AN ALGORITHM FOR A RESIDUE NUMBER SYSTEM BASED VIDEO ENCRYPTION SYSTEM

Akinbowale N. Babatunde [1,2], Rasheed G. Jimoh [2], Kazeem A. Gbolagade [1]

[1] **Department of Computer Science, Kwara State University, Malete, Nigeria**
[2] **Computer Science Department, University of Ilorin, Ilorin, Nigeria**

Corresponding Author: Akinbowale N. Babatunde, akinbowale.babatunde@kwasu.edu.ng

ABSTRACT: In recent times, the security of digital video storage and transmission has been gaining serious attention due to the advancement in internet technologies and development of efficient compression techniques. The advancement has enabled the widespread usage of video in various devices and the transmission of sensitive information such as medical, military, governmental confidential information etc. This multimedia data over open network (internet) is always vulnerable to interception by malicious and unauthorized users all over the world. Encryption is the widely established and suitable technique for addressing these security issues based on total encryption or selective encryption. It has been proved and shown that the total video encryption approach(also called Naïve Approach) produces higher level of video security. However, it is computationally expensive because of its slow nature in processing the very large volume of video data and consequently has limited usage in video encryption. The paper presents a scheme that reduces the computational complexity in the total video encryption. The proposed scheme utilizes residue number system. The proposed scheme which will be implemented using Java programming language is envisaged to efficiently secure video data from unauthorized access during transmission and storage.
KEYWORDS: Residue Number System (RNS), Moduli set, Video Encryption, Java Programming Language, Moving Pictures Experts Group IV (MPEG IV).

1. BACKGROUND OF THE STUDY

In the recent years, research on the security of digital video storage and transmission has been gaining serious attention by researchers because of it's wide usage in various devices and the transmission of sensitive information such as medical, military, governmental confidential information etc via these multimedia data through open network (internet) which is always vulnerable to interception by malicious and unauthorized users all over the world. Hence, the security of these multimedia data is at stake.

Encryption is any method or process used in transforming the content of a plaintext into a form unreadable, invisible or unintelligible during transmission or storage. [AZK10] Ciphertext is the product of encryption. Encryption is the widely established and suitable technique to address these security issues [DP12, JM12, MRN12, Yog13, A+13, JS11]. Researchers over the years have proposed various security measures such ascryptography, digital watermarking, scrambling, compression, steganography etc for protecting these videos from unauthorized access [DP12, MP11, MRN12, JS11, Yog13. The security of any encrypted data is entirely dependent on two (2) things; the secrecy of the key and the strength of the cryptographic algorithm. Cryptographic strength is measured in the time and resources it would require to unauthorizely recover the plaintext.

A digital video is comprised of a series of orthogonal bitmap or discrete digital images displayed in rapid succession at a constant rate. In videos, these images are called frames with each given video frame likely to bear a close resemblance to neighboring frames. The rate at which frames are displayed is measured in frames per second (fps). A frame is an orthogonal bitmap/ digital image, it comprises of a raster of pixel. A pixel is a small square with two properties; pixel location and color. Hence, we say a frame with a width of W pixels and a height of H pixels has a frame size of W*H pixels. The color of a pixel is represented by a fixed number of bits, the more the bits the more subtle variations of color can be reproduced. This is called the color depth (CD) of a video.

The origin of residue number system (RNS) can be linked to a verse from a third century book written by a Chinese scholar who posed a mathematical riddle with the following statements:

"We have things we do not know the number;
If we count them by 3's, we have two left over
If we count then by 5's, we have three left over
If we count them by 7's, we have two left over
How many things are there? "

This riddle means which number yields remainder 2, 3, 2 when divided by 3, 5, 7 respectively.

Sun Tzu gave the solution to this puzzle called the Taiyen (Great Generalization) which gave the answer as 23. The Taiyen was later in 1247 generalized to what we now call the Chinese Remainder Theorem (CRT) by a Chinese mathematician (Qin Jiushao), [BBG11, Gbo10, OP07].

