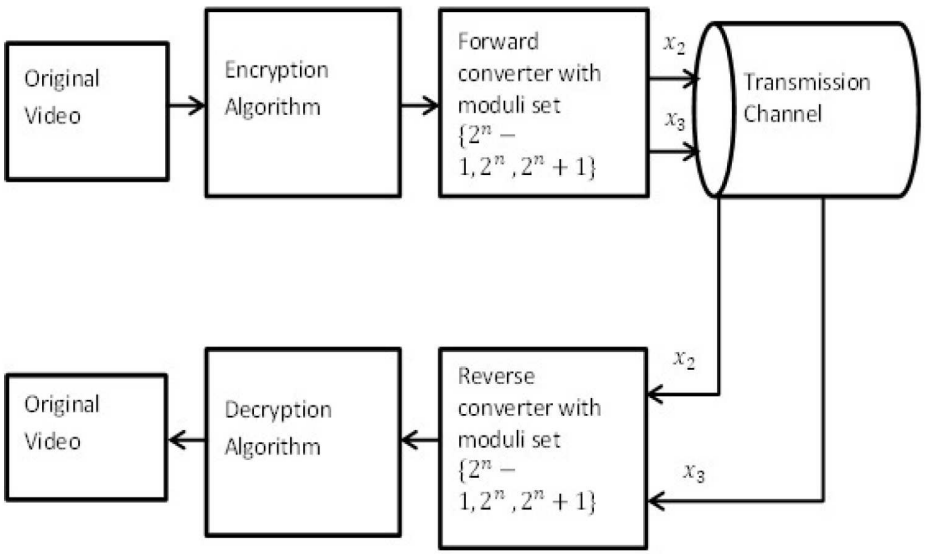

Figure 2. Block diagram of proposed integration of RNS with perceptual video cryptosystems.

The MATLAB Simulink system to test the proposed integrated scheme is shown in Figure 3. RNS is integrated with the work of [2]. After encryption with 'Encryption Algorithm1' sub-block, the cipher video is passed through the sub-block 'RNSEncoder' to be encoded into two residual videos *x*2 and *x*3 for transmission. Since residual values are less than that of the originals, transmission is much easier and faster. At the receiver's end, residual videos are decoded by the 'RNSDecoder' sub-block into the cipher video followed by decryption into the plain video using the 'Decryption Algorithm1' sub-block.

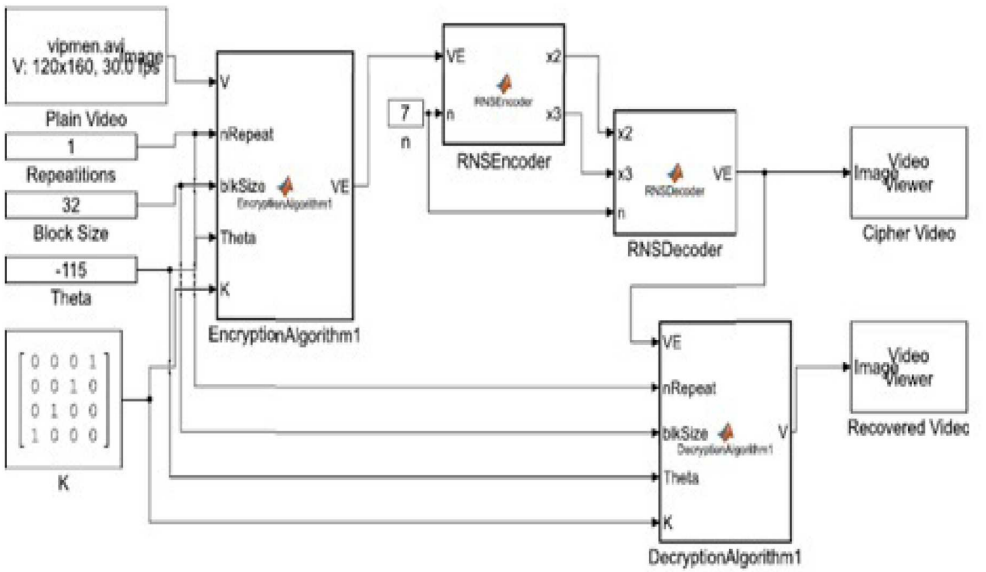

Figure 3. Integration of RNS with proposed perceptual video via unit anti-diagonal matrix.

Table 1. Processing time of encryption/decryption algorithm.

