Enhanced image security using residue number system and new Arnold transform

Akinbowale Nathaniel Babatunde[1)], Oke Afeez Adeshina[*2)], Abdulkareem Ayopo Oloyede[3)], Bello Aisha Oiza[4)]

[1,4)]*Department of Computer Science, Faculty of Communication and Information Technology, Kwara State University
Kwara State University Rd, 241103, Malete, Kwara State, Nigeria*

[2)]*Department of Computer Science, College of Natural and Applied Science, Summit University
P.M.B 4412, Irra Road, Offa, Kwara State, Nigeria*

[3)]*Department of Telecommunication Science, Faculty of Communication and Information Sciences, University of Ilorin
P.M.B 1515, Ilorin, Kwara State, Nigeria*

How to cite: A. N. Babatunde, A. A. Oke, A. A. Oloyede, and A. O. Bello, "Enhanced image security using residue number system and new Arnold transform," *Jurnal Teknologi dan Sistem Komputer*, vol. 9, no. 4, pp. 205-210, 2021. doi: 10.14710/jtsiskom.2021.14038, [Online].

Abstract – This paper aims to improve the image scrambling and encryption effect in traditional two-dimensional discrete Arnold transform by introducing a new Residue number system (RNS) with three moduli and the New Arnold Transform. The study focuses on improving the classical discrete Arnold transform with quasi-affine properties, applying image scrambling and encryption research. The design of the method is explicit to three moduli set {2^n, 2^{n+1}+1, 2^{n+1}-1}. These moduli set includes equalized and shapely moduli leading to the effective execution of the residue to binary converter. The study employs an arithmetic residue to the binary converter and an improved Arnold transformation algorithm. The encryption process uses MATLAB to accept a digital image input and subsequently convert the image into an RNS representation. The images are connected as a group. The resulting encrypted image uses the Arnold transformation algorithm. The encrypted image is used as input at decryption using the anti-Arnold (Reverse Arnold) transformation algorithm to convert the picture to the original RNS (original pixel value). Then the RNS was used to retransform the original RNS to its binary form. Security analysis tests, like histogram analysis, keyspace, key sensitivity, and correlation coefficient analysis, were administered on the encrypted image. Results show that the hybrid system can use the improved Arnold transform algorithm with better security and no constraint on image width and size.

Keywords *- cryptosystem; forward conversion; residue number system; reverse conversion*

I. Introduction

The protection of data and digital images has been the main interest in the last few decades because of the rapid development of internet and networking technologies [1]–[5]. Images have been used in different fields, including medicine, military, technology, engineering, fashion, music, advertisement, and education. However, since digital image processing and storage systems are increasingly being used, the fundamental issue of confidentiality, authenticity, and image validity has become a major concern. Over the years, numerous open and concealed forms of communication have been proposed to meet this need [4].

A lot of image scrambling and encryption techniques have been developed to increase the security standard [1], [5]-[8]. Most techniques, however, have used the old Arnold transform, which is not suitable for images with different numbers of columns and rows. Thus, they automatically increase these images' redundancy and disk size with decreasing quality [2], [4].

Oyinloye and Gbolagade [1] introduced the use of RNS to add extra security to the image scrambling involves pixel scrambling by random number generation and second layer encryption with Residue Number System (RNS) the forward conversion for the moduli set {2n-1, 2n, 2n +1} for the encryption stage. However, the quality of the decrypted image is reduced, especially for colored images.

Wu et al. [9] introduced a compact image encryption system using Arnold transformation. The authors used the Arnold Transform for the diffusing and confusing operations while simultaneously encrypting a pixel distribution instead of a data stream. The authors demonstrated an improvement in performance by analyzing the key-space, key sensitivity, correlation, cost time, and system security. A multi-region algorithm for the image scrambling encryption would provide additional security.

