IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received April 25, 2020, accepted May 15, 2020, date of publication May 26, 2020, date of current version June 9, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2997838

A Multi-Layered Data Encryption and Decryption Scheme Based on Genetic Algorithm and Residual Numbers

EDWARD YELLAKUOR BAAGYERE[1,2], (Member, IEEE), PETER AWON-NATEMI AGBEDEMNAB[2], (Graduate Student Member, IEEE), ZHEN QIN[1], (Member, IEEE), MOHAMMED IBRAHIM DAABO[2], AND ZHIGUANG QIN[1], (Member, IEEE)

[1]School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu 610054, China
[2]Department of Computer Science, C. K. T. University of Technology and Applied Sciences, Navrongo, Ghana

Corresponding author: Zhiguang Qin (qinzg@uestc.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61672135, and in part by the Sichuan Science Technology Support Plan Program under Grant 2015GZ0095 and Grant 2016JZ0020.

ABSTRACT Over the years, Steganography and Cryptography have been complementary techniques for enforcing security of digital data. The need for the development of robust multi-layered schemes to counter the exponential grow in the power of computing devices that can compromise security is critical in the design and implementation of security systems. Therefore, we propose a new combined steganographic and cryptographic scheme using the operators of genetic algorithm (GA) such selection, crossover and mutation, and some properties of the residue number system (RNS) with an appropriate fusing technique in order to embed encrypted text within images. The proposed scheme was tested using MatLab® R2017b and a CORE™ i7 processor. Simulation results show that the proposed scheme can be deployed at one level with only the stego image containing the encrypted hidden message and at another level where the stego message is further encrypted. An analysis based on standard key metrics such as visual perception and statistical methods on steganalysis and cryptanalysis show that the proposed scheme is robust, is not complex with reduced runtime and will consume less power due to the use of residue numbers when compared to similar existing schemes.

INDEX TERMS Cryptography, data security, genetic algorithm, residual numbers, steganography.

I. INTRODUCTION

Data security has become a critical issue lately as the result of the emergence of digital computing as it is possible for ill-minded persons within the corridors of an organisation or on the line of communication to gain an unauthorised access in some instances or eavesdrop in some other instances on vital information that ought to be kept secret. These intruders have devised sophisticated methods, which include computational, subjective or statistical in order to bypass the existing security systems. For this reason, computer security systems including those using the science of cryptography and steganography have been developed over the years with different number of keys, and levels of encryption/encoding and decryption/decoding. The sole of objective of such schemes is to make it difficult for unintended persons on the line of communication to notice the presence of the information or message and/or if they ever did, then it will be very difficult for such persons to decode its contents. However, the degree of security offered by any of the algorithms for securing data depends to a larger extent on the type and length of the keys utilised, the levels of encoding, the complexities of the algorithms, which can affect the throughput rate as well as the ability of such algorithms to encode smaller messages. If computing power increases linearly every one and half years, [1] then hitherto powerful cryptosystems can easily be broken with the use of powerful computing devices/systems, which implies the need for the continuous research into developing novel multi-layered cryptosystems capable of resisting security breaches of these devices.

The associate editor coordinating the review of this manuscript and approving it for publication was Kim-Kwang Raymond Choo.

Cryptography, which involves encryption and decryption is a science that is as old as communication where transmitted data is scrambled in a way that no person rather than the intended receiver will have knowledge of the its content, [2], [3]. Encryption involves the scrambling of the data into a meaningless form based on a rule that is revertible so that the scrambled information can be decrypted into a form that is meaningful. The rule for encryption and decryption usually involves a key that is either symmetric (e.g. Data Encryption Standard and Advanced Encryption Standard), employed in this paper or asymmetric (e.g. RSA and Elgamal); whilst the key sharing is a challenge in the case of the symmetric cryptography, the computational complexities is very high for the asymmetric cryptography. Thus, the symmetric cryptography is faster and can be employed for smaller organisations, [4], [5]. Whereas, cryptography is concerned with the development and creation of the mathematical algorithms used to encrypt and decrypt messages, cryptanalysis is the science of analysing and breaking encryption schemes. Steganography on the other hand, involves the art of covered or hidden writing, [6]. The process involves concealing a file, message, image, or video within another file, message, image, or video. The fact is that, whiles the intended secret message may not attract attention to itself as an object of scrutiny when concealed, plainly visible encrypted messages, no matter how unbreakable they are, arouse interest for attackers to attempt to break in. Thus, steganography further enforces the security of the secret message by hiding it. Steganography also follows defined rules as that for cryptography.