	Processing Time(s)	
Video File(Dimension)	Encryption(RNSEncoder)	Decryption(RNSDecoder)
vipmen.avi (160×120)	0.058(0.008)	0.061(0.026)
carphone.avi (176×144)	0.092(0.014)	0.098(0.035)
xylophone.mpg (320×240)	0.468(0.036)	0.475(0.097)

Figure 4 shows experimental results of the residual videos after encoding a cipher frame using $n = 4$. The dark pictures of parts (b) and (c) confirm the smaller values achieved through the RNS encoder. Any adversary receiving these will need extra efforts to decode them to the cipher state before efficient decryption can occur.

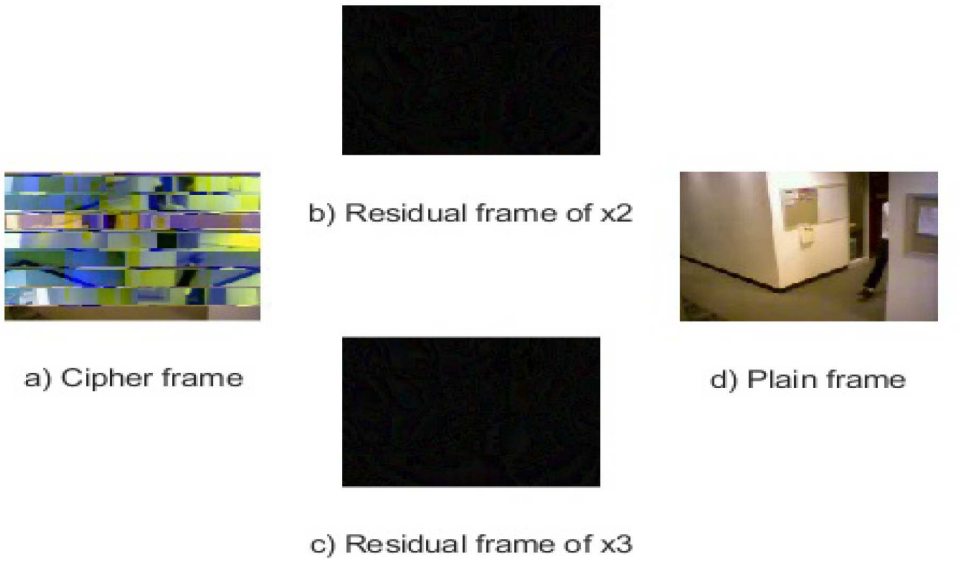

Figure 4. Residual frames of encoded video using RNS. (a) Cipher frame, (b) Residual frame $x2$, (c) Residual frame $x3$ and (d) Recovered frame.

5. Analysis of Results

5.1. *Procession time*

The average processing time (in seconds) for ten (10) simulations of the encryption and decryption processes are summaries in Table 1. The results indicate that the 'RNSEncoder' consumes about 9% of the average encryption time while 25% of the average decryption time is consumed by the 'RNSDecoder'. Thus, RNS constitutes about 34% of the total processing time of any given encryption and decryption operation. Also, the increase in the decryption time enhances security especially against Bruce-force

5.2. *Encoding analysis*

Video data is made up of several frames(images) arranged over time. The elements of these frames are called pixels. The weight of a pixel for the Red-Green-Blue (RGB) format of video span 0 to 2^8. Thus, 8-bits are required to encode and transmit each pixel. However, the introduction of RNS reduces this to 4-bits when $n = 4$ is used for the 'RNSEncoder'. This saves half of the bits required to encode and transmit cipher videos. Consequently, transmission speed is enhanced by the introduction of RNS.

6. Conclusion

This paper proposes an enhancement to the perceptual video encryption and decryption algorithms proposed in [2] using RNS. Analysis of simulated results shows that the enhanced scheme increases transmission speed and adds extra security to cipher video.

References

[1] S. Alhassan and K. Gbolagade, Enhancement 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 & Technology* (*IJARCET*) 2(7) (2013), 2223-2229.

[2] S. Alhassan, M. M. Iddrisu and M. I. Daabo, Perceptual video encryption via unit antidiagonal matrix, *Appl. Math. Inf. Sci.* 12 (2018), 923-929. https://doi.org/10.18576/amis/120504

[3] S.-K. Au Yeung and B. Zeng, Improved perceptual video encryption using multiple 88 transforms in MPEG-4, *7th IEEE International Conference on Communications and Networking in China*, Kun Ming, 2012a, pp. 185-188.