RNS is an integer system which speeds up arithmetic operations by splitting numbers into smaller parts in such a way that each unit is independent of the other [GC09, Roo08. It is based on the congruence relation which explains that two (2) integers a and b are said to be in congruent modulo m if m divides exactly the difference of a and b; mathematically represented as $a \equiv b(mod\ m)$. E.g. $10 \equiv 4(mod\ 3)$ [OP07]. RNS is defined in terms of a relatively prime moduli set $\{m_1, m_2, m_3, \dots, m_n\}$ such that $\gcd(m_i, m_j) = 1$ for $i \neq j$, where gcd means the greatest common divisor f m_i and m_j

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

while is the dynamic range. RNS is capable of uniquely representing all integer X that lie in its dynamic range, that is, $(0 \leq X < M)$ where the dynamic range (M) is determined by the multiplication of the moduli sets. If the result of a calculation however exceeds M (Dynamic Range), we say that an overflow has occurred.

RNS architectures are typically composed of three (3) main parts; a binary –to – residue converter, residue arithmetic units and a residue – to – binary converter. This residue – to –binary converter is the most challenging part of any RNS architecture. However, for any successful application of RNS, data transformation from binary to residue and vice versa must be very fast so that conversion overhead does not nullify the advantage provided by the RNS [GC09]; Data conversion and moduli selection are the two (2) most important issues for a successful RNS realization [BBG11].

The residues of a conventional number X can be obtained as $x_i = |X|_{m_i}$. This is referred to as the forward conversion. The conversion from residue notation to a conventional one (binary or decimal representation) is known as reverse conversion. Two (2) most widely used techniques of reverse conversion are the Chinese Remainder Theorem (CRT) and Mixed Radix Conversion (MRC). Although, many other methods have been devised but are still based on the CRT and MRC.

2. RELATED WORK

2.1 RNS and Its areas of Application

Residue Number System is an unweighted Integer number system which speeds up arithmetic computations by splitting numbers into smaller parts independent of each other with arithmetic operations being performed on these smaller parts independently rather than on the original number. The inherent and advantageous properties of this number system such as very fast arithmetic computations, parallel arithmetic operations, error detection and correction abilities etc has made scientists since in the 1950's put them to use in the implementation of fast arithmetic and fault tolerant computing [Baa11, Gbo10, OP07]. In RNS, arithmetic operations on residue numbers are executed at the same time on each residue.

Since the rediscovery of RNS, it has been well applied to areas in which critical arithmetic operations are additions and multiplications e.g Digital Signal Processing such as digital filtering, convolution, fast fourier transform, digital image processing, Low power design, cryptography, bioinformatics etc. [SVP14, DP13, SA13, BBG11, Baa11, Gbo10, GC09, OP07, ZB06, CNR07, Mi04, WSA04].

The two cryptosystems were designed to enhance the security of non-square digital images. He proposed two algorithms using RNS. The first with coprime moduli sets {2^n-1, 2^n, 2^n +1} and a modified Arnold's transform and another scheme based on the moduli sets {2n+2, 2n+1, 2n} and a Bitwise-XOR operation. Both schemes were divided into encryption and decryption processes and they both guarantee the recovery of the plaintext after decryption with no loss of any inherent information. After implementation, both schemes were tested on both gray-scale and true-color images and results showed that the systems achieved excellent results in terms of security, high speed during transmission because of smaller pixel values and sizes, disk space and memory management but the second cryptosystem out performs the first in terms of security.

[WAY12] proposed a digital image coding scheme using RNS with a three length moduli set with common factor {2n+2, 2n+1, 2n}. The scheme offered a very high speed when compared with even other RNS architectures whose reverse converters (RNS to binary converter) are based on CRT because the computation of the multiplicative inverse is eliminated. It also achieved in terms of area, critical path delay and low power VLSI implementation for image processing. After all possible evaluations, it was shown that the scheme out performed most available encryption schemes in terms of area and delay due to the fact that the scheme operated on smaller magnitude operands as it requires less complex adders and multipliers which potentially offers high processing speed.