Alhassan et al. [10] implemented a secure information encryption and decryption scheme to improve the Huffman process. With four modules set {2^{n-1}}, {2^n-1},{2^n+1},{2^{n+1}-1} and two redundant modules set {2^{2n}-3, 2^{2n}+1}, the Residue Number System (RNS) is used for error handling using the standard Huffman algorithm definition. The rate of occurrence of all letters was employed to produce binary codes. Their projected

[*)] Corresponding author (Oke Afeez Adeshina)
Email: okeafeez@summituniversity.edu.ng

Copyright ©2021, The authors. Published by Department of Computer Engineering, Universitas Diponegoro

Submitted: 5 January 2021; Revised: 8 July 2021; Accepted: 18 July 2021; Published: 31 October 2021

method permitted an incomprehensible collection of encoded bits so the intended receiver could decrypt it with the right set of modules, decreased documents conveyance and storing costs, fault discovery, and rectification. The efficiency of the proposed RNS four-set encryption algorithm is theoretically assessed in terms of space, protection and the projected structure provides an excellent level of invulnerability compared to the traditional Huffman coding mentioned in [11] and the equivalent state of the art three-set.

Wu [12] proposed improving image scrambling and encryption effect in traditional two-dimensional discrete Arnold transform. The authors used the classical discrete standard map and embedded the nonlinear expressions of output results of one congruence equation for classical two-dimensional discrete Arnold transform into the input item of the other congruence equation for two-dimensional discrete Arnold transform. However, the proposed transform no longer has the quasi-affine invariance properties in the existing two-dimensional discrete Arnold transform, but it is still a reversible mapping with periodic properties.

Bajard et al. [13] used the RNS algorithm for a Closest Vector Problem (CVP) solution. This application is predominantly effective in some base classes of lattices. The method provides a complete round-off period of RNS without costly conversion to an alternative system of positional numbers, for instance, the Mixed Radix Conversion Method (MRC). An improved Cox-Rower structure is used, which is adapted to the algorithm proposed. The core alterations are in the Rower part, which has the flexibility to employ a single multiplier. These consents release two out of three Rower unit multipliers by re-using the equivalent one with an overhead of three extra sets per internal lessening. An overview of the viability of execution within FPGA is as well specified in the paper. At the end of the study, it was shown that RNS could be used to implement lattices with hardware. The authors applied an edge error of 25% to the maximum design occurrence, and about 20s was required to calculate a near-lattice vector in dimension l=64 that can be executed in FPGA.

Irani et al. [14] scrambled encryption process using Chaotic Coupled Sine Map. The authors' designed a methodology to increase the security of the key-space relative to the basic maps, such as the Logistic map and Sine map. A dynamic algorithm based on the size of blocks was used in the scrambling process to increase flexibility. Experimental result shows efficiency in terms of security and visual quality.

The use of three-moduli set for the encryption scheme was used by Reddy and Karumuri [15]. The proposed scheme was built on three modules set {2^n - 1, 2^n, 2^n +1}, which is efficient, requires little hardware, and the active span of the residue number system has not been reduced. It also promises high speed, reduces field, decreases the conversion from residue number system (RNS) to binary to internal delays. As a result, the reverse converter eliminates the multiplicative inverse calculation, and extensive integration implementations for image processing, such as digital image filtering, are done at low power. The outcome of the RNS picture encoder is in small-word length and arranged in some encrypted order. A Residue-Binary Converter (decoder) is applied to restore the plain image. The proposed scheme was simulated on an image with a matrix test method. The intruder who breaks into the network does not know the moduli set is in parallel computation and the encrypted bitstream order. The scheme can extend to any picture type against the top-known state-of-the-art.

Singh et al. [16], proposed using Arnold transform to provide additional security through a random selection of blocks via sharable keys. The technique obtained the YCbCr color model of an RGB image using the superpixel on only the Y color component. Additionally, the acquired labeled image of the superpixel is partitioned into 8 X 8 blocks and categorized as homogeneous and heterogeneous blocks. Based on the categorization, DCT and CA were applied to embed the confidential data in the Cb and Cr color components.

Belazi et al. [17] implemented image encryption with the aid of substitution boxes (S–boxes) that were used to generate chaotic structures and linear fractional transformation (LFT). Here, block permutation, substitution, and diffusion with uncertainty and diffusion were used for the encryption scheme. The authors constructed the S-boxes using both a chaotic map and an LFT. The scheme is used to encrypt necessary bits. The estimated constants of the LWT incidence provide delicate evidence.

Noshadian et al. [18] suggested the image encryption technique to solve security issues through pictures. In the first step, the authors applied the image for the confusion method to get a chaos-based function with the help of a logistic map, and diffusion was implemented by a shuffling algorithm called KNUTH shuffling algorithm. The authors used the algorithm to speed up the optimization technique, which results in the lowest co-relationship between the highest entropy.

