Earthline Journal of Mathematical Sciences
ISSN (Online): 2581-8147
Volume 4, Number 2, 2020, Pages 399-424
https://doi.org/10.34198/ejms.4220.399424

Enhancing Image Security during Transmission using Residue Number System and k-shuffle

Issah Zabsonre Alhassan, Edward Danso Ansong, Gaddafi Abdul-Salaam and Salamudeen Alhassan

Abstract

This paper proposes an algorithm that enhances the speed of transmission and secure images that are transmitted over internet or a network. The proposed cryptosystem uses a modified k-shuffling technique to scramble pixels of images and further decomposes them using Residue Number System. Simulations are done using two moduli sets with the modified k-shuffle technique. Analyses of results showed that both simulations could secure images without any loss of information and also the time taken for a complete encryption/decryption process is dependent on the moduli set. Among the chosen moduli sets, the even moduli set optimizes and completes execution using less time as compared to the traditional moduli set. The proposed scheme also showed resistance to statistical attacks (histogram, ciphertext, correlation attacks) and a significant reduction in the size of cipher images which enhances the speed of transmission over network.

I. Introduction

In the field of data communication, security and privacy remains the utmost concern over the years. The significant progress in computer and internet technologies have contributed to the survival of data communication but the internet has also made it possible to corrupt data easily during transmission since its possible for an adversary to manipulate his/her way to unauthorized information [1]. Digital images are widely used to communicate in different areas such as health, law enforcement, education, advertisement, entertainment and art [2]. They are used to carry several confidential information contents over public network which is not secure and hence the need to be

Received: May 7, 2020; Accepted: June 12, 2020

2010 Mathematics Subject Classification: 94A60.

Keywords and phrases: encryption, decryption, moduli set, k-shuffle, cryptography.

able to send them incognito. Steganography, cryptography and watermarking are options for securing images sent over computer networks. Several encryption algorithms have been proposed by researchers to help secure images during transmission but according to Kumari et al. [3], chaotic encryption algorithms are more secured than other schemes and are resistant to various statistical attacks; this means they are able to provide the security and privacy required during communication. Others such as Advanced Encryption Standard (AES) and Data Encryption Standard (DES) are not suitable for image encryption because of their file size, spatial redundancy etc. [4]. A good chaotic encryption algorithm should have a high-level confusion and diffusion; diffusion to reduce the correlation between pixel values and confusion to further change the pixel values [5]. Most of these algorithms are based on chaotic maps such as Arnold's transform, logistic maps, 2D cat map, tent map, baker map, standard map etc. However, these transforms have their own weaknesses ranging from inability to process rectangular images to small key space. Alhassan and Gbolagade [6] modified Arnold's transform to process images of all dimensions but increased the time taken to process rectangular images because the algorithm was modified to resize images. Noura et al. [7] stated clearly that 2D cat map only iterates once and has a small key space which cannot withstand a brute-force attack. Irrespective of weaknesses in some chaos algorithms, extensive research is still ongoing in this area of cryptography. Clearly, chaos encryption algorithms are better suited for the security and privacy of images.

Against these backdrops, the need to design an algorithm that can ensure the security and privacy of digital images cannot be overemphasized. Although there have been several researches on chaos image encryption algorithms, many are based on the traditional transforms mentioned earlier. This study is designed to use Residue Number System (RNS) and k-shuffle which is a card shuffling technique to formulate a new chaos image encryption algorithm.

II. Related Work

A. *Digital Images*

Picture elements also known as pixels are the building blocks of digital images; they are the smallest basic unit of images. Each colour (or gray level for black and white images) is represented by a pixel at every single point in the image; this means that a pixel is a small dot of a colour [8] which can be thought of as a discrete sample value of continuous real image.

Consider a 512 × 512 image as shown in Figure 1. Let the image be the matrix X. Thus X consists of 512 rows of pixels and 512 columns of pixels, with a total of 262144 pixels.

Figure 1. A 512 × 512 'lena' image.

There are three main types of images, namely, binary images, black and white images and colour images. Binary images are made up two distinct colours; black and white. With this kind of image, a pixel is either white or black and no midway shades of gray. A single bit can be used to represent a pixel in binary images, either 1 or 0. Black and white image consists of pixels that range from black to white. These kinds of images display different shades of gray. A 256 gray level can have each pixel stored in a single byte (8 bits) memory. A colour image consists of pixels that hold three numbers that represents red, green and blue in a location. Red, green and blue (RGB) are the primary colours used in mixing light to generate any other colour provided the correct amount is mixed. A 256 level of each colour will require 8 bits for each colour which implies that, each colour pixel requires three bytes (24 bits) of memory to be stored [9].

Images carry much information and therefore need to be protected especially from unauthorized users. Sending images over internet makes it vulnerable and hence the need to encrypt before sending them across networks.

B. *Cryptography*

A field in computer science and mathematics that deals with the formulation of secured communication between two parties in the presence of a third party is cryptograph [10, 11].

Data or information that can be understood at its original state without any special technique applied on it is called a plain-text (cipher-image). The method of disguising plain – text in a way its contents cannot be understood is encryption. When a plain-text is encrypted, the output is called cipher-text (cipher-image). Encryption is used to ensure

that, only the intended receiver of a message understands it. The method used in converting cipher-text back to plain-text is called decryption [12]. Figure 2 depicts the encryption and decryption process.

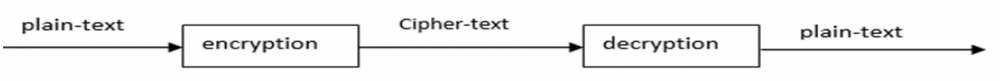

Figure 2. The encryption and decryption process.

C. *Image Cryptosystems based on Chaos*

Image scrambling transforms are mainly used to generate a chaos image aimed at making it difficult for human vision/ computer vision systems to decipher the true meaning of original images and to make it possible to retrieve the original image from the scrambled image if the user understands the scrambling technique that was used [13].

Over the years, many image encryption schemes based on chaotic systems have been proposed by researchers. The first of this kind was proposed in 1960 by a Russian mathematician Vladimir I. Arnold known as Arnold's cat map [14].

Arnold's cat map is defined as the mapping [15];

$$\Gamma : \mathbb{R}^2 \to \mathbb{R}^2 \text{ where } \Gamma\left(\begin{bmatrix} x \\ y \end{bmatrix}\right) = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix} \bmod 1 \quad (1)$$

where x, y are vector values of X and Γ is Arnold's cat map operation.

Arnold's encryption scheme is robust but periodic and cannot be used on rectangular images except square images. The periodicity in it was its greatest vulnerability since a cryptanalyst can easily study the number of times an image needs to be shuffled before the original image is retrieves from the encrypted one.

Chung and Chang [16] presented a novel method for binary image encryption. In their approach, dissimilar scan patterns are put at similar level in the structure of the scan tree and a run-encoding technique that is two-dimensional is employed. The encryption scheme can encrypt images well, giving higher security and a good compression ratio when compared to the earlier results. However, this new approach requires high processor power to be able to encrypt and compress an image in time before transmission because of the several scan patterns that is being used and can be used on binary images only.