[Baa11, BBG11] applied RNS into bioinformatics by using the inherent properties of the number system in solving the problems of sequence alignment. In his work, he enhanced the smith-waterman algorithm (SWA) using the residue number system. SWA is very sensitive in performing sequence alignment but has not been adopted because it is computationally expensive. After using the properties exhibited by RNS in the SWA, a hardware implementation of SWA was performed in VHDL (VHSIC Hardware Descriptive Language). The result of the implementation was compared with state of art as at then and the outcome of the comparison showed that the implementation is efficient in both area and speed. Hence, it can be concluded that RNS is a good platform for the implementation of SWA since it has a potential for improving the overall computational cost of SWA.

[WSA04] designed an image encoding system that offers a very high speed and low power implementation which does not require any other additional component other than a RNS system. As against the use of Look up tables in the decryption process of [A+01], Wang used the modified Chinese remainder theorem (CRT) for its decryption process which is more efficient in terms of VLSI than the scheme by [A+01]. The designed algorithms were simulated using matlab tools and tested. Result shows that the cryptosystem encrypts the entire image with a very high security level.

[A+01] used RNS in the coding of digital images. He read digital signal as either a binary or decimal, quantized the image pixels into eight (8) bits and encoded the image using RNS. Look up tables were used for the reverse conversion (decryption) as it was found to be faster and suitable for decryption purposes. The proposed algorithms were implemented using C programming language and tested successfully. The technique provided a totally unreadable image and cannot be decrypted by anyone except with users that has the key.

Residue number system can be applied to multicarrier-code division multiple access (CDMA) systems to enhance its bandwidth efficiency. The work proposed a new method of bandwidth efficiency enhancement of a MC-CMDA system by increasing the number of bits per symbol which in normal cases lead to parallel transmission of data bit with orthogonal spread codes. The maximum possible number of orthogonal sequences causes a limit in the achievable bandwidth efficiency of the system and degradation in system performance with an increment in bits per symbol which is not so using an RNS based representation. In RNS representation, one can increase the number of bits per symbol without increasing the number of parallel channels. The performance of the proposed system was analyzed in a slow fading Rayleigh channel, it was found to have a high bandwidth efficiency and robustness against channel impairments. Hence, the proposed system can be considered as an alternative to high speed data transmission.

3. VIDEO CRYPTOSYSTEMS

The security of video data is becoming more important nowadays because of the rapid development in multimedia video compression and the latest development in internet technologies. These breakthroughs have enabled video data to be used as a medium through which sensitive information can be easily stored and transmitted. Hence, video data needs to be protected from unauthorized access during the cause of transmission and storage. Video encryption is the widely established and secured means of video content protection [A+13, Yog13, DP12, JM12, MRN12, JS11].

Video encryption algorithms generally work with videos in a compressed format because of its large volume nature to enable its storage and transmission over bandwidth-limited networks [RS13, Yog13, MP11]. No single technology can provide a complete solution for securing video transmission [E+01, JS11]. Video compression is a technology for transforming video signals that aims to retain original quality under a number of constraints taking the advantage of data redundancy between successive video frames [SM14]. Encryption of a video data can take place before compression, during compression (Joint) compression or after compression. Irrespective of when the encryption of the video data occurs, an ideal video encryption algorithm for real- time video applications in any consumer device must be able to provide an acceptable level of security, minimize the computational storage and overhead and comply with standard codec formats [WB05].

Typically, video encryption algorithms can be classified into four basic categories; completely layered encryption, permutation based encryption, selective encryption and perceptual encryption [A+13, Yog13, ZGJ12, JS11].

1. Completely Layered Encryption: In a completely layered encryption, a cryptosystem is used in the encryption process to encrypt the whole the whole video data after being compressed without considering any region of interest. Encryption is done on the video data frame by frame without considering the video objects or any other semantic information. They produce the highest security and they have higher computational complexity than the other groups and thus more

suitable for secure video storage [ZGJ12, WB05]. They are however not suitable for real time video applications due to their high computational complexity [JS11]. Examples of this group can be found in the works proposed by [L+02, GSN08] etc.