The Genetic Algorithm (GA) is a search based algorithm using the the mechanics of natural selection and/or natural genetics [7]–[9]. In addition to genetic programming, evolutionary strategies and evolutionary programming, the GA belongs to the family of evolutionary algorithms. Mutation, recombination (crossover) and choice/selection are generally the set of operators. These operators together makes GA a powerful search algorithm, [10] that can be employed in data security in a manner that can be very chaotic and robust. Residue Number System (RNS) uses remainders from conventional number systems such as the decimal or binary number system for representation. The RNS possesses inherently desirable properties such as parallel computation, and carry free arithmetic; these operations are predominantly used in digital signal processing, cryptography, digital communication and image processing [11]–[13]. The RNS is capable of enhancing schemes in these applications by providing fewer hardware resources, improved delays and power profiles in devices that run on batteries. It has not yet found widespread usage because of some few challenges including moduli selection, forward/reverse conversion, and magnitude evaluation. However, these challenges would rather be harnessed into creating a robust scheme for securing data. The decomposition of numbers into residues by sight looks chaotic and thus makes the RNS suitable for encryption purposes.

It is worthy of note that, there exist some works that have employed either the GA or RNS with other methods in some instances, or only the GA or RNS in some other instances in cryptography [14]. Similarly, existing works on steganography includes the one in [15], which proposed a steganographic method for hiding information in 3D images using the RNS with three moduli sets, [16] also proposed an image steganographic scheme to hide image information within another image using RNS. In [17], a scheme was proposed that combined a number of algorithms including AES, a hybrid of Discrete Wavelet Transform and Discrete Cosine Transform watermarking techniques and RNS for image security. A scheme by [18] used the Least Significant Bit technique to hide texts in images. It investigated the multiple approaches of steganography for images, and argued that compression in the frequency domain algorithms are appropriate for effectively hiding text within images without perceptibility. In [19] also, a scheme using Redundant Residue Numbers System (RRNS) codes were employed in steganography. The scheme in [20] discussed the exploration in the use of the operators of GA on a cover medium on text such that hidden data will not be perceptible to any attacker. Before then, a scheme by [21] presented another form of image steganography using GA for RGB (i.e. red, green and blue colour channels) images. Other schemes include those by [22], [23] and [24]. All these presented techniques offer single layer of confusion (encryption) in addition to the GA or RNS layers in some cases or just a single layer. But the degree of any cryptographic/steganographic scheme depends to a larger extent on the length or stages of confusion that an attacker will have to be confronted with, which can easily be achieved when GA is combined with the RNS.

The main contributions of the paper are outlined below:

(i) A multi-layer data encryption and decryption scheme that uses the science of steganography and cryptography is proposed and developed.

(ii) The operators of GA such as selection, crossover and mutation are leveraged on at different levels of encoding and decoding in order to build a secure and robust data encryption and decryption scheme.

(iii) The desirable features of RNS such as residues and parallelism together with a fusing criteria to embed text within images are also employed to further enhance the security, robustness and the throughput of the scheme.

(iv) We experimentally demonstrated the feasibility of the scheme in securing data en route an open channel, e.g. the Internet.

The rest of the paper is organized as follows: Section II presents basic information on the key concepts used in this paper as a way of background information. The Proposed Scheme is presented in Section III – the algorithm, implementation and hardware realisation, and simulation results. The results of the simulation are analysed and discussed in Section IV. A comparison of the proposed scheme vis-à-vis existing similar state-of-art schemes is performed in Section V whiles the paper is concluded in Section VI.

TABLE 1. Notations used in the paper.

SYMBOL	DESCRIPTION
GA	Genetic Algorithm
RNS	Residue Number System
RSA	Rivest, Shamir, and Adelman
RRNS	Redundant Residue Number System
AES	Advanced Encryption Standard
RGB	Red,Green and Blue
DR	Dynamic Range
CRT	Chinese Remainder Theorem
MRC	Mixed Radix Conversion
MRDs	Mixed Radix Digits
$\mathcal{C}$	Ciphertext
$\mathcal{P}$	Plaintext
E	Encryption rule
D	Decryption rule
k	Key for encryption and decryption transformation
GARN	Genetic Algorithm-Residue Numbers Based
ASCII	American Standard Code for Information Interchange
CPA	Carry Propagate Adder
CSA	Carry Save Adder
OPU	Operands Preparation Unit
NPCR	Number of Pixels Change Rate
UACI	Unified Average Changing Intensity
XOR	Exclusive OR
PSNR	Peak Signal to Noise Ratio
MSE	Mean Square Error
R/C	Reverse Converter
N	Number of Moduli

The various notations used in the paper are shown in Table 1.