Salleh et al. [17] have proposed an alternative symmetric-key encryption approach for securing images. This encryption scheme comprises of three main functions. The first uses Baker's transformation to transform unit square [0, 1] to [0, 2] × [0, ½] (stretch operation) and transform [0, ½] × [0, 1] to [0, 1] × [0, ½] and [½, 1] × [0, 1] to [0, 1] × [½, 1] (stretch operation). The second is the nonlinear feedback substitution which changes gray scale level of pixels by performing a bitwise non-linear feedback operation. The last which is the third function is used to further randomize the position of pixels by rotating each pixel to the left with 0, 1, 2, 3 or 5 shifts depending of the modulus of the value of the row number in which the pixel is located. But the gray level of encrypted images changes due to permutation and substitution operation on the bits in the algorithm. This algorithm proved robust but could not encrypt colour images.

Zhang et al. [18] improved the features of confusion and diffusion with regards to discrete exponential chaotic maps. A key scheme was designed for the resistance to differential attack, grey code attack, and statistic attack. Results analysis indicate that the scheme is efficient and very secure. The only flaw in this algorithm is that, it was designed with the assumption that all images to be encrypted are square images and will not encrypt rectangular images efficiently.

Mitra et al. [19] proposed a new approach for image encryption using a blend of different permutation techniques of bits, pixels and blocks aimed at reducing the correlation among neighboring pixels. The application of different permutation techniques is random and does not follow a prescribed order. This approach to encryption proved effective and easy to implement. Implementation of this algorithm during transmission over a network will require more time or higher resource since the sequence of the permutation process must be the precise reverse of the order used at the transmission end. So, the random combination seed generated at transmission must also be sent to the destination of the encrypted image through a secure communication/ transmission channel else the output will produce no visible information.

Shao et al. [13] proposed two kinds of two-dimensional matrix transforms called 2D triangular mappings meant to overcome the short comings of the 2D Arnold transform and 2D Fibonacci-Q. These transforms can encrypt and decrypt rectangular images without resizing them at a low computational cost. However, it could not encrypt 3D images.

Younes and Jantan [20] made known a block-based transformation process that is

based on the combined knowledge of image transformation and Blowfish encryption algorithm. Results after simulation showed that the correlation between values of pixels was decreased significantly but required high computer resources to complete encryption and decryption process.

Struss [21] used both the Arnold's cat map and Chen's chaotic map for an image encryption algorithm. The first transform is used to shuffle the pixel values of images whiles the second is used to change the grayscale values of pixels. This blend of the two transforms approach changes the gray values and mixes up the location of pixels. This make it more secure than using a single approach. However, this encryption scheme works on grayscale images and affects the original appearance of the image.

Ahmad and Alam [22] proposed a novel image cryptosystem based on three chaotic maps. In the proposed algorithm, the original image is disintegrated into blocks of dimensions 8×8. Thus, image random playback is performed using the 2D cat map in blocks. Random order parameters are randomly generated using a coupled 2D logistics map. Subsequently, the mixed image is further encrypted using a one-dimensional generated logistic sequence of maps. This scheme was safe but works only in 2D square images.

A novel algorithm proposed by Chattopadhyay et al. [23] for encoding digital images uses a circle map with three parameters. Their algorithm showed an increase in security of encrypted image against chosen-plaintext, cipher-text-only and chosen-cipher-text attacks. But had a relatively small key space that may not stand a brute-force attack.

Mishra et al. [14] introduce a novel spatial domain image scrambling map formed on Fibonacci and Lucas series that is capable of being used in several spatial domain image processing approaches of disguising data and secret communications such as Steganography and watermarking. Though it was a good system, it was periodic and could only encrypt grey scale images.

Alhassan and Gbolagade [6] used a modified Arnold transform algorithm and the moduli set $\{2^{n+1}-1, 2^n, 2^n-1\}$ to propose an image encryption scheme. Their encryption scheme uses RNS to Decimal encoder to decompose an image into three residues. These residues are then merged together and then encrypted using the modified Arnold transform. Their approach proved robust against several attacks. However, their proposed scheme resizes the original image into a perfect square before processing which increases the processing time.

An encryption scheme founded on the moduli set $\{2^n, 2^{n+1}-1, 2^{n+1}+1, 2^n-1\}$ was proposed by Reddy and Karumuri [24]. Their approach was to reduce the pixel values to their residues and combine them to form continuous words that could be further encrypted using advance encryption standard. However, advanced encryption standard is likely to increase the file sized because of the redundancy in image data. Also, AES comes with padding which also increases data size slightly.

Amalarethinam and Geetha [25] proposed an encryption and decryption in public key cryptography based on magic rectangle. In their approach, the images to be encrypted will have their byte values extracted and transposed as magic rectangle values. These magic rectangle values are further encrypted to produce a cipher text. Numerical values of the magic rectangle are displaced from their original positions and encrypted to produce the cipher text. Therefore, images that are encrypted using this approach are stored as text and converted back to images after transmission by reading the text, decrypting it and rearranging the values in the magic rectangle and transforming it into an image. This increases the average time taken to decrypt an image.

Chakraborty et al. [26] proposed an encryption scheme using DNA substitution and chaotic maps. This method selects an image pixel, converts it into 8 bits binary format and now reverses it. The reversed bits are then divided into four pairs and four new parameters are chosen for the logistic map as key. For every pair, a 12 bits sequence is generated using chaotic logistic map. And the 12-bit sequence is divided into 3 groups of length 4. Then a binary sequence of length 4 is generated by performing an XOR operation on the three groups key sequence. The 4-bit sequence is reversed, decimal value found, and the mod 6 value is calculated to select the transformation sequence. Now, the key is divided into 6 groups of length 2 by performing an XOR operation on the 6 groups key sequence, and the 2 bits are reversed. The decimal value of the reversed two bits is then found and converted to mod 3 as the iteration number. A complementary value is chosen from the sequence and used to find the encoding value in decimal. After all these operations produces four values which is converted to binary and all pairs are reversed. The pairs are then combined to get an 8-bit binary sequence and for the 4 pairs, a 48 bits key sequence of which we divide into 6 groups of length 8. A binary sequence of length 8 is generated by performing XOR operation on the 6 group key sequence which is reversed, and the decimal value is then calculated. The calculated value is then assigned as the encoded image pixel. This approach for securing images proved robust but uses more time to complete an encryption process.

An image encryption technique proposed by Ferdush et al. [27] combines the idea of one time pad with RGB value. Their scheme performs a bitwise XOR operation between RGB and a false image which is generated by the key generator. The bitwise operation is what is referred to as one - time pad. The R, G and B value of the resultant image are swapped in the follow order;

- Green image = Blue image
- Blue image = Red image
- Red image = Green image.

After the above operation, every pixel value of the red images is randomized using a formula and mod 255 of each pixel is calculated. The final red green and blue image is the cipher image.

Deshmukh [28] proposed image encryption and decryption using Advanced Encryption Standard (AES) algorithm. This encryption scheme encrypts by substituting the bytes, shifting rows, mixing columns and adding a round key. These four transformations mentioned are applied on an image respectively to encrypt it. This algorithm proved secured because it has large key space and resistant to attacks such as plaintext attack, cipher attacks and brute force attack. Apply four transforms will require high computer resources making this encryption scheme quite expensive in terms of computer resources and AES will increase the size of image after encryption.

Kalubandi et al. [29] proposed an encryption algorithm using AES and visual cryptography. There are two inputs in this approach; the image to be encrypted and the key which is a string. The key is then converted to hashes using SHA 256 hashing algorithm. The image is then encoded into Base64 string. The encoded image and the hashed key are then used to produce a cipher text by passing them through AES 256 encryption algorithm. The original key is then transformed into an image using ASCII encoding and then splitting the produced image into shares. This was simulated using python. After the cryptanalysis on this encryption scheme, the system proved robust against all known attacks. However, it involves several time-consuming processes which slow down the entire encryption and decryption system.