[4] S.-K. Au Yeung and B. Zeng, A new design of multiple transforms for perceptual video encryption, *19th IEEE International Conference on Image Processing*, Orlando, 2012b, pp. 2637-2640. https://doi.org/10.1109/ICIP.2012.6467440

[5] S. Banhanfar and N. Zarei, Reverse converter for the moduli set $\{2^n-1, 2^n, 2^n+1\}$ base on grouping number, *IJCSI International Journal of Computer Science Issues*, 10(6) (2013), 97-102.

[6] A. Baraniecka and G. Jullien, On decoding techniques for residue number system realizations of digital signal processing hardware, *IEEE Transactions on Circuits and Systems* 25(11) (1978), 935-936. https://doi.org/10.1109/TCS.1978.1084399

[7] T. Bernatin, S. Kuzhaloli, M. S. Godwin Premi and L. Brathesia Queen, Perceptual video encryption in multimedia secure communication, *2016 IEEE Online International Conference on Green Engineering and Technologies* (*IC-GET*), Coimbatore, 2016, pp. 1-4. https://doi.org/10.1109/GET.2016.7916722

[8] M. Bhardwaj, A. B. Premkumar and T. Srikanthan, Breaking the 2*n*-bit carry propagation barrier in residue to binary conversion for the $\{2^n-1, 2^n, 2^n+1\}$ module set, *IEEE Transactions on Circuits and Systems I*: *Fundamental Theory and Applications* 45(9) (1998), 998-1002. https://doi.org/10.1109/81.721268

[9] N. I. Chervyakov, P. A. Lyakhov, D. I. Kalita and K. S. Shulzhenko, Effect of RNS moduli set selection on digital filter performance for satellite communications, *2015 IEEE International Siberian Conference on Control and Communications* (*SIBCON*), Omsk, 2015, pp. 1-7. https://doi.org/10.1109/SIBCON.2015.7147268

[10] M. I. Daabo, K. A. Gbolagade and P. A. Agbdemnab, Fast over flow detection scheme by operands examinations method for length three moduli sets, *Computer Engineering and Intelligent Systems* 7(9) (2016), 8-13.

[11] X. Ding, Y. Deng, G. Yang, Y. Song, D. He and X. Sun, Design of new scan orders for perceptual encryption of H.264/AVC videos, *IET Information Security* 11(2) (2017), 55-65. https://doi.org/10.1049/iet-ifs.2015.0492

[12] D. Gallaher, F. E. Petry and P. Srinivasan, The digital parallel method for fast RNS to weighted number system conversion for specific moduli $\{2^k-1,\ 2^k,\ 2^k+1\}$, *IEEE Transactions on Circuits and Systems II*: *Analog and Digital Signal Processing* 44(1) (1997), 53-57. https://doi.org/10.1109/82.559370

[13] A. Kirthanaa, N. Mathan and T. Vino, Improved perceptual video encryption and decryption using S-transform, *2015 IEEE International Conference on Control*, *Instrumentation*, *Communication and Computational Technologies* (*ICCICCT*), Kumaracoil, 2015, pp. 145-148. https://doi.org/10.1109/ICCICCT.2015.7475265

[14] M. R. Kosek, F. J. Taylor, M. Grin and R. R. Hardy, RNS-based GaAs signal processing system, *IEEE Military Communications Conference*, '*Bridging the Gap*. *Interoperability*, *Survivability*, *Security*', Boston 2 (1989), 615-619.

[15] S. Li, G. Chen, A. Cheung, B. Bhargava and K.-T. Lo, On the design of perceptual MPEG-video encryption algorithms, *IEEE Transactions on Circuits and Systems for Video Technology* 17(2) (2007), 214-223. https://doi.org/10.1109/TCSVT.2006.888840

[16] J. Y. Low and C. H. Chang, A new RNS scaler for $\{2^n-1,\ 2^n,\ 2^n+1\}$, *2011 IEEE International Symposium of Circuits and Systems* (*ISCAS*), Rio de Janeiro, 2011, pp. 1431-1434.

[17] M. Lu, *Arithmetic and Logic in Computer Systems*, New Jersey: John Wiley & Sons, Inc., 2004. https://doi.org/10.1002/0471728519

[18] J. Mathew, D. Radhakrishnan and T. Srikanthan, Residue-to-binary arithmetic converter for moduli set $\{2^n-1,\ 2^n,\ 2^n+1\}$, *IEEE-EURASIP Workshop on Nonlinear Signal and Image Processing* (*NSIP'99*), 1999, pp. 20-23.