Kumar et al. [19] postulated a new cheat immune picture encoding approach. The encoding of the picture will be unsuccessful once an individual intermediary attempts to change the encoded data. The original picture is split into three parts in the encoding process, and the decoding takes.

The reviewed literature establishes that security is not high enough as an independent cryptosystem because of its periodicity [9]. Additional diffusion operations are also essential to diffuse the pixel values to achieve greater security. Additionally, to improve the security of image scrambling methods, most implementations add sophisticated algorithms without a significant improvement [20].

Furthermore, the studies that have used RNS for improving image scrambling have used moduli sets that have limited the efficiency of the scrambling algorithm [1], [2]. This study aims to demonstrate the feasibility of a three-moduli set {2n, 2n+1+1, 2n+1-1} on the

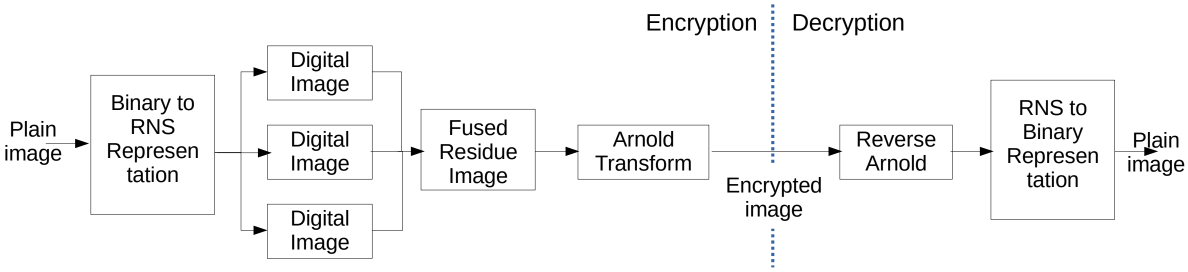

Figure 1. Image encryption and decryption framework

Improved Arnold Transform. RNS is an accurate, successful, and efficient image encryption/decryption scheme. The resulting software development will ensure adequate security because the module array is not exposed to an intruder breaking into the network. The built-in decoder would successfully decrypt the sequence of parallel computed encrypted images. Another primary objective is to build a VLSI implementation scheme for high-speed and low-power image processing, such as digital image transformation and filtering.

II. Research Methods

Shortcomings of the standard Arnold transform is that the four modified constraints or coefficients are set in a character. The image is easily divided once the standard Arnold transform is employed to encode the image with the steady rate of those coefficients. Arnold transform is specified by (1). The x, y denote standard image co-ordinate, x’, y’ modified image co-ordinate, and M the digital image size.

$$\begin{pmatrix} \grave{x} \\ \grave{y} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} mod\ M \tag{1}$$

This study uses the Improved Arnold transform (IAT) as suggested in [21]. The modified equation for IAT is shown in (2). The matrix manipulation of the enhanced Arnold Transform was derived in (3). Additionally, K can be derived from (2) as shown in (4). the K ensures that the transformed values of non-negative when the transform matrix chooses different parameters.

$$\begin{pmatrix} \grave{x} \\ \grave{y} \end{pmatrix} = \begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix}^{-1} \begin{pmatrix} x \\ y \end{pmatrix} + K \begin{pmatrix} N \\ N \end{pmatrix} mod\ N \tag{2}$$

$$a_{00} \times a_{11} + a_{01} \times a_{10} = \mp 1 \tag{3}$$

$$K = max\left[|a_{00}|, |a_{11}|, |a_{10}|, |a_{01}| \right] \tag{4}$$

If the transform matrix chooses separate coefficients, K has a maximum value from the transform matrix coefficient, which guarantees that the altered parameters should not be negative. So, when this matrix is of a non-singular form, the determinant of that matrix is non-zero as shown in (5).

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix}^{-1} \begin{pmatrix} \acute{x} \\ \acute{y} \end{pmatrix} + K \begin{pmatrix} N \\ N \end{pmatrix} modN \tag{5}$$

Different sets of matrix coefficients may be used in improved Arnold transform, whereas traditional Arnold alteration employs fixed matrix coefficients. For IAT, the four matrix coefficients are entirely separate from each other, thereby providing alternatives. For the block position encryption algorithm, the first parameter is set to the unit, giving two choices to choose three coefficients to rest. The scrambling factor used to evaluate the difference between the actual picture and the modified picture should be as outstanding as conceivable. It would be impossible for the attacker to reach the original image content if we could raise the scrambling factor. That is what we suggested with this algorithm.