Fu et al. [4] suggested a new image security algorithm for colour images. This algorithm employs the hyperchaotic Lu system and logistic map. The hyperchaotic Lu system generates the keystream sequence for encoding pixel values whiles the logistic

map generates the keystream sequence for mixing up the pixels. A disturbance is also introduced during the iteration period to increase entropy of pixel values. Results from the analysis of this encryption scheme proved some higher security against various statistical attacks but take a longer time to process given limited computer resources.

Ye et al. [30] introduced an encryption algorithm that contains modulation, permutation and diffusion in processes in it. Entropy of image information is involved in the generation of keystream. Keys used in the permutation and diffusion processes interact with each other so that the algorithm can act as one entity to enhance security.

Yu et al. [31] proposed a new cryptographic scheme for four images based on Fresnel transformations (QFST) quaternion, computer hologram and the two-dimensional map regulated sinusoidal logistics (LASM) (2D) generated is presented. To treat the four images holistically, two types of Fresnel transform (QFST) were used to defined quaternions and the corresponding calculation method for a derived matrix quaternion. In the proposed method, the four original images, which are represented by the quaternion algebra are processed in a holistic vector mode using QFST first. Therefore, the input of complex amplitude, is constructed with components of the clear images transformed with QFST, codified by the Fresnel transforming two virtual independent random phase masks (RPM). To avoid sending RPMs complete the receiver for decryption, the RPMs are generated using 2D-LASM, which makes the amount of key data drastically reduced. Subsequently, using the Burch method and the displacement interferometry, the hologram generated by the computer is produced. To improve security and weaken correlation, the encrypted hologram is encoded in 2D-LASM. The experiments demonstrate the validity of the cryptographic technique of the proposed image. But there is a significant increase in the size of cipher images produces from this method.

Liu et al. [32] experimentally implemented a color image cryptography system based on optical chaos with embedded ARM hardware. The experiment uses a vertical cavity surface emission laser (VCSEL) subject to positive optoelectronic feedback and the chaotic signal is obtained with the appropriate parameters. The chaotic optical signal is transformed into chaotic optical data via an analog-to-digital converter. In the experiment, chaotic optical data dominates the cryptographic process of the image in which the advanced gravitational model and the double-breast map serve to encrypt the color image. The encrypted image can be transmitted securely through cloud services and therefore the hardware card can decode the encrypted image in an incomprehensible

way. The experimental results clearly show that cryptography of color images was successfully performed.

III. Methodology

A. *Residue Number System*

The study of Residue Number System (RNS) started in the third century by Sun Tsu who presented an approach to using the remainders of an integer after dividing it by 3, 5 and 7. Congruence relation is the bases for RNS, which is defined as follows.

Two whole numbers a and b are considered congruent modulo m if the difference of a and b can be divided by m without a remainder: mathematically, it is common to write $a \equiv b \pmod{m}$ to represent this. In this way, for example, $11 \equiv 8 \pmod 3$, $11 \equiv 5 \pmod 3$, $10 \equiv 1 \pmod 3$, and $10 \equiv -2 \pmod 3$. The whole number m is a modulus or base, and the assumption is that, its values exclude unity, which produces only trivial congruencies [33].

If r and q represent remainder and quotient, respectively, of the integer a when divided by m, that is, $a = q \cdot m + r$ then, by definition, $a \equiv r \pmod{m}$. The number r is referred to as the residue of a with respect to m, and usually denoted by $r = |a|_m$. The set of smallest values of m, $(0, 1, 2, \ldots, m-1)$, which the residue can assume is said to be the set of least positive residue modulo m. Except if otherwise stated, the assumption is that these are the residues in use. Assuming a set $\{m_1, m_2, \ldots, m_N\}$ of N positive and pairwise relatively prime moduli. Let M represent the product of the moduli $(M = \prod_{i=1}^{n} m_i)$. M is referred to as the dynamic range. Then every number $Y < M$ has a distinct representation in the residue number system, which is the set of residues $|Y|_{m_i} : 1 \le i \ge N$ [34].

For example, using the moduli set $\{7, 8, 9\}$, the number 150 can be represented in residue number system as;

$$y_1 = |Y|_{m_1} = |150|_7 = 3, \quad y_2 = |Y|_{m_2} = |150|_8 = 6, \text{ and}$$

$$y_3 = |Y|_{m_3} = |150|_9 = 6.$$

Thus, the RNS representation of 150 is thus $(3, 6, 6)_{RNS(7, 8, 9)}$.

B. *The k-shuffle*

A deck containing 52 cards can be separated into 2 piles, each containing 26 cards. These two piles can further be re-arranged via 8 different iterations to obtain the original arrangement back. This is referred to as the perfect-2-shuffle or faro shuffle. There exist two instances of perfect-2-shuffle or faro shuffle; an out shuffle which leaves the top card at its original position and the second shuffle which makes the top card the second [35, 36], Ramnath and Scully [37], [38].

Assuming $n, m \in Z$ and $n, m > 1$. Given that $l = nm$ cards are numbered in order from 1 to *l*. The cards are placed *n* cards each in *m* piles in the following order; the first pile of cards contain cards from *1* through to *n*. the second has cards $n + 1$ through to $2n$, the third pile contain cars $2n + 1$ through to $3n$. The sequence is continuous until the last pile which would be $(m - l)n + l$ up to *nm*. According to Packard [36], a perfect k-shuffle rearrange the cards in the following way; draw all first cards from each pile, followed by the second, third, fourth, right up to the last card in each pile. The first and the last card remain at their respective positions after the re-arrangement. The order of a perfect k-shuffle as described [36]; $d_k(n)$, is the minimum number of times the k-shuffle need to be iterated to return cards to their original arrangement.

(1) *Modified k-shuffle Algorithm for Images Encryption*

The traditional k-shuffle is a technique for shuffling cards and will not be better suited for shuffling images. Therefore, it has been modified in the algorithm below for images;

Let *P* be the image, *s* be the number of rows or pixel values in *P*, *k* be the number of columns of pixels in *P* and *I* be the number of iterations.

- Read *P*
- Put the rows (*s*) of *P* into one column (*dp*)
- For each item in column *dp*
  - Pick the next *s*-value and stack into the *i*th column of *P*
- Present the scrambles image as *y*.

(2) *Reverse for Modified k-shuffle Algorithm for Images*

This shuffling technique is top to down shuffling and non-reversible [39], but a

reverse algorithm has been formulated to be used in the decryption process of the proposed cryptosystem. The algorithm is as follows:

Let y be the cipher image, k be the number of columns in y, n be the first item in column dp, i be the position which item is to be found and l the position of the last item in column dp

- Read cipher image y
- Put the rows (s) of y into one column (dp)
- The first (1st) and last (l) items in column dp remain in the original position in y
- For the rest of each item in column dp (2nd through to l–1) calculate the position
    - position = ((k*(i–1) + 1) mod(l–1))
    - Go to the position and pick the item to the next position in y
- Present the final arrangement as p.

C. *Proposed Image Encryption Algorithm via k-shuffle and RNS*

The encryption algorithm takes as input the original image (P), number of iterations for the k-shuffle (i) and number of bits (n) for the moduli set adopted. The output will be the cipher images x_1, x_2 and x_3 that will be transmitted over network. The proposed encryption algorithm is stated as follows:

- Input P, i and n
- For each i
    - Scramble P using k-shuffle technique into the disguised form y
- Find the residual cipher images x_1, x_2 and x_3 using the RNS encoder
- Transmit x_1, x_2 and x_3.