II. BACKGROUND

The cryptography processes start with an unencrypted data referred to as *plain data* which is *encrypted* into a *cipher data* after which, is then *decrypted* back into accessible plain data. The encryption and decryption are based on the form of cryptography and some kind of key as:

$$\begin{cases} \mathcal{C} = E_k(\mathcal{P}) \\ \mathcal{P} = D_k(\mathcal{C}) \end{cases} \tag{1}$$

where, $\mathcal{P}$ and $\mathcal{C}$ are the plaintext and ciphertext; E and D are the encryption and decryption rules respectively, whilst k is the key used for the encryption and decryption transformations.

Steganography encompasses the process of communication in an obscured and concealed manner, [6], [25]. The general equation of Steganography is given as

$$\begin{aligned} \text{Stego medium} = \text{Cover medium} \\ + \text{Secret message} + \text{Stego key} \end{aligned} \tag{2}$$

Depending on the number of stego keys employed, steganography can be classified as pure, secret key or public key steganography, thus, from no key to more than one key.

In GA, the basic operators are *selection*, *crossover*, and *mutation*. It mimics a natural system for a group of individuals to adapt to a certain environment and an individual being's survival and reproduction are facilitated by removing useless traits and enhancing useful behaviour. It usually starts with a randomly generated set of individuals, then enters a loop once the initial population has been established and by applying a certain number of stochastic operators to the previous population, a new population is generated at the end of each iteration. *Selection* is the mechanism of choosing parents for matting and recombination to build off-springs for the next generation. *Crossover* is the process where two chromosomes mate and a resultant chromosome is formed by taking some attributes of the first chromosome and the rest from the second chromosome. The *mutation* operation is similar to biological mutation and is used to create genetic diversity of a generation from its successive generations, [7], [8].

The RNS is defined by a set of relatively prime moduli $\{m_1, m_2, \ldots, m_N\}$ such that the $\gcd(m_i, m_j) = 1$ for $i \neq j$, where gcd means greatest common divisor of m_i and m_j; and $M = \prod_{i=1}^{n} m_i$, is the Dynamic Range (DR). Any integer, X obtained as $x_i = |X|_{m_i}$, $0 \leq x_i \leq m_i$ is unique in $[0, M-1]$, this is referred to as *Forward Conversion*; and arithmetic operations such as addition, subtraction and multiplication are performed totally in parallel on the independent residues, [26]. *Reverse Conversion* is the reverse order of converting back from RNS notation into conventional notation but is a more complex operation. This has been computed generally, by two techniques: Chinese Remainder Theorem (CRT) and Mixed Radix Conversion (MRC) with modified variants lately in the new CRTs I-III, Core Function Method and Modular Weighed Sum Method, [11].

The the MRC as:

$$X = \sum_{i=2}^{n} \vartheta_i \prod_{j=1}^{i-1} m_j + \vartheta_i \tag{3}$$

where $\vartheta_i, i = 1, 2, \cdots, n$ are the Mixed Radix Digits (MRDs) and computed as follows:

$$\begin{aligned} \vartheta_1 &= x_1 \\ \vartheta_2 &= \left| (x_2 - \vartheta_1) \left| m_1^{-1} \right|_{m_2} \right|_{m_2} \\ \vartheta_3 &= \left| \left((x_3 - \vartheta_1) \left| m_1^{-1} \right|_{m_3} - \vartheta_2 \right) \left| m_2^{-1} \right|_{m_3} \right|_{m_3} \\ &\vdots \\ \vartheta_n &= \left| \left(\cdots \left((x_3 - \vartheta_1) \left| m_1^{-1} \right|_{m_n} - \vartheta_2 \right) 0 \right. \right. \\ &\quad \left. \left. \times \left| m_2^{-1} \right|_{m_n} - \cdots - \vartheta_{n-1} \right) \left| m_{n-1}^{-1} \right|_{m_n} \right|_{m_n} \end{aligned} \tag{4}$$

Each ϑ_i is within the range $0 \leq \vartheta_i \leq m_i$, [27], such that a positive integer, X, in the interval $[0, M)$ can be uniquely represented. The MRC technique makes use of mod-m_i instead of mod-M as in the case of the CRT thereby reducing the complexity of the architecture. It is however, by its nature involving sequential operations that can tend to sometimes limit speed, [28].