2. Selectively Encryption: In order to reduce the computational complexity inherited as a result of encrypting the whole video data, algorithms that selectively encrypt a particular video bytes within the video frames are designed in this category. These algorithms selectively encrypt only sensitive or important bytes within the video frames. Although this algorithms reduces computational complexity by selecting only a minimal set of data to encrypt but their security and speed level is dependent on how many parameters they encrypt [JS11]. The works proposed by [SM95, MG95, SB98, WK05] etc. are examples of algorithms in this group.
3. Perceptual Encryption: The perceptual encryption requires that the audio/ video quality of the data be partially degraded by encryption such that the encrypted data are still partially perceptible after encryption and the audio/ video quality of the data is continuously controlled. Perceptual encryption algorithms are not suitable for applications which demand high security, they are suitable for entertainment applications e.g. pay per view etc [JS11].
4. Permutation Encryption: The permutation based encryption uses different permutation algorithms to scramble or encrypt video contents. The entire video does not necessarily need to be scrambled as a particular set of bytes might be scrambled and a permutation list used as a secret key. Permutation based algorithms are generally fast but provides an insufficient level of security [JS11]. Pure permutation, Zig-zag permutation, Huffman codeword (1998), correlation preserving (2006) etc are examples of algorithms in this category.

It has however important to note that the completely layered video encryption scheme provides the highest level of video security but has a very low level of acceptance because it is computationally expensive [DP12, JS11, AZK10, P+12]. Many video encryption techniques have been proposed and designed in literature. Irrespective of the encryption classification used in the design of these techniques, the rate of security, transmission error tolerance, encryption ratio, compression efficiency, computational efficiency, lossless visual quality and format compliance are the metrics used to evaluate and compare their performance [A+13, DP12, ZGJ12, JS11].

4. THE PROPOSED ALGORITHM

The RNS procedure for the proposed video encryption system is presented in figure 1.

5. PROCESS FLOW OF THE ALGORITHM

The process flow of the proposed residue number system based encryption algorithm for the video encryption system is shown in figure 2. Details of the encryption stage are shown in figure 3.

6. DISCUSSION

The algorithm in Figure 1 depicts the complete process from the point of video acquisition to end of the encryption system where we will have our encrypted video data. Our proposed residue number system based encryption algorithm for encrypting video data begins by applying MPEG IV compression algorithm on any video data format to compress the video data such that the size of the video file can be reduced and the compression ratio computed. The compressed video file is then being separated into frames after which the pixel value of each frame is computed. The traditional residue number system moduli set $\{2^n - 1, 2^n, 2^n + 1\}$ is then applied on the pixel values to obtain the residue of each frame which is then saved on a lookup table. This forms the first encryption stage of the system.
To further increase the security and reduce the size of the video file, we will subject the output of the first encryption stage to RNS column addition followed by a RNS row addition. The Result of this is followed by performing scaling on the output file to further reduce the video size. The encrypted video file and lookup table is however stored or transmitted over the internet.

```
Begin
        Input the video file
        Determine the size of the video_file (vf1)
        Compress the video file using MPEG IV_Algorithm
        Determine the size of the compressed_video_file (vf2)
        {
        Compute the compression ratio = (vf1/vf2)
        }
        Extract frames from the compressed_video_file ()
        {
                For (i=0; i<n; i++)
                Extract (from compressed_video_file) = frame [i]
                Frame [i] = frame [i+1]
        }
        Convert_each_frame_to_pixel_value ()
        {
                For (i=0; i<n; i++)
                Convert (frame [i] )
        }
        Compute the residue of each frame which is already in pixel values using the moduli set
        {2^n − 1, 2^n, 2^n + 1}where n=2
        {
                For (l=0; l<m; l++)
                For (j=0; j<n; j++)
                {
                        Split_frame ()
                        {
                                For (k=0; k<n; k++)
                Number_of_sub_pixel_value_of_frame [i] = pixel_value_of_frame% m[l]
                Save the residues into lookup tables (a lookup table for each modulus)
                        }
                }
        }

        Merge the frames for each residue position using RNS addition operation
        {
                Number_sub_frame2[i] = 0
                For (i=0; i<n; i++)
                Number_sub_frame2[i] =
number_of_sub_pixel_value_of_frame[i][l]+number_sub_pixel_value_of_frame[i][l+1]+
number_sub_pixel_value_of_frame[i][l+2]+…..+ number_sub_pixel_value_of_frame[i][l+m]
        }
        Merge the output of the above addition and take the modulus of the result using scaling
        {
                For (i=0; i<n; i++)
                Merge_number_sub_pixel_value_of_frame [i]
                Take modulus of merged_number_sub_pixel_value_of_frame[i] by scaling.
        }
        Save the new residue values
        Store or send as the encrypted video attaching the lookup tables and the key
End
```