D. *Proposed Image Decryption Algorithm*

The decryption algorithm is the reverse of the encryption algorithm where the receiver receives the residual cipher images x_1, x_2 and x_3 together with i and n, and decrypt them to the plain image P. The decryption algorithm is thus stated as follows;

- receive x_1, x_2, x_3, i, n

- Compute *y* using the RNS decoder
- For each *i*
    - o Descramble *y* into *P* using the k-shuffle decoder
- Show *P* to user.

The block diagram of the proposed cryptosystem is shown in Figure 3.

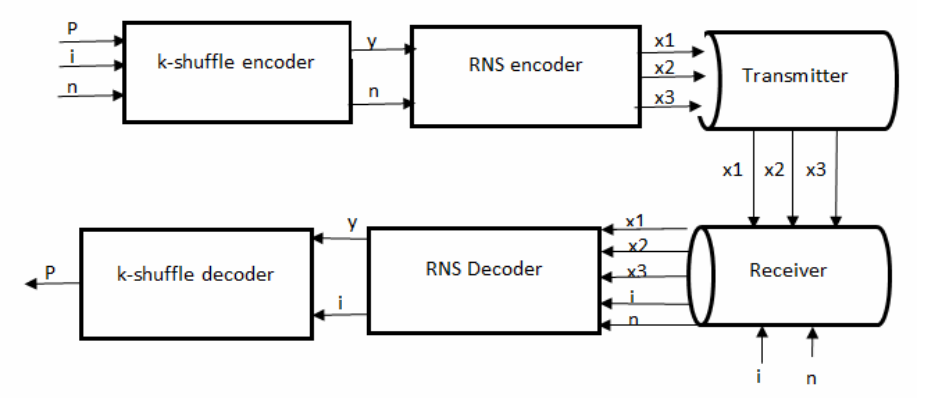

Figure 3. A block diagram of the proposed cryptosystem.

IV. Results Analysis and Interpretation

Results and interpretation of the proposed cryptosystem are presented here. All simulations and interpretations of results obtained are done using MATLAB Simulink simulation tool. The simulations were done using the moduli sets $\{2^n-1, 2^n, 2^n+1\}$ and $\{2n+2, 2n+1, 2n\}$. The Chinese remainder theorem (CRT) was adopted for $\{2^n-1, 2^n, 2^n+1\}$ while the reverse converter proposed by Gbolagade and Cotofana [40] was used for $\{2n+2, 2n+1, 2n\}$. The images, 'footbal.jpg', 'cameraman.tif' and 'hands1.jpg' were used for the simulation.

A. *Image Encryption using k-shuffle and the Moduli Set* $\{2^n-1, 2^n, 2^n+1\}$

The MATLAB Simulink system for simulating the proposed image encryption and decryption algorithms using the moduli set $\{2^n-1, 2^n, 2^n+1\}$ is shown in Figure 4. The encryption process consists of '*kshuffle_Encoder*' and '*RNS_Encoder_CRT*' subblocks. '*kshuffle_Encoder*' receives the original image (*P*) together with the number of

reshuffles (*iter*) and number of bits (n) and encrypts P into the cipher image (y). y is fed into '*RNS_Encoder_CRT*' as X along with n to be encoded into the residual images x_1, x_2 and x_3 for transmission. At the receiver's side, the residual cipher images (i.e. x_1, x_2, and x_3) are decoded back into the cipher image X using the '*RNS_Decoder_CRT*'. X is subsequently de-shuffled into the original image P using the '*kshuffle_Dencoder*'. The subblock '*Video ViewerCRT*' receives y as image and displays it.

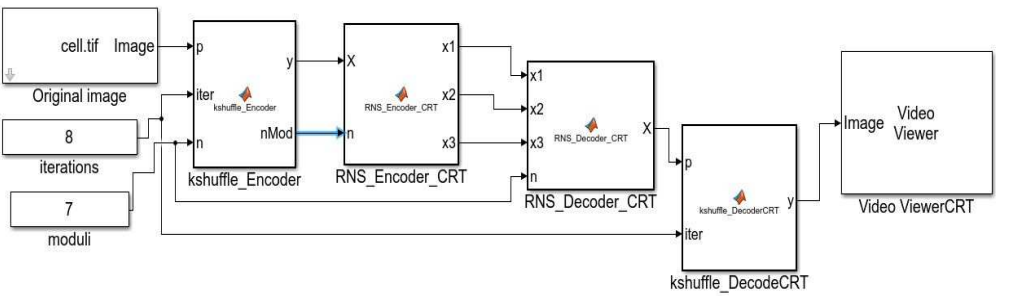

Figure 4. MATLAB Simulink system for simulating the proposed image encryption and decryption algorithm using the moduli set $\{2^n - 1, 2^n, 2^n + 1\}$.

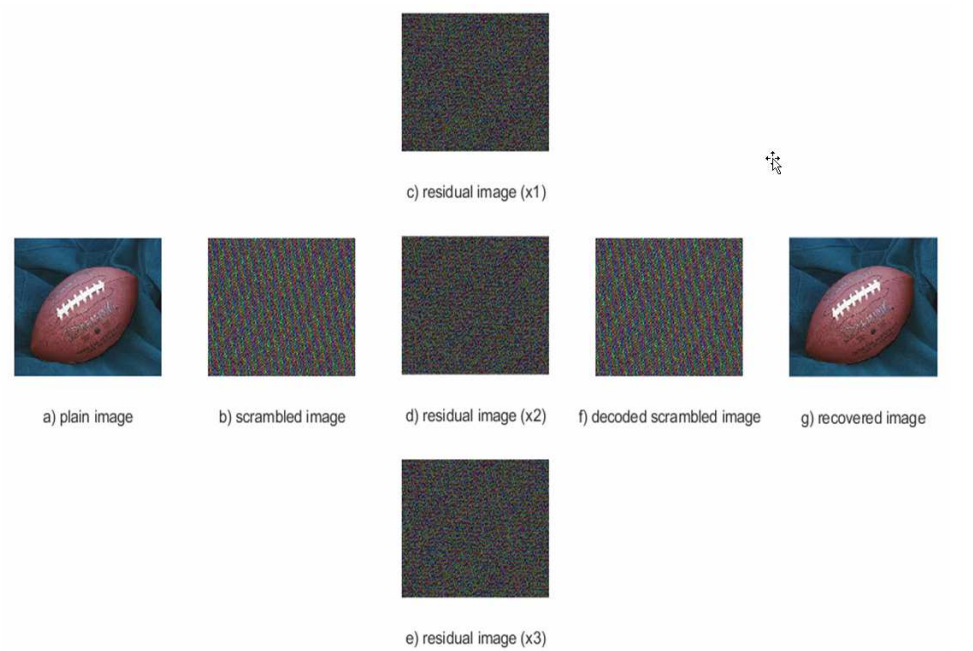

Figure 5. Simulated results of 'football.jpg' using 4–shuffles and 7-bits as cipher keys.