III. PROPOSED SCHEME

We present a scheme, which combines cryptography (encryption and decryption) and steganography on digital data for communication using GA and RNS; exploiting all the operators of GA including *selection, crossover and mutation*. The RNS component also includes suitable application of the moduli set $\{2^{n-1}-1, 2^n-1, 2^n\}$, which is well-balanced with efficient properties such as non-derailment of the various channels in order not to impose unnecessary delay on schemes and a conversion to/from conventional representation. Thus, we propose a scheme for image encryption and decryption which will serve as a cover medium for hiding text, encrypted or not.

Algorithm 1 Algorithm for Proposed Scheme

`/* Encoding Process */`

Input: Determine the size and length of inputted image then get all pixel values.

Input: Read plain text, get ASCII/Unicode equivalent values of characters and determine its size.

Result: Compute fusing gap;

$$\zeta = Aveg\left(\frac{\text{Size of image pixels}}{\text{Length of text}}\right)$$

, `// store as Stego Key.`

Result: Randomly replace image pixel values with ASCII/Unicode values based of ζ. `// this gives stego image`

Apply $\mathbf{GARN_{TEXT\_ENCRYPT}}$ on ASCII/Unicode values to obtain cipher text behind the stego image.

Output: Apply $\mathbf{GARN_{IMAGE\_ENCRYPT}}$ to get cipher image with cipher text.

`/* Decoding Process */`

Input: Read cipher image

Result: Apply $\mathbf{GARN_{IMAGE\_DECRYPT}}$ to recover original/hidden text

Output: Using the Stego Key, place back pixels obtained from encryption into original locations to get back original image.

A. ALGORITHM FOR THE PROPOSED SCHEME

The algorithm for this proposed scheme in shown in Algorithm 1. It employs the text encryption and decryption from [14] and that for the image from [29]. This is further elaborated using a flowchart in Fig. 1. The figure shows the various stages of the proposed algorithm. It includes the encryption/encoding unit, which takes in the text to be hidden and the cover image followed by the steganographic process after the stego key (comprising of the fusing gap, length of the text and moduli). $\text{GARN}_{\text{TEXT\_ENCRYPT}}$ and $\text{GARN}_{\text{IMAGE\_ENCRYPT}}$ comprise of the encryption algorithms from [14] and [29] respectively. These will encrypt the hidden text and transform the stego image into a cipher image respectively. The decoding process is the second stage of the algorithm. This is executed in order to recover the origin/hidden text.

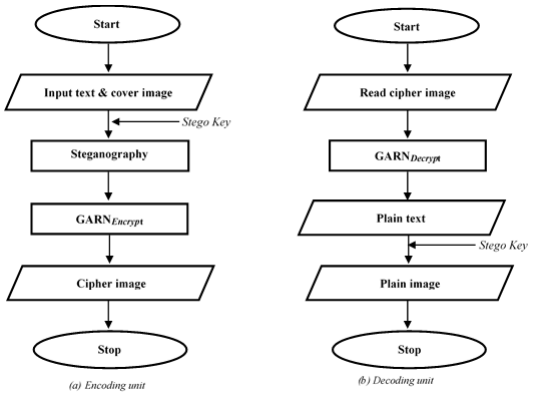

FIGURE 1. Flowchart for the Proposed algorithm.

B. IMPLEMENTATION OF THE PROPOSED SCHEME

We adopt the forward converter from [14] to get the residue set for the chosen moduli set $\{2^{n-1}-1, 2^n-1, 2^n\}$. The residues obtained from this operation will be used both during the steganography and encryption processes. The decoding process involves a reversal of the encoding process but to do the reverse conversion, we employ the MRC method in Equations 3 and 4. The ensuing mathematical manipulation in Equations 5 – 7 and Equations 8 – 15 respectively is a further simplification of this method in order to obtain Equation 20 for an efficient and a simplified architecture.