[19] U. Meyer-Base, J. Mellott and F. Taylor, Design of RNS frequency sampling filter banks,

1997 IEEE International Conference on Acoustics, Speech, and Signal Processing, Munich 3 (1997), 2061-2064.

[20] A. Omondi and B. Premkumar, *Residue Number Systems*: *Theory and Implementation*, London: Imperial College Press, 2007. https://doi.org/10.1142/p523

[21] A. Persson and L. Bengtsson, Forward and reverse converters and moduli set selection in signed-digit residue number systems, *Journal of Signal Processing Systems* 56(1) (2009), 1-15. https://doi.org/10.1007/s11265-008-0249-8

[22] S. J. Piestrak, Design of high-speed residue-to-binary number system converter based on Chinese remainder theorem, *Proceedings 1994 IEEE International Conference on Computer Design*: *VLSI in Computers and Processors*, Cambridge, 1994, pp. 508-511.

[23] S. J. Piestrak, A high-speed realization of a residue to binary number system converter, *IEEE Transactions on Circuits and Systems II*: *Analog and Digital Signal Processing* 42(10) (1995), 661-663. https://doi.org/10.1109/82.471401

[24] J. Ramirez, A. Garcia, U. Meyer Base, F. Taylor, P. G. Fernandez and A. Lloris, Design of RNS-based distributed arithmetic DWT filterbanks, *2001 IEEE International Conference on Acoustics, Speech, and Signal Processing*, Salt Lake City, Proceedings (Cat. No.01CH37221) 2 (2001), 1193-1196. https://doi.org/10.1109/ICASSP.2001.941137

[25] A. Shetty, R. Kiran, S. Shetty, S. Naik, S. Nayak and D. J. D'Souza, Image cryptography using RNS algorithm, *2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering* (*ICPCSI*), Chennai, 2017, pp. 1936-1939. https://doi.org/10.1109/ICPCSI.2017.8392052

[26] T. Singh, Residue number system for fault detection in communication networks, *2014 IEEE International Conference on Medical Imaging*, *m-Health and Emerging Communication Systems* (*MedCom*), Greater Noida, 2014, pp. 157-161. https://doi.org/10.1109/MedCom.2014.7005995

[27] F. J. Taylor, An RNS discrete Fourier transform implementation, *IEEE Transactions on Acoustics*, *Speech*, *and Signal Processing* 38(8) (1990), 1386-1394. https://doi.org/10.1109/29.57573

[28] W. Wang, M. N. Swamy and M. O. Ahmad, RNS application for digital image processing, *4th IEEE International Workshop on System-on-Chip for Real-Time Applications*, Ban, 2014, pp. 77-80.

[29] Y. Wang, Residue-to-binary converters based on new Chinese Remainder Theorems, *IEEE Transactions on Circuits and Systems II*: *Analog and Digital Signal Processing* 47(3) (2000), 197-205. https://doi.org/10.1109/82.826745

[30] Y. Wang, M. O'Neill and F. Kurugollu, Partial encryption by randomized zig-zag scanning for video encoding, *2013 IEEE International Symposium on Circuits and Systems* (*ISCAS2013*), Beijing, 2013, pp. 229-232.

[31] O. Watanabe, T. Fukuhara and H. Kiya, A perceptual encryption scheme for motion JPEG 2000 standard, *15th IEEE International Symposium on Communications and Information Technologies* (*ISCIT*), Nara, 2015, pp. 125-128. https://doi.org/10.1109/ISCIT.2015.7458323

[32] W. Yang, M. Zhao, X. Chen, L. Huang and J. Wang, Application of residue number systems to Bent-pipe satellite communication systems, *6th IEEE International ICST Conference on Communications and Networking in China* (*CHINACOM*), Harbin, 2011 pp. 1083-1087.

[33] Y. Yao, J. Zhou, B. Yan and Y. Li, RNS-based embedding scheme for data hiding in digital images, *17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/ 12th IEEE International Conference on Big Data Science and Engineering* (*TrustCom/BigDataSE*), New York, 2018, pp. 1480-1483. https://doi.org/10.1109/TrustCom/BigDataSE.2018.00207

[34] B. Zarei and M. Askarzadeh, A high-speed residue number comparator for the 3-moduli set $\{2^n-1, 2^n, 2^n+1\}$, *International Journal of Advanced Research in Computer Science* 3(1) (2010), 270-272.