B. *Image Encryption using k-shuffle and the Moduli Set* $\{2n + 2,\ 2n + 1,\ 2n\}$

The MATLAB Simulink system for simulating the proposed image encryption and decryption algorithms using the moduli set $\{2n + 2,\ 2n + 1,\ 2n\}$ is shown in Figure 6. The encryption process consists of '*kshuffle_Encoder*' and '*RNS_Encoder_LCM*' subblocks. '*kshuffle_Encoder*' receives the original image (*P*) together with the number of reshuffles (*iter*) and number of bits (*n*) and encrypts *P* into the cipher image (*y*). *y* is fed into '*RNS_Encoder_CRT*' as *X* along with *n* to be encoded into the residual images x_1, x_2 and x_3 for transmission. At the receiver's side, the residual cipher images (i.e. x_1, x_2, and x_3) are decoded back into the cipher image *X* using the '*RNS_Decoder_LCM*'. *X* is subsequently de-shuffled into the original image *P* using the '*kshuffle_Dencoder*'. The subblock '*Video ViewerLCM*' receives *y* as image and displays it.

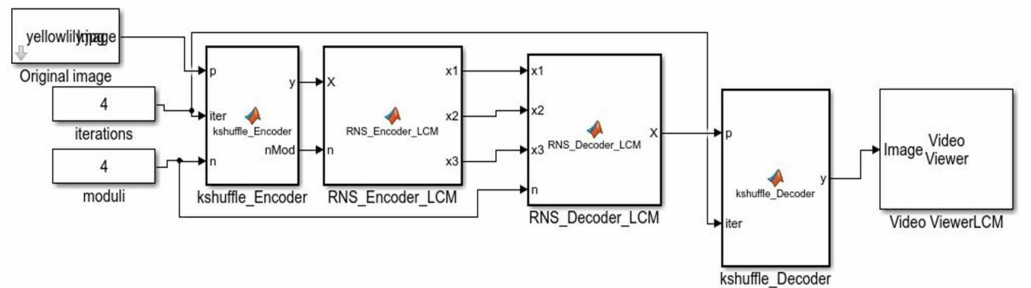

Figure 6. MATLAB Simulink system for simulating the proposed image encryption and decryption algorithm using the moduli set $\{2n + 2,\ 2n + 1,\ 2n\}$.

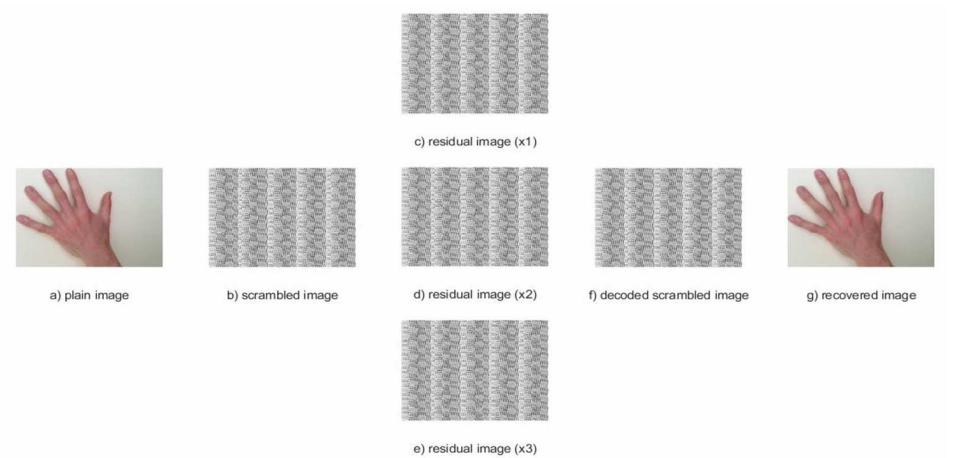

Figure 7. Simulated results of 'hands1.jpg' using 6–shuffles and 7-bits as cipher key.

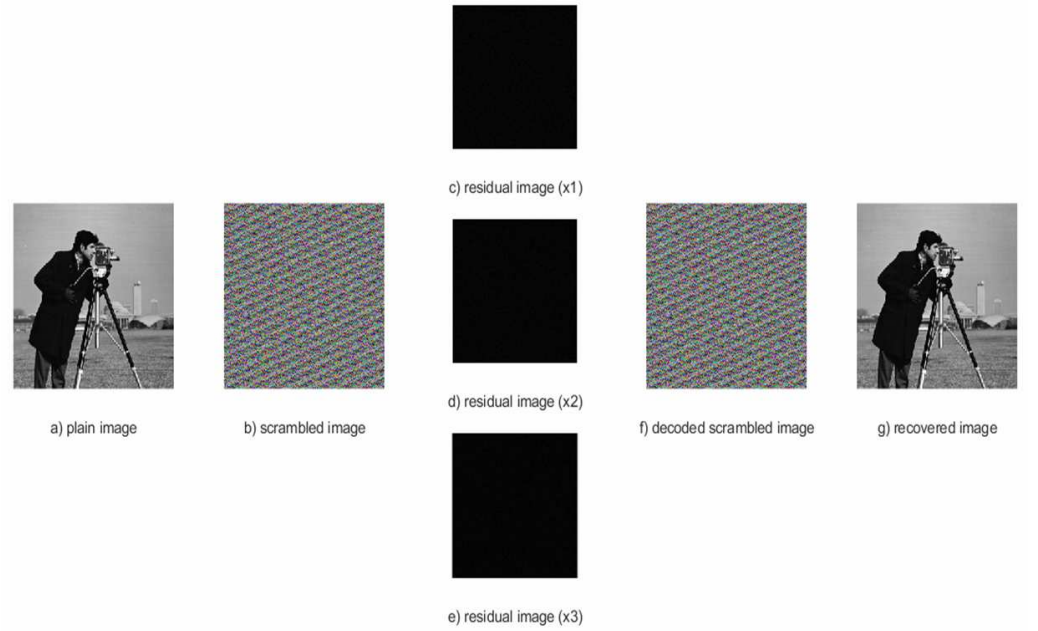

Figure 8. Simulated results of 'cameraman.tif' using 15–shuffles and 5-bits as cipher key.

C. *Analysis of Results*

(1) *Visual degradation*: In this analysis the original and cipher images are compared using visual inspection to establish whether they bear some resemblance. Figures 5, 7 and 8 show the results obtained. It is clearly seen through visual inspection that the cipher images (c, d and e) and their corresponding original images (a) are completely different from each other. This difference is reinforced with the histograms of the images shown in Figure 9. Figure 9, (a) and (e) are the histograms of the plain images while (b), (c), and (d) are the histograms of the residual images for (a); and (f), (g) and h) are the histograms of the residual images for (e). The histograms of the originals and their residual counterparts are completely different; hence the proposed scheme can withstand a histogram attack.

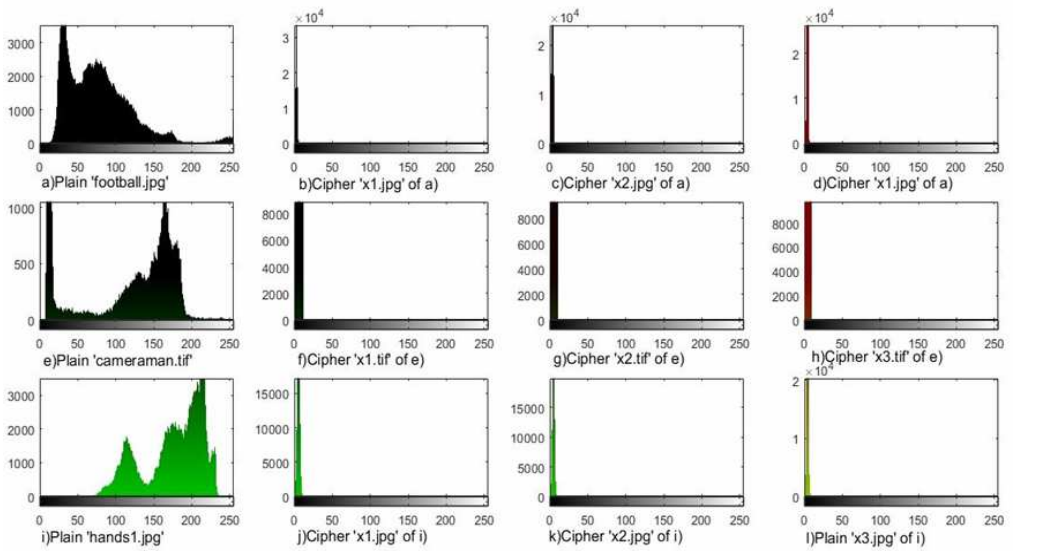

Figure 9. Histogram of plain images and their respective ciphers.