Theorem 1: Given the moduli set $\{2^{n-1}-1, 2^n-1, 2^n\}$, *let* $m_1 = 2^n$, $m_2 = 2^n - 1$ *and* $m_3 = 2^{n-1} - 1$, *we have*

$$\left|m_1^{-1}\right|_{m_2} = 1 \tag{5}$$

$$\left|m_1^{-1}\right|_{m_3} = -\left(2^{n-2}-1\right) \tag{6}$$

$$\left|m_2^{-1}\right|_{m_3} = 1 \tag{7}$$

Proof: If it can be demonstrated that $|m_i \times m_j|_{m_i} = 1$, then $|m_i|_{m_i} = \left|m_i^{-1}\right|_{m_i}$ is the multiplicative inverse of m_i. Thus for Equation (5),

$$\begin{aligned}\left|(2^n)\times 1\right|_{2^n-1} &= |1\times 1|_{2^n-1}\\ &= |1|_{2^n-1} = 1\end{aligned}$$

Hence 1 is the multiplicative inverse of m_1 with respect to m_2.

Also, for Equation (6),

$$\begin{aligned}\left|2^n(2^{n-2}-1)\times(-1)\right|_{2^{n-1}-1} &= \left|(2^{n-1}-2^n)\times(-1)\right|_{2^{n-1}-1}\\ &= \left|2^n-1\right|_{2^{n-1}-1}\\ &= |1|_{2^{n-1}-1} = 1\end{aligned}$$

Hence $-\left(2^{n-2}-1\right)$ is the multiplicative inverse of m_1 with respect to m_3.

Finally, for Equation (7),

$$\begin{aligned}\left|(2^n-1)\times 1\right|_{2^{n-1}-1} &= |(2)1-1|_{2^{n-1}-1}\\ &= |2-1|_{2^{n-1}-1}\\ &= |1|_{2^{n-1}-1} = 1\end{aligned}$$

Hence 1 is the multiplicative inverse of m_2 with respect to m_3. □

Now from Equation (4), we have

$$\vartheta_1 = x_1 \tag{8}$$

$$\begin{aligned}\vartheta_2 &= |(x_2 - x_1) \times (1)|_{2^n-1} = |x_2 - x_1|_{2^n-1} \\ &= |t_1 + t_2|_{2^n-1} = \left|t_{1,n-1} \cdots t_{1,1} t_{1,0} + t_2\right|_{2^n-1} \\ &= \left|\vartheta_{2,n-1}\vartheta_{2,n-2} \cdots \vartheta_{2,1}\vartheta_{2,0}\right|_{2^n-1}\end{aligned} \tag{9}$$

where,

$$t_1 = |x_2|_{2^n-1} = \left|x_{2,n-1}x_{2,n-2} \cdots x_{2,1}x_{2,0}\right|_{2^n-1} \tag{10}$$

and

$$t_2 = |-x_1|_{2^n-1} = \left|\bar{x}_{1,n-1}\bar{x}_{1,n-2} \cdots \bar{x}_{1,1}\bar{x}_{1,0}\right|_{2^n-1} \tag{11}$$

$$\begin{aligned}\vartheta_3 &= \left|\left((x_3 - x_1) \times (1 - 2^{n-2}) - \vartheta_2\right) \times (1)\right|_{2^{n-1}-1} \\ &= \left|\left(2^{n-2}(x_1 - x_3) - (x_1 - x_3) - \vartheta_2\right)\right|_{2^{n-1}-1} \\ &= |\gamma_1 - \gamma_2 + \gamma_3|_{2^{n-1}-1} \\ &= \left|\gamma_{1,n-2} \cdots \gamma_{1,0} + \bar{\gamma}_{2,n-2} \cdots \bar{\gamma}_{2,0} + \gamma_{3,n-2} \cdots \gamma_{3,0}\right|_{2^{n-1}-1} \\ &= \left|\vartheta_{3,n-2}\vartheta_{3,n-3} \cdots \vartheta_{3,1}\vartheta_{3,0}\right|_{2^{n-1}-1}\end{aligned} \tag{12}$$

where,

$$\begin{aligned}\gamma_2 &= |x_1 - x_3|_{2^{n-1}-1} \\ &= \left|x_{1,n-1}x_{1,n-2} \cdots x_{1,1}x_{1,0} + \bar{x}_{3,n-2}\bar{x}_{3,n-3} \cdots \bar{x}_{3,1}\bar{x}_{3,0}\right|_{2^{n-1}-1} \\ &= \gamma_{2,n-2}\gamma_{2,n-3} \cdots \gamma_{2,1}\gamma_{2,0},\end{aligned} \tag{13}$$