Figure 1: Proposed Encryption Procedure

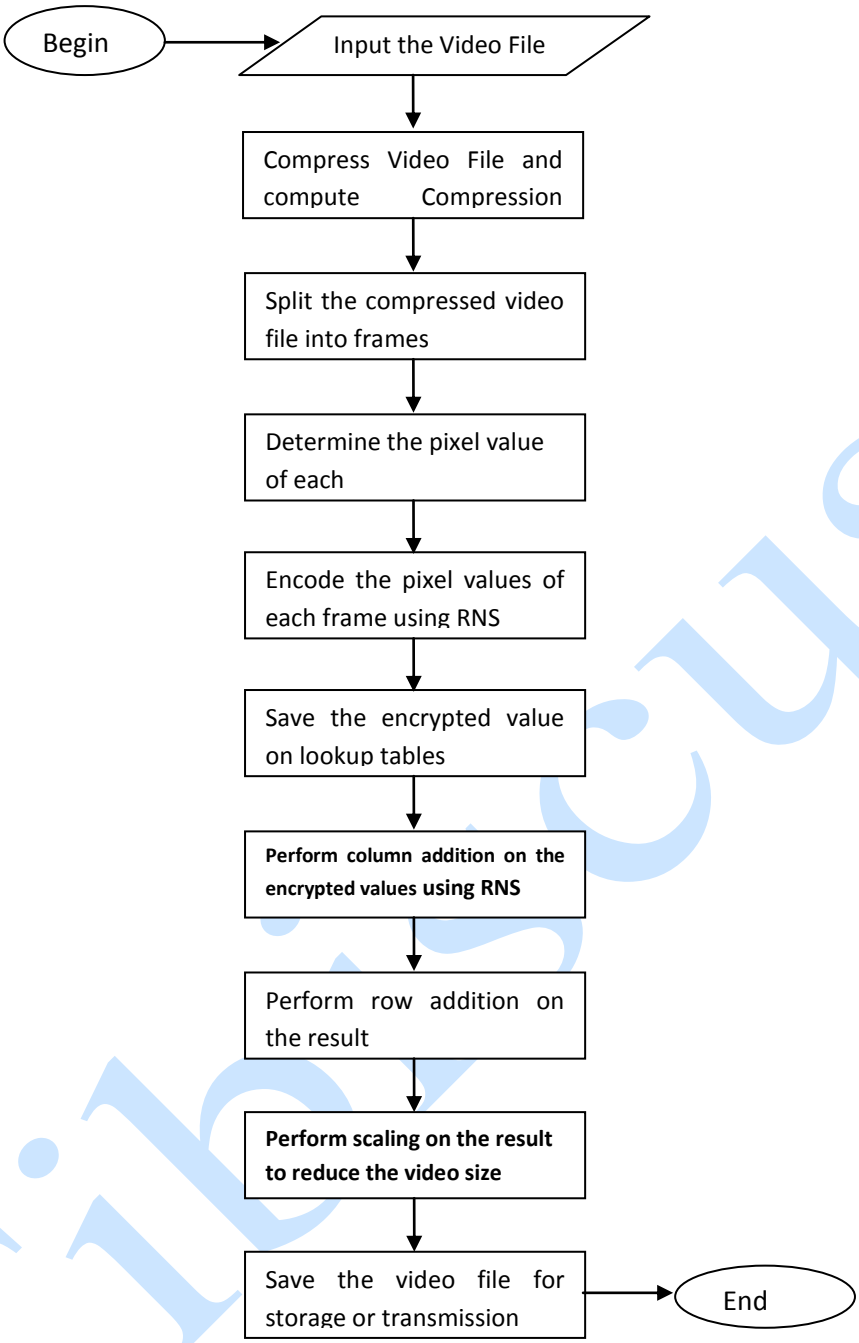

Figure 2: Process flow for the RNS based Video Encryption System

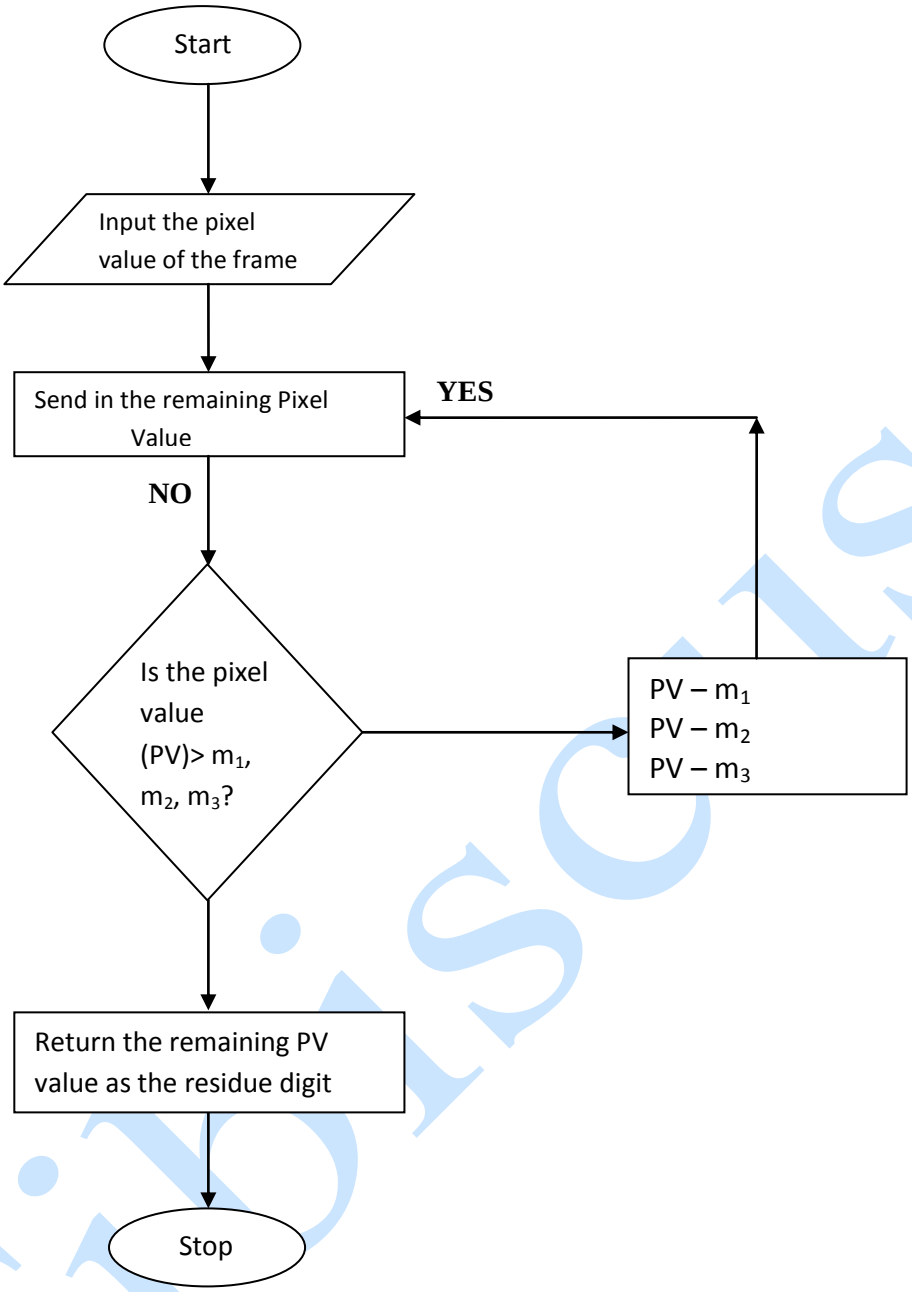

Figure 3: Flowchart for the Encryption System

7. CONCLUSION AND FURTHER WORK

This research develops residue number system based encryption algorithm for encrypting all formats of video data. The algorithm was developed to look into the possibility of ameliorating the computational complexity problems in total video encryption. The next intent is to implement this algorithm on JAVA programming language, test and evaluate the implemented system using the security, encryption ratio, degradation, compression efficiency and transmission error tolerance metrics. The expectation here is that the proposed approach will successfully and efficiently encrypt any video file format during transmission and storage and reduce the computational complexity of total video encryption algorithms.

REFERENCES

[AZK10] **M. Abombara, O. Zakaria., O. Khalifa** - *An overview of video encryption techniques*. *International* Journal of computer theory and engineering. 2 (1). 2010

[A+01] **A. Ammar, A. Alkabbany, M. Youssef, A. Emam** - *A secure image coding scheme using RNS.* Eighteenth National Radio Science Conference, Mansoura University, Eygpt. 2001.