(2) *Key space analysis*: For any cryptosystem to resist Bruce-force attack, its key space should be reasonably high since this form of attack depends exhaustively on the search of the key space. The proposed scheme has two key parameters (number of reshuffles(i) and number of bits for encoding(n)). The length of i depends on the dimension of the given image while n does not exceed 2^8. Thus, for a 256×256 image, $i = 2^{16}$ and $n = 2^8$. Any adversary using Bruce-force attack needs approximately $2^{16} \times 2^8 = 2^{24} \approx 16{,}777{,}217$ key combinations to exhaustively search the entire key space in order to recover the original image. Also, cipher images can be transmitted in 3! different ways which adds extra security to transmitted cipher images. The adversary needs the correct association of moduli set to residue images. Hence, given limited computing resources the proposed scheme offers some level of resistance to Bruce-force

(3) *Key sensitivity analysis*: Every good cryptosystem should be highly sensitive to slight changes to the key parameters used for both encryption and decryption process. Each key parameter set should produce different cipher/recovered image when used. To test the effectiveness of the proposed scheme, one set of key parameters are used for encryption and different sets of key parameters are used for decryption of the cipher images obtained. The difference here are the change in only one of the key parameters (an increment of 1 was used in this case for i) used for encryption and the other maintained. Figure 10 shows failed recovered images when the cipher key parameters are

changed; (a) p = 'football.jpg', i = 3 and n = 7 using the moduli set $\{2^n - 1, 2^n, 2^n + 1\}$ and the moduli set $\{2n + 2, 2n + 1, 2n\}$.

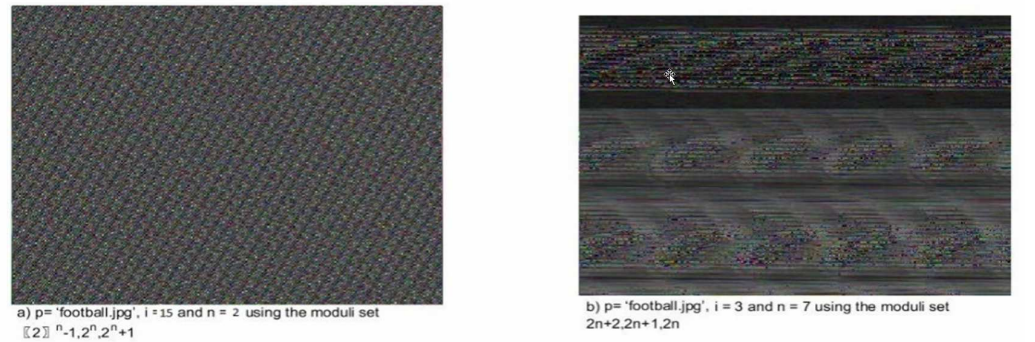

Figure 10. A failed recovered images when the cipher key parameters are changed.

(4) *Procession time*: In order to measure the speed of the proposed schemes the processing time used by MATLAB to encrypt/decrypt given images were measured using a system with 1.6GHz (2 CPUs) processor and 4GB memory. Table 1 summarizes the results obtained by using the cipher key parameters $i = 15$, $n = 5$ for different image formats and dimensions. The results reveal that the encryption time is less than a third of the decryption time and both encryption and decryption processing times increase as the dimension of the given image increases. While the encryption times for both schemes are approximately the same, the decryption time for the scheme with the moduli set $\{2n + 2, 2n + 1, 2n\}$ is slightly lower than that of the moduli set $\{2^n - 1, 2^n, 2^n + 1\}$. Thus, in terms of processing speed the former is better than the later. This is because the reverse conversion of the earlier is optimized as compared to the later. The processing times of each of the sub-blocks in proposed schemes are summarized in Table 2. In comparison, 94% of the encryption processing time is attributed to the k-shuffle process while the RNS process only takes approximately 6%. On the other hand, approximately 15% of the decryption time is attributed to the RNS decoding process while k-shuffle decoding process takes 85%.

Table 1. Average processing time of proposed scheme.

File (dimension)	**Proposed Scheme** $i = 15,\ n = 5$			
	k-shuffle and the moduli set $\{2^n - 1,\ 2^n,\ 2^n + 1\}$		**k-shuffle and the moduli set** $\{2n + 2,\ 2n + 1,\ 2n\}$	
	Encryption time(s)	**Decryption time(s)**	**Encryption time(s)**	**Decryption time(s)**
Hands1.jpg (240x320x3)	14.388	50.868	14.563	45.088
ColoredChips.png (391x518x3)	36.944	136.859	37.469	123.375
Cameraman.tif (256x256)	11.475	43.351	12.113	38.322

Table 2. Average processing time for each sub-block

File (dimension)	**Proposed Scheme** $i = 15,\ n = 5$			
	k-shuffle and the moduli set $\{2^n - 1,\ 2^n,\ 2^n + 1\}$		**k-shuffle and the moduli set** $\{2n + 2,\ 2n + 1,\ 2n\}$	
	k-shuffle (RNS) encryption time(s)	**k-shuffle (RNS) decryption time(s)**	**k-shuffle (RNS) encryption time(s)**	**k-shuffle (RNS) decryption time(s)**
Hands1.jpg (240x320x3)	13.528(0.859)	43.019(7.849)	13.694(0.869)	42.934(2.153)
ColoredChips.png (391x518x3)	34.738(2.206)	116.488(20.372)	35.266(2.203)	117.556(5.819)
Cameraman.tif (256x256)	10.728(0.747)	36.653 (6.698)	11.363(0.750)	36.478(1.844)

File (dimension)	Proposed Scheme $i = 10,\ n = 5$			
	k-shuffle and the moduli set $\{2^n - 1,\ 2^n,\ 2^n + 1\}$		k-shuffle and the moduli set $\{2n + 2,\ 2n + 1,\ 2n\}$	
	k-shuffle (RNS) encryption time(s)	k-shuffle (RNS) decryption time(s)	k-shuffle (RNS encryption time(s)	k-shuffle (RNS) decryption time(s)
Hands1.jpg (240x320x3)	9.064(0.859)	28.823(7.849)	9.174(0.869)	28.766(2.153)
ColoredChips.png (391x518x3)	23.170(2.206)	77.697(20.372)	23.522(2.203)	78.409(5.819)
Cameraman.tif (256x256)	7.152(0.747)	24.436 (6.698)	7.575(0.750)	24.319(1.844)

(5) *Encoding analysis*: The weight of a pixel in an image with 8 bits-per-pixel (8 bpp) spans 0 to 255. Thus, 8 bits are required to encode every pixel in such an image. The introduction of RNS reduces this bit requirement to a significant level. For instance, at best performance, the chosen moduli sets encode a 255 pixel to a 3 bpp value. This is less than half the original bits required to encode and transmit a 255 pixel. Thus, transmission speed is enhanced since smaller values are used. Table 3 shows a summary of original size and size of cipher during transmission. It is therefore clear that the proposed schemes reduce the size of cipher images significantly. Hence improving the speed of transmission.