$$\begin{aligned}\gamma_1 &= \left|2^{n-2}\gamma_2\right|_{2^{n-1}-1} \\ &= \left|\gamma_{2,0}\gamma_{2,n-2} \cdots \gamma_{2,1}\right|_{2^{n-1}-1} \\ &= \gamma_{1,n-2}\gamma_{1,n-3} \cdots \gamma_{1,1}\gamma_{1,0}\end{aligned} \tag{14}$$

and

$$\begin{aligned}\gamma_3 &= |-\vartheta_2|_{2^{n-1}-1} = \left|\bar{\vartheta}_{2,n-1}\bar{\vartheta}_{2,n-2} \cdots \bar{\vartheta}_{2,1}\bar{\vartheta}_{2,0}\right|_{2^{n-1}-1} \\ &= \gamma_{3,n-2}\gamma_{3,n-3} \cdots \gamma_{3,1}\gamma_{3,0}\end{aligned} \tag{15}$$

Let $\gamma_{21} = x_{1,n-1}x_{1,n-2} \cdots x_{1,1}x_{1,0}$ and $\gamma_{22} = \bar{x}_{3,n-2}\bar{x}_{3,n-3} \cdots \bar{x}_{3,1}\bar{x}_{3,0}$

But from Equation (3),

$$\begin{aligned}X &= 2^n(2^n - 1)\vartheta_3 + 2^n\vartheta_2 + \vartheta_1 \\ &= 2^{2n}\vartheta_3 - 2^n\vartheta_3 + C \\ &= D + E\end{aligned} \tag{16}$$

where,

$$C = 2^n\vartheta_2 \bowtie \vartheta_1 = C_{2n-1}C_{2n-2} \cdots C_1C_0 \tag{17}$$

$$D = 2^{2n}\vartheta_3 \bowtie C = D_{3n-2}D_{3n-3} \cdots D_1D_0 \tag{18}$$

$$\begin{aligned}E &= -2^n\vartheta_3 = \bar{\vartheta}_{3,n-2}\bar{\vartheta}_{3,n-3} \cdots \bar{\vartheta}_{3,1}\bar{\vartheta}_{3,0}\overbrace{11 \cdots 1}^{n} \\ &= E_{2n-2}E_{2n-3} \cdots E_1E_0\end{aligned} \tag{19}$$

Therefore,

$$\begin{aligned}X &= \underbrace{D_{3n-2}D_{3n-3} \cdots D_1D_0}_{3n-1} + \overbrace{00 \cdots 0}^{n}\underbrace{E_{2n-2}E_{2n-3} \cdots E_1E_0}_{2n-1} \\ &= X_{3n-2}X_{3n-3} \cdots X_1X_0\end{aligned} \tag{20}$$

C. HARDWARE REALISATION

The hardware realisation of the proposed scheme is shown in Fig. 2 depicting the usage of simple adders made of CPAs and CSAs to achieve the backward/reverse conversion process. From the block diagram in Fig. 2, the residue set (x_1, x_2, x_3) is fed into the Operands Preparation Unit (OPU), which prepares and manipulates the parameters in Equations (8), (10), (11) and (13) for appropriate routing of the bits. Therefore, the parameters in Equations (10) and (11) are summed up using CPA2 in order to obtain the second MRD and at the same time, the result in Equation (13) is achieved by using CPA1, which is summed together with Equations (14) and (15) using CSA1. The save (s_1) and carry (c_1) from the summation in CSA1 are further computed using CPA3 to obtain the third MRD, ϑ_3 in Equation (12). Equations (17) and (18) are obtained by a concatenation process requiring no hardware, and finally the results of Equations (18) and (19) are computed using CPA4 in order to get the binary number X as in Equation (20).

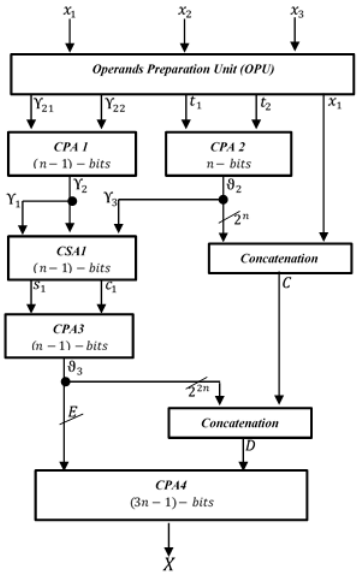

FIGURE 2. Block Diagram of reverse conversion process for proposed scheme.