The encryption process uses Matlab to accept a digital image input and would be converted into an RNS representation of the digital image. Since the algorithm involved is a Three-moduli set algorithm, digital images are encrypted into three different images. The images are fused, and the Arnold transform algorithm is applied to the resulting encrypted image. At the decryption phase, the encrypted image is accepted as input. The anti-Arnold transformation algorithm (Reverse Arnold) is applied to the image. The RNS to the binary algorithm would be used to convert each RNS set back to its original decimal value (original pixel value). Figure 1 shows the image encoder and decoder framework of implementation/simulation of the hybrid image cryptosystem.

The study also performed security analysis tests to test the strength of the proposed hybrid scheme. The histogram of the plain images and the encrypted ones is compared. Mean-squared error (MSE), peak signal-to-noise ratio (PSNR), and correlation are also used to compare the original and modified images. The MSE between two images $g(x,y)$ and $\hat{g}(x,y)$ is expressed in (6). The scale of the pictures is MN. PSNR value in decibels (dB) is given by (7) where S signifies the number of maximum pixels. The correlation coefficient for adjacent pixel pairs must be as (8)-(11) where *x* and *y* reveal adjacent pixel grayscale values in the picture.

$$MSE = 1/MN \sum_{i=0}^{m} \sum_{j=0}^{n} \left(g(m,n) - \tilde{g}(m,n) \right)^2 \tag{6}$$