Table 3. Summary of original size of plain images and size of cipher during transmission.

Original image (size)	Cipher image size			Total size $(x_1 + x_2 + x_3)$
	x_1	x_2	x_3	
Hands1.jpg (21.6 kb)	3.58 kb	3.05 kb	2.73 kb	9.36 kb
Football.jpg (12.8 kb)	2.10 kb	2.43 kb	2.58 kb	7.11 kb
ColoredChips.png (296 kb)	6.67 kb	5.64 kb	5.37 kb	17.68 kb

(6) *Chosen /known plaintext attacks*: Figure 11 shows the histogram analysis of chosen/known plain text attacks. Part (c) is the histogram of XOR-ing the plain image (a) and its corresponding cipher image (b). Part (e) is obtained by XOR-ing part (c) and an unknown cipher image (d). Since the histogram of (a) and (e) are completely different the proposed techniques are resistant to chosen/known plaintext attacks.

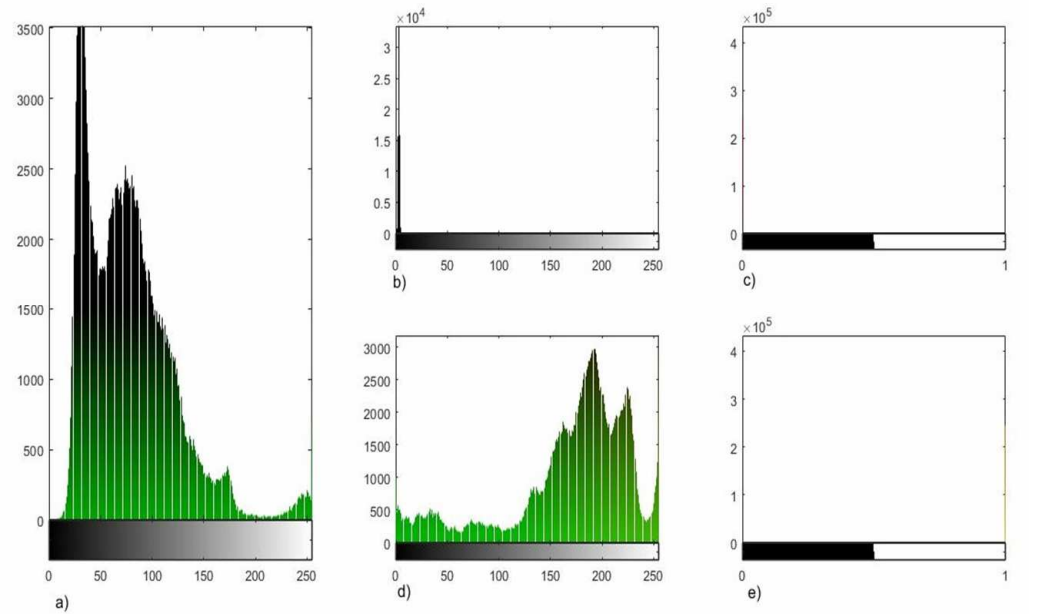

Figure 11. Histogram analysis of chosen/known plain text attacks.

(7) *PSNR and MSE for the encryption schemes*: The peak signal-to-noise ratio (PSNR) and the Mean Square Error (MSE) are error metrics that are used to ascertain the quality of a compressed image compared to the original. PSNR is used to determine the quality of the compressed image whiles the MSE is the cumulative square error between original and compressed image. A high PSNR indicates a quality image whiles a high MSE indicates a high error margin between original and compressed image. Therefore, a low PSNR and a high MSE between an original and cipher image shows the vast difference between original and cipher images. In this analysis, the MSE and PSNR of images and their respective ciphers will be calculated and interpreted.

(8) *Entropy analysis*: The statistical measure of the randomness that characterizes image texture is known as entropy. The entropy (H) of a source (S) can be calculated using the following (Ahmad and Alam [22]);

$$H(S) = -\sum_{(i=1)}^{N} p(s_i)\log_2 p(s_i),$$

where $p(s_i) =$ probability of s_i, and entropy is expressed in bits. If the source S produces 2^8 symbols with equivalent probability, i.e. $S = \{s_1, s_2, ..., s_{256}\}$, then the result of entropy is $H(S) = 8$. This is the ideal representation of a true random source and value of entropy for the message source (S). The entropy of the information in a cipher image shows the grey value distribution. The higher the uniform distribution of grey values, the higher the entropy of information. A significantly low value than the ideal, which is 8, then, the higher the predictability which threatens the security of the image (Ahmad and Alam [22]).

From Table 4 the entropy of the image after k-shuffle is higher than the original image and are not significantly lower than the ideal value 8. Therefore, the scheme is secure against entropy attacks.

Table 4. PSNR and MSE for $\{2^n - 1, 2^n, 2^n + 1\}$.

Original Image	**Cipher Image**					
	MSE			**PSNR**		
	x_1	x_2	x_3	x_1	x_2	x_3
football.jpg	2.4895e+03	2.4653e+03	2.4407e+03	14.2117	14.2546	14.2987
coloredChips.png	1.0491e+04	1.0425e+04	1.0386e+04	7.9990	8.0270	8.0435
cameraman.tif	5.7633e+03	5.7246e+03	5.6911e+03	10.5241	10.5533	10.5788

V. Conclusion

The major contributions of this paper are presented below. The proposed cryptosystem produces cipher-images that:

- Require a smaller number of bits and memory allocation to represent cipher-images;
- Can be transmitted faster across networks due to smaller pixel values and sizes;
- Consume less disk space;
- Has strong resistance to statistical attacks (brute-force, correlation coefficient, information entropy and histogram);

- Is independent of periodicity in its decryption process. Thus, the number of iterations to conduct is at the discretion of the user;
- Is also highly sensitive to a small change in any of the cipher keys;
- Recovers plain-image with minimal or no loss of any inherent feature.

References

[1] A. Roy, A. P. Misra and S. Banerjee, Chaos-based image encryption using vertical-cavity surface-emitting lasers, *Optik* 176 (2019), 119-131. https://doi.org/10.1016/j.ijleo.2018.09.062

[2] G. Ke, H. Wang, S. Zhou and H. Zhang, Encryption of medical image with most significant bit and high capacity in piecewise linear chaos graphics, *Measurement* 135 (2019), 385-391. https://doi.org/10.1016/j.measurement.2018.11.074

[3] M. Kumari, S. Gupta and P. Sardana, A survey of image encryption algorithms, *3D Research* 8(4) (2017), 37. https://doi.org/10.1007/s13319-017-0148-5

[4] C. Fu et al., A new chaos-based color image encryption scheme with an efficient substitution keystream generation strategy, *Security and Communication Networks* 2018 (2018), Article ID 2708532, 13 pp. https://doi.org/10.1155/2018/2708532

[5] M. Hazarika, A Review of Chaos Based Image Encryption Techniques, *International Journal of Engineering Research & Technology* (*IJERT*) 3(2) (2014), 2209-2212.

[6] S. Alhassan and K. Gbolagade, Enhancement of the Security of a Digital Image using the Moduli Set, *International Journal of Advanced Research in Computer Engineering & Technology* (*IJARCET*) 2(7) (2013), 2223-2229.