The area complexity of this architecture is $(7n-4)_{\Delta FA}$ comprising of three $(n-1)$-bits full adders (i.e. CPA1, CSA1 and CPA3), an n-bit full adder and a $(3n-1)$-bit full adder. Regarding the speed of the reverse converter, it is observed however, that it will impose a total delay of $(5n-1)_{\Delta FA}$ because CPA1 and CPA2 will compute at the same time resulting in an imposition of n-bits, CSA1 is unity plus the delays imposed by CPA3 and CPA4.

These three Proposed Schemes were simulated using MatLab® R2017b and a CORE™i7 Processor Laptop.

D. SIMULATION

The proposed scheme was tested on different data types of images and texts of variant sizes. The simulated results show that it is possible to transmit an image with the hidden and encrypted message/text in a manner that does not give any clues to the existence of a hidden text by visual inspection. Also, it can further conceal an encrypted message within a stego image that is also encrypted thus, combining steganography with cryptography to achieve data security. It is worthy of note that, the scheme works for both grayscale and colour images of variant dimensions as well as any form of character making up text. Fig. 3 contains the MatLab® simulation systems for the encoding and decoding in (a) and (b) respectively. In Fig. 3 (a), the 'Encrypt_GN_Image TextMixer' is the steganographic stage which inputs are the plain text and plain image as well a value for n to indicate the number of bits for the chosen moduli set; the stego key and the length of the text are stored at this stage. These parameters will be passed on after fusing the text values with image pixel values onto the three stages of $\text{GARN}_{\text{TEXT\_Encrypt}}$ and $\text{GARN}_{\text{IMAGE\_Encrypt}}$ for the scrambling of both the text and pixels values respectively, after which, they are recombined to get the cipher image with a hidden cipher text as the final output.

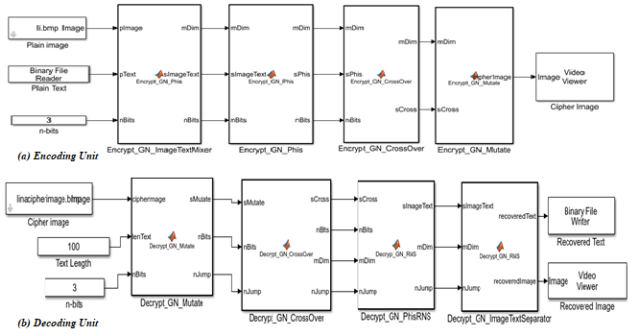

FIGURE 3. MALAB® simulation units.

The decoding unit in Fig. 3 (b) on the other hand, will take in as inputs the cipher image, the text length and the number of bits through the various blocks of processing – $\text{GARN}_{\text{IMAGE\_Decrypt}}$ stages of mutation, crossover and reverse conversion in 'Decrypt_GN_Mutate', 'Decrypt_GN_Crossover' and 'Decrypt_GN_PhisRNS' respectively, and then through a text separator, ''Decrypt_GN_ImageTextSeparator' to recover both the covered text and image.

Figures 4 – 7 are samples of the experiments performed using the proposed scheme: 'Lena; is a grayscale image with 128×128 dimension shown in Fig. 4. The image 'Peppers' is a colour image with dimension 512×512 as shown in Fig. 6. From the experiments, the 'ImageName_Stego' in (b) of both Fig. 4 and Fig. 6 is a stego image with cipher messages

FIGURE 4. Experiment with Grayscale image "Lena".

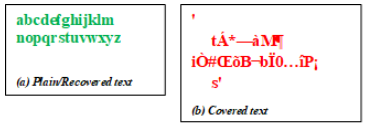

FIGURE 5. Sample text for experiment in Grayscale image "Lena".

FIGURE 6. Experiment with colour image "Peppers".

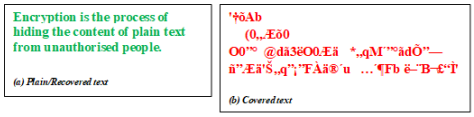

FIGURE 7. Sample text for experiment in colour image.

in (b) of 5 and 7 concealed in it respectively. The plain form of the cipher text is in (a) of Fig. 5 and Fig. 7 respectively. The stego images look similar to the original images in both cases by visual inspection. A further processing of the stego images results in the encrypted image in (c) of Fig. 4 and Fig. 6; here, both the texts and images are encrypted. Every character in the covered texts were recovered without error as well as the encrypted images.