$$PSNR = -10 \log_{10} MSE/S^2 \tag{7}$$

$$r_{xy} = \frac{cor(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{8}$$

Copyright ©2021, The authors. JTSiskom ISSN: 2338-0403

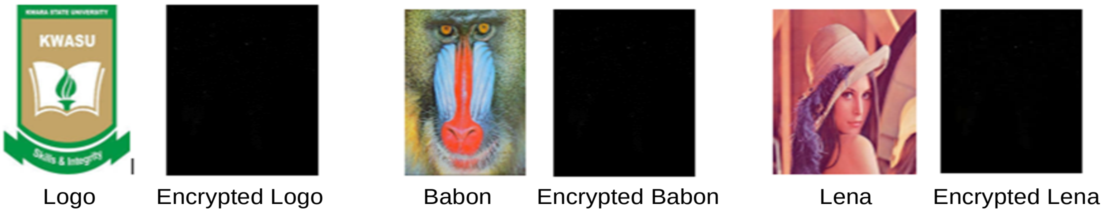

Figure 2. Visual tests after encryption

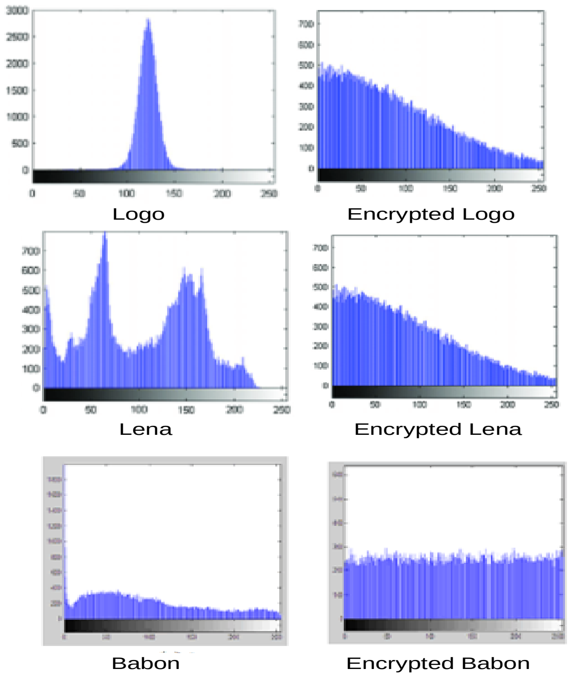

Figure 3. Histograms of the plain and encrypted image

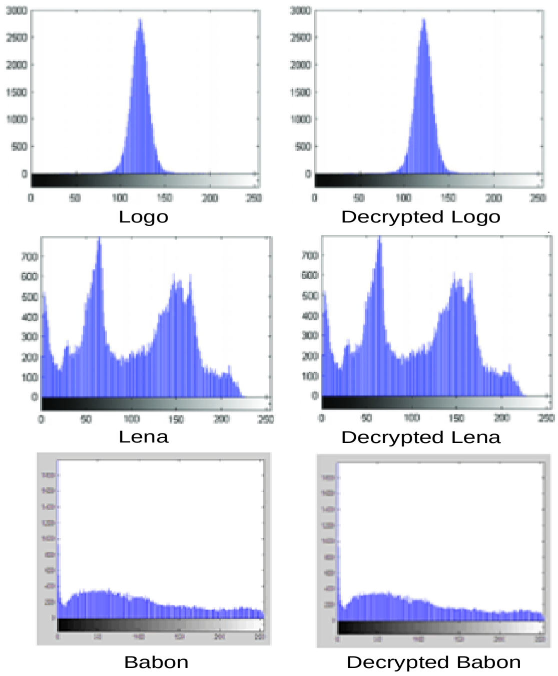

Figure 4. Histograms of the decrypted image

$$cor(x_i)=\frac{1}{N}\sum_{i=1}^{N}\left(x_i-E(x)\left(y_i-E(y)\right)\right) \tag{9}$$

$$D(x)=\frac{1}{N}\sum_{i=1}^{N}\left(x_i-E(x)\right)^2 \tag{10}$$

$$E(x)=\frac{1}{N}\sum_{i=1}^{N}x_i \tag{11}$$

III. Results and Discussion

A detailed investigation of the postulated approach is summarized in this segment. Simulations were performed using Matlab. The analysis includes visual inspection, quality analysis, and description of system metrics results. The quality of the encryption scheme is assessed, including the histogram analysis, the MSE, the peak PSNR, and the correlation analysis coefficient.

In visual inspection, the resulting images are not visually recognizable after encryption (Figure 2). Each image has a 512 x 512 pixels resolution. The histogram of the plain images and their encrypted ones are shown in Figure 3. A cipher image is more protected against statistical attack when its histogram disguises some knowledge about the plain image and fully defers its plain image from the histogram. It is evident that the two histograms are entirely different, and therefore the histogram of the cipher image does not provide any hint about the plain image. The plain images are fully converted from their original state. It indicates that the proposed is protected from histogram attacks since an image histogram shows how the pixels in an image are distributed [22].

Figure 4 displays both original and decrypted pictures in the histogram to check whether the proposed scheme fully recovers plain images. Pixel histograms showed that the distribution of the plain images and their decrypted image equivalents has the same pixel distributions, which ensures that the original images are always retrieved after decryption. It can be concluded from the similarities between the two histograms that the proposed scheme completely recovers plain images.

The comparison of the plain and encrypted images is also expressed in MSE and PSNR. Table 1 shows the MSE and PSNR of the diverse red, green and blue constituents of the Logo, Lena, and Baboon, and their respective encoded images. The high MSE and low PSNR values suggest that the original image data were changed entirely [22]. Therefore, no information about the original image can be retrieved from the encrypted picture without using the decryption program.

Copyright ©2021, The authors. JTSiskom ISSN: 2338-0403

Table 1. The MSE and PSNR of the original and encrypted images

Image	Metric	Red	Green	Blue
Logo	MSE	1.838e+004	1.821e+004	1.817e+004
	PSNR	5.485	5.528	5.536
Lena	MSE	2.051e+004	2.052e+004	2.049e+004
	PSNR	5.012	5.009	5.016
Babon	MSE	1.051e+002	1.052e+004	1.049e+004
	PSNR	4.012	4.009	4.016

Table 2. The adjacent pixels of the encrypted Logo image

Color dimension	Horizontal	Vertical	Diagonal
Red	0.0134	0.0594	0.1132
Green	0.0036	0.0585	0.1068
Blue	0.0155	0.0495	0.0925

A digital image is essential for human vision if neighboring pixels have a high correlation. Disturbing the connection will affect the product's visual identity. One of the criteria for a good encryption scheme is to create encrypted images with significantly low coefficient values for correlation. For this study, the correlation coefficients of randomly selected 1000 pairs of two adjacent pixels of both transparent and encrypted images (horizontal, vertical, and diagonal) are determined. For horizontal, vertical, and diagonal pairs of adjacent pixels, the high correlation coefficient values of 0.9910, 0.9959, and 0.9874 are given by applying the correlation coefficient equation on the grayscale of the test images.