[7] H. Noura, L. Sleem and R. Couturier, A revision of a new chaos-based image encryption system: Weaknesses and limitations, arXiv preprint arXiv:1701.08371, 2017.

[8] J. Sachs, *Digital Image Basics*, Digital Light & Color, Cambridge, Massachusetts, 1999.

[9] V. Mishra, S. Kumar and N. Shukla, Image acquisition and techniques to perform image acquisition, *A Journal of Physical Sciences, Engineering and Technology* 9(1) (2017), 21-24. https://doi.org/10.18090/samriddhi.v9i01.8333

[10] M. Barakat, C. Eder and T. Hanke, *An Introduction to Cryptography*, Timo Hanke at RWTH Aachen University, 2018.

[11] P. Dixit et al., Traditional and hybrid encryption techniques: A survey, in: *Networking Communication and Data Knowledge Engineering*, Lecture Notes on Data Engineering

and Communications Technologies, vol. 4, Springer, Singapore, 2018, pp. 239-248. https://doi.org/10.1007/978-981-10-4600-1_22

[12] W. Stallings, *Cryptography and Network Security*, 4/E, Pearson Education India, 2006.

[13] L.-P. Shao et al., 2D triangular mappings and their applications in scrambling rectangle image, *Information Technology Journal* 7(1) (2008), 40-47. https://doi.org/10.3923/itj.2008.40.47

[14] M. Mishra et al., Image encryption using Fibonacci-Lucas transformation, 2012. arXiv preprint: arXiv:1210.5912. https://doi.org/10.5121/ijcis.2012.2312

[15] K. Shaw, *Arnold's Cat Map*, 2006.

[16] K.-L. Chung and L.-C. Chang, Large encrypting binary images with higher security, *Pattern Recognition Letters* 19(5-6) (1998), 461-468. https://doi.org/10.1016/S0167-8655(98)00017-8

[17] M. Salleh, S. Ibrahim and I. F. Isnin, Image encryption algorithm based on chaotic mapping, *Journal Teknologi* 39(D) (2003), 1-12. https://doi.org/10.11113/jt.v39.458

[18] L. Zhang, X. Liao and X. Wang, An image encryption approach based on chaotic maps, *Chaos, Solitons & Fractals* 24(3) (2005), 759-765. https://doi.org/10.1016/j.chaos.2004.09.035

[19] A. Mitra, Y. S. Rao and S. Prasanna, A new image encryption approach using combinational permutation techniques, *International Journal of Computer Science* 1(2) (2006), 127-131.

[20] M. A. B. Younes, and A. Jantan, Image encryption using block-based transformation algorithm, *IAENG International Journal of Computer Science* 35(1) (2008).

[21] K. Struss, *A Chaotic Image Encryption*, Mathematics Senior Seminar, University Minnesota, USA, 2009, pp. 1-19.

[22] M. Ahmad and M. S. Alam, A new algorithm of encryption and decryption of images using chaotic mapping, *International Journal on Computer Science and Engineering* 2(1) (2009), 46-50.

[23] D. Chattopadhyay, M. Mandal and D. Nandi, Symmetric key chaotic image encryption using circle map, *Indian Journal of Science and Technology* 4(5) (2011), 593-599.

[24] P. V. N. Reddy and R. Karumuri, Image encryption and decryption in RNS domain based on $\{2^n, 2^{2n+1}-1, 2^n+1, 2^n-1\}$ moduli set, *2016 International Conference on Communication and Electronics Systems* (*ICCES*), Coimbatore, 2016, pp. 1-5. https://doi.org/10.1109/CESYS.2016.7889984

[25] D. G. Amalarethinam and J. S. Geetha. Image encryption and decryption in public key cryptography based on MR, *2015 International Conference on Computing and Communications Technologies* (*ICCCT*), Chennai, 2015, pp. 133-138. https://doi.org/10.1109/ICCCT2.2015.7292733

[26] S. Chakraborty et al., A novel lossless image encryption method using DNA substitution and chaotic Logistic map, *International Journal of Security and Its Applications* 10(2) (2016), 205-216. https://doi.org/10.14257/ijsia.2016.10.2.19

[27] J. Ferdush, M. Begum and A. Mahmood, A new image encryption technique combining the idea of one time pad with RGB value, *International Journal of Computer Applications* 178(5) (2017), 12-15. https://doi.org/10.5120/ijca2017915823

[28] P. Deshmukh, An image encryption and decryption using AES algorithm, *International Journal of Scientific & Engineering Research* 7(2) (2016), 2229-5518.

[29] V. K. P. Kalubandi et al., A novel image encryption algorithm using AES and visual cryptography, *2016 2nd International Conference on Next Generation Computing Technologies* (*NGCT*), Dehradun, 2016, pp. 808-813. https://doi.org/10.1109/NGCT.2016.7877521

[30] G. Ye et al., A chaotic image encryption algorithm based on information entropy, *International Journal of Bifurcation and Chaos* 28(01) (2018), 1850010. https://doi.org/10.1142/S0218127418500104

[31] C. Yu et al., Four-image encryption scheme based on quaternion Fresnel transform, chaos and computer generated hologram, *Multimedia Tools and Applications* 77(4) (2018), 4585-4608. https://doi.org/10.1007/s11042-017-4637-6

[32] B. Liu et al. Experimental realizing image encryption based on optical chaos, Proc. SPIE 11052, *Third International Conference on Photonics and Optical Engineering*, 1105219, 24 January 2019. https://doi.org/10.1117/12.2522014

[33] N. Singh, An overview of Residue Number System, *National Seminar on Devices, Circuits & Communication*, November 06th – 07th, 2008, Organized by Department of ECE, B.I.T, Mesra, Ranchi, 2008.

[34] K. Isupov and V. Knyazkov, Interval estimation of relative values in residue number system, *Journal of Circuits, Systems and Computers* 27(01) (2018), 1850004. https://doi.org/10.1142/S0218126618500044

[35] P. Diaconis, R. Graham and W. M. Kantor, The mathematics of perfect shuffles, *Advances in Applied Mathematics* 4(2) (1983), 175-196. https://doi.org/10.1016/0196-8858(83)90009-X

[36] E. S. Packard, *The Order of a Perfect k-shuffle*, Texas Tech University, 1990.

[37] S. Ramnath and D. Scully, Moving card *i* to position *j* with perfect shuffles, *Mathematics Magazine* 69(5) (1996), 361-365. https://doi.org/10.1080/0025570X.1996.11996475

[38] A. Madain et al., Audio scrambling technique based on cellular automata, *Multimedia Tools and Applications* 71(3) (2014), 1803-1822. https://doi.org/10.1007/s11042-012-1306-7

[39] S. Goel, Analysis of top to bottom-*k* shuffles, *Annals of Applied Probability* 16(1) (2006), 30-55. https://doi.org/10.1214/10505160500000062

[40] K. A. Gbolagade and S. D. Cotofana, A residue to binary converter for the {2n + 2, 2n + 1, 2n} moduli set, *2008 42nd Asilomar Conference on Signals, Systems and Computers*, Pacific Grove, CA, 2008, pp. 1785-1789. https://doi.org/10.1109/ACSSC.2008.5074734

Issah Zabsonre Alhassan, Edward Danso Ansong, Gaddafi Abdul-Salaam
Department of Computer Science, Kwame Nkrumah University of Science and Technology, Kumasi, Ghana

Salamudeen Alhassan
Department of Mathematics and ICT, Bagabaga College of Education, Tamale, Ghana