[A+13] **K. Ajay, K. Sourabh, H. Ketki, M. Aniket** - *Proposed video encryption algorithm vs other existing algorithms:*

A comparative study. International Journal of Computer Applications. 65 (1). 2013.

[Baa11] **Y. E. Baagyere** - *Application of residue number system to smith-waterman algorithm.* A Thesis Submitted to Kwame Nkrumah University of Science and Technology. 2011.

[BBG11] **E. Y. Baagyere, K.O. Boateng, K. A. Gbolagade** - *Bioinformatics: An important application area of RNS:* Journal of Engineering and Applied Sciences 6 (2): (174 -179). 2011.

[CNR07] **G. C. Cardarilli, A. Nannarelli, M. Re** - *RNS for low-power DSP Applications*. Institute of Electrical and Electronics Engineer, 2007. (1412-1416). 2007.

[DP12] **H. Darshana, S. Parinder** - *A comprehensive survey of video encryption algorithms.* International Journal of Computer Applications. 59 (1). 2012.

[DP13] **Y. Dina, S. Pavel** - *A comparative study on different moduli sets in residue number system.* Institute of Electrical and Electronics Engineer. 2013.

[E+01] **T. Eugene, W. C. Gregory, S. Paul, J. D. Edward** - *An overview of security issues in streaming video*. Retrieved via www.google.com. 2001.