Table 2 shows the correlation coefficient values of the encrypted Logo image generated for the various color dimensions of the image. The result shows that the encrypted image has low coefficient, approximately zero, correlation values between pairs of adjacent pixels. It also showed that in the encrypted images, there were low correlation coefficient values between pairs of adjacent pixels, which also suggests complete encryption of the original images.

The encoding analysis shows the compression ratio of the encrypted images, their encryption time, and used memory. Table 3 shows the reduced size of the encrypted images, which implies a faster transmission rate during their transmission. The required memory for storing the encrypted images is also reduced, as presented in Table 4. The scheme outperforms the schemes in [5], [23] in terms of computational time and its ability to secure non-square images.

The developed scheme could be used for protecting privacy in biometrics, medical imaging systems, and video surveillance systems. In future challenges, the researcher intends to conduct additional statistical analysis and also extend the system to test the applicability of continuous images (video).

IV. Conclusion

This improved Arnold transform algorithm provides better security and no constraint on image width and size. This system encrypts both color and gray images comfortably. Image security is guaranteed because of mixed RNS encryption and the new Arnold scrambling algorithm used to encrypt images with a different histogram of the encrypted images from the plain ones, a high MSE, and a low peak signal-to-noise ratio.

References

[1] D. P. Oyinloye and K. A. Gbolagade, “An improved image scrambling algorithm using {2n -1, 2n, 2n+1},” *Computing and Information Systems Journal, vol. 22, no. 3, pp. 1-7, 2018.*

[2] D. Peter, “Image encryption system based on length three moduli set,” *International Journal of Computer Applications*, vol. 179, no. 42, pp. 12–14, 2018. doi: 10.5120/ijca2018916989

[3] A. N. Babatunde, R. G. Jimoh, and K. A. Gbolagade, “An algorithm for a residue number system based video encryption system,” *Annals Computer Science Series Journal*, vol. XIV, pp. 137–145, 2016.

[4] S. Alhassan and K. A. Gbolagade, “Enhancement of the security of a digital image using the moduli

Table 3. Sizes of plain, encrypted, and decrypted images

Image (png)	Pixel	Size on disk			
		Initial (kB)	Encrypted (kB)	Ratio (%)	Decrypted (kB)
Logo	512 x 512	622	344	55.64	525
Lena	512 x 512	500	280	57.40	403
Baboon	512 x 512	350	202	69.60	322.3

Table 4. Time elapsed and stored memory requirement

Image (png)	Elements count	Time elapsed (s)		Memory requirement (Bytes)		
		Encryption	Decryption	Plain	Encrypted	Decrypted
Logo	262,144	6	6	566,928	221,296	530,000
Lena	262,144	6	6	412,000	196, 208	432,072
Baboon	262,144	5	5	233,516	55,120	134,619

Copyright ©2021, The authors. JTSiskom ISSN: 2338-0403

set,” *International Journal of Advanced Research in Computer Engineering & Technology*, vol. 2, no. 7, pp. 2223–2229, 2013.

[5] A. N. Babatunde, "Methodology for image cryptosystem based on a gray code number system," *Computing and Information Systems Journal*, vol. 23, no. 2, pp. 1-5, 2019.

[6] I. Z. Alhassan and E. D. Ansong, “Enhancing image security during transmission using residue number system and k-shuffle ”, *Earthline Journal of Mathematical Sciences*, vol. 4, no. 2, pp. 399–424, 2020. doi: 10.34198/ejms.4220.399424

[7] E. Y. Baagyere, P. A. N. Agbedemnab, Z. Qin, M. I. Daabo, and Z. Qin, “A multi-layered data encryption and decryption scheme based on genetic algorithm and residual numbers,” *IEEE Access*, vol. 8, pp. 100438–100447, 2020. doi: 10.1109/ACCESS.2020.2997838

[8] M. Boussif, N. Aloui, and A. Cherif, “Securing DICOM images by a new encryption algorithm using Arnold transform and Vigenère cipher,” *IET Image Processing*, vol. 14, no. 6, pp. 1209-1216, 2020. doi: 10.1049/iet-ipr.2019.0042

[9] J. Wu, Z. Liu, J. Wang, L. Hu, and S. Liu, “A compact image encryption system based on Arnold transformation,” *Multimedia Tools and Applications*, vol. 80, pp. 2647–2661, 2021. doi: 10.1007/s11042-020-09828-z

[10] A. Alhassan, I. Saeed, and P. A. Agbedemnab, “The Huffman’s method of secured data encoding and error correction using residue number system (RNS),” *Communications on Applied Electronics*, vol. 2, no. 9, pp. 14–18, 2015. doi: 10.5120/cae2015651844

[11] D. A. Huffman, “A method for the construction of minimum-redundancy codes,” *Resonance*, vol. 11, no. 2, pp. 91–99, 1952. doi: 10.1007/bf02837279

[12] C. M. Wu, “An improved discrete Arnold transform and its application in image scrambling and encryption,” *Acta Physica Sinica*, vol. 63, no. 9, pp. 1–20, 2014. doi: 10.7498/aps.63.090504

[13] J. C. Bajard, J. Eynard, N. Merkiche, and T. Plantard, “RNS arithmetic approach in lattice-based cryptography: accelerating the ‘rounding-off’ core procedure,” in *the 22nd Symposium on Computer Arithmetic*, Lyon, France, Jun. 2015, pp. 113–120. doi: 10.1109/ARITH.2015.30

[14] B. Yosefnezhad Irani, P. Ayubi, F. Amani Jabalkandi, M. Yousefi Valandar, and M. Jafari Barani, “Digital image scrambling based on a new one-dimensional coupled Sine map,” *Nonlinear Dynamics*, vol. 97, no. 4, pp. 2693–2721, 2019. doi: 10.1007/s11071-019-05157-5

[15] 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,” in *International Conference on Communication and Electronics Systems*, Coimbatore, India, Oct. 2016, pp. 1–5. doi: 10.1109/cesys.2016.7889984

[16] P. K. Singh, B. Jana, and K. Datta, “Superpixel based robust reversible data hiding scheme exploiting Arnold transform with DCT and CA,” *Journal of King Saud University - Computer and Information Sciences*, InPress, 2020. doi: 10.1016/j.jksuci.2020.09.014

[17] A. Belazi, A. A. Abd El-Latif, A. V. Diaconu, R. Rhouma, and S. Belghith, “Chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transforms,” *Optics and Laser Engineering*, vol. 88, pp. 37–50, 2017. doi: 10.1016/j.optlaseng.2016.07.010

[18] S. Noshadian, A. Ebrahimzade, and S. J. Kazemitabar, “Optimizing chaos based image encryption,” *Multimedia Tools and Application*, vol. 77, no. 19, pp. 25569–25590, 2018. doi: 10.1007/s11042-018-5807-x

[19] R. Kumar, S. Kini, L. Akshatha, and B. G. Deeksha, “Cheat immune visual cryptographic for secure transmission of images,” *International Journal of Engineering and Advanced Technology*, vol. 8, no. 4, pp. 1175–1181, 2019.

[20] Q. Sun, P. Guan, Y. Qiu, and Y. Xue, “A novel digital image encryption method based on one-dimensional random scrambling,” in *International Conference on Fuzzy Systems and Knowledge Discovery*, Chongqing, China, May 2012, pp. 1669–1672. doi: 10.1109/FSKD.2012.6233963

[21] M. Ding and F. Jing, "Digital image encryption algorithm based on improved Arnold transform," in *International Forum on Information Technology and Applications*, Kunming, China, Jul. 2010, pp. 174-176. doi: 10.1109/IFITA.2010.17

[22] Z. Bashir, T. Rashid, and S. Zafar, “Hyperchaotic dynamical system based image encryption scheme with time-varying delays,” *Pacific Science Review A: Natural Science and Engineering*, vol. 18, no. 3, pp. 254-260, 2016. doi: 10.1016/j.psra.2016.11.003

[23] A. N. Babatunde, E. R. Jimoh, O. Oshodi, and O. A. Alabi, “Performance analysis of gray code number system in image security,” *Jurnal Teknologi dan Sistem Komputer*, vol. 7, no. 4, pp. 141–146, 2019. doi: 10.14710/jtsiskom.7.4.2019.141-146

©2021. This open-access article is distributed under the terms and conditions of the Creative Commons Attribution-ShareAlike 4.0 International License.