[GSN08] **K. Ganesan, I. Singh, M. Narian** - *Public key cryptography of images and videos in real time using chebyshev maps*. Proceedings of the 2008 Fifth International Conference on Computer Graphics, Imaging and Visualization, Institute of Electrical and Electronics Engineer Computer Society, Washington DC, USA. (211-216). 2008.

[GC09] **K. A. Gbolagade, D. Cotofana** - *Residue-to-Decimal converters for moduli sets with common factors*. Institute of Electrical and Electronics Engineers. 624-627. 2009.

[GS09] **K. A. Gbolagade, D. C. Sorin** - *A reverse converter for the new 4-moduli set* $(2n+3, 2n+2, 2n+1, 2n)$. Institute of Electrical and Electronics Engineers. 2009.

[Gbo10] **K. A. Gbolagade** - *Effective reverse conversion in RNS processors*. A Thesis Submitted to Delft University, Netherlands. 2010.

[JM12] **J. John, S. Mamimurugan** - *A survey on various encryption techniques*. International Journal of Soft Computing and Engineering (IJSCE). 2 (1). 2012.

[JS11] **S. Jolly, V. Saxena** - *Video encryption: A Survey*. International Journal of Computer Science Issues.8 (2). 2011.

[L+02] **S. Li, X. Zheng, X. Mou, Y. Cai** - *A chaotic encryption scheme for real time digital video*. Proceedings of SPIE, SPIE press, San Jose, CA. 149-160. 2002.

[Mi04] **L. Mi** - *Arithmetic and logic in computer systems*. John Wiley and Sons, Inc. Hoboken, New Jersey. 2004.

[MG95] **J. Meyer, F. Gadegast** - *Security mechanism for multimedia data with the example MPEG-1 video*, project description of SECMPEG. 1995.

[MP11] **R. Mukut, C. Pradhan** - *Secured selective encryption algorithm for MPEG-2 video*. Journal of Institute of Electrical and Electronics Engineers. 2011.

[MFP00] **A. S. Madhukumar, C. Francois, A. B. Premkumar** - *Proceedings of the 43rd Institute of Electrical and Electronics Engineers Mid-West Symposium on Circuits and Systems*, Lansing, 2000.

[MRN12] **A. C. Mayank, P. Ravindra, R. Navin** - *A novel approach of digital video encryption*. International Journal of Computer Applications. 49 (4). 2012.

[OP07] **A. Omondi, B. Premkumar** - *Residue Number Systems: Theory and Implementation*. Imperial College Press. 2007.

[P+12] **W. Puech, Z. Erkin, M. Barni, S. Rane, R. L. Lagendijk** - *Emerging cryptographic challenges in image and video processing*. Journal of Institute of Electrical and Electronics Engineers. 2012.

[Roo08] **G. C. Rooju** - *RNS enhancement for programmable processors.* A Thesis Submitted to Arizona State University. 2008.

[RS13] **S. Rajagopal, A. Shenbagavalli** - *A survey of video encryption algorithm implemented in various stages of compression*. International Journal of Engineering Research and Technology (IJERT). 2 (2). 2013.

[SA13] **J. J. Somayyeh, S. M. Amir** - *Hybrid RNS-to-binary converter for moduli set* $\{2^{2n}, 2^n - 1, 2^n + 1, \quad 2^{n+1} - 1\}$ Research Journal of Applied Sciences, Engineering & Technology. 6 (11). (2027 - 2031). 2013.

[SB98] **C. Shi, B. Bhargava** - *A fast MPEG video encryption*. Proceedings of the 6th ACM International Conference on Multimedia, New York, USA. (81-88). 1998.

[SM14] **G. Suganya, K. Mahesh** - *A survey of various techniques of video compression.* International Journal of Engineering Trends and Technology (IJERT). 7(1). 2014.

[SM95] **G. A. Spanos, T. B. Maples** - *Performance study of a selective encryption scheme for the security of networked, real-time video*. In the Proceedings of the 4th International Conference on Computer and Networks (ICCCN '95). (2-10). 1995.

[SVP14] **K S. Suraj, P. G. Varun, P. Palamisamy** - *Image Security using DES & RNS with reversible watermarking.* 2014 International Conference on Electronics and Communications System. 2014.

[WB05] **A. Wong, W. Bishop** - *An efficient parallel multi-key encryption of compressed video streams*. Department of Electrical and Computer Engineering, University of Waterloo. 2005.

[WK05] **C. P. Wu, C. C. Kuo** - *Design of integrated multimedia compression and encryption systems*. Institute of Electrical and Electronics Engineer. Transaction of Multimedia. 7(5). (828-839). 2005.

[WAY12] **B. A. Weyori, P. N. Amponsah, P. K. Yeboah** - *Modeling a secured digital image encryption using 3 moduli sets.* Global Journal of Computer Science and Technology Interdisciplinary. 12. (10). 2012.

[WSA04] **W. Wang, M. N. S. Swamy, M. O. Ahmad** - *RNS application for digital image processing.* Proceedings of the 4th Institute of Electrical and Electronics Engineers International Workshop on System on Chip for Real – Time Applications. 2004.

[Yog13] **N. Yogita** - *A survey of video encryption techniques*. International Journal of Emerging Technology and Advanced Engineering. 3 (4). 2013.

[ZB06] **L. Zhining, J. P. Bradon** - *An RNS – Enhanced Microprocessor Implementation of Public Key cryptography*. Institute of Electrical and Electronics Engineer 2006. (1430–1433). 2006.

[ZGJ12] **S. Zhaopin, Z. Guofu, J. Jianguo** - *Multimedia security, a survey of chaos based encryption technology multimedia.* School of Computer and Information, Hefei University of Technology, China. 2012.