IV. RESULTS AND ANALYSIS OF THE SCHEME

The keys for the steganographic component of the proposed scheme are (i) the fusing gab and (ii) the length of text. We then employ $\text{GARN}_{\text{TEXT}}$ and $\text{GARN}_{\text{IMAGE}}$ respectively to encrypt the text and image. The encrypted text is first concealed in the image before it is encrypted. Therefore, it is possible to deploy the scheme up to the stage of only hiding the text in an image which is proven to be just similar as the original (further analysis will buttress this point later in subsequent subsections), in this case, it will be only steganography or deploy the full scheme combining the steganography with cryptography; in which case an attacker will have no idea whatsoever that the encrypted image has a text hidden in it that is even in a cipher form.

A. VISUAL TESTING

Before the interest of an attacker can be aroused, he/she should have noticed some form of difference in two images of the same content. From the simulation results

in Figures 4 and 6, we notice that at the stage of only applying the proposed steganographic component of the scheme, nobody can tell that the two images are not the same, meanwhile, the stego image has a hidden encrypted text. However, the encrypted images look completely different from the original images without any perceptual similarities.

B. NUMBER OF PIXELS CHANGE RATE AND UNIFIED AVERAGE CHANGING INTENSITY ANALYSIS

The point of perceptual similarity or otherwise of the stego and encrypted images to the original image is strengthened when the Number of Pixels Change Rate (NPCR) and the Unified Average Changing Intensity (UACI) analysis are performed. These statistical measurements as shown in Table 2 show that the stego images look virtually the same as the original images, but the encrypted images look completely different from the original. This is because, higher values indicate that the pixels positions have been randomly altered significantly in the case of NPCR and almost all pixel gray-scale values of the cipher-images being changed from their values in the plain-images in the case of UACI. The reverse is the case for lower values.

TABLE 2. Difference measure between plain-images and cipher-images.

Image	*NPCR(in %)*	*UACI(in %)*
Lena *(Original vs Stego)*	0.1667	0.0216
Lena *(Original vs Encrypted)*	99.8767	18.1552
Peppers *(Original vs Stego)*	0.0081	2.6927e-04
Peppers *(Original vs Encrypted)*	99.6521	8.4364

C. HISTOGRAM ANALYSIS

Histogram analyses were also performed first, to ascertain the similarities or otherwise of the images and second to prove that the proposed scheme can withstand statistical attacks.

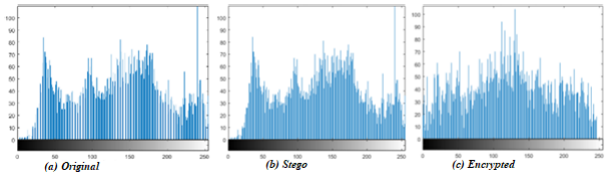

FIGURE 8. Histogram of experimentation with image "Lena".

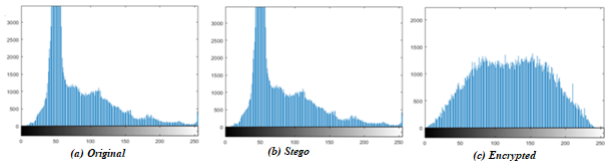

FIGURE 9. Histogram of experimentation with image "Peppers".

From the histograms in Fig. 8 and 9, it is seen that whilst the histograms of the stego images (in (b) of both figures) look very similar to the original/plain images (in (a) of both figures, respectively), the encrypted images (in Figures 8(c) and 9(c)) look completely different. Thus, when the stego image is transmitted, an attacker will find it difficult to notice that a message is hidden in it, but on the other hand, an attacker who gets hold of the encrypted image will have no clue to the original image and for that matter, the hidden text. It therefore suffices to state that, the proposed scheme can withstand both steganographic and cryptographic attacks.

D. CORRELATION COEFFICIENT ANALYSIS

The correlation coefficient analysis is also another very important measure of the perturbation of the pixel values of an image. Strong correlation of adjacent coefficient pixel values imply appeal to the human eye whilst the reverse is the case for very low correlation. In this analysis, we calculated the correlation coefficients of randomly selected 1000 pairs of two adjacent pixels (horizontal, vertical and diagonal) of plain, stego and cipher images. Table 2 shows the respective correlation coefficient values for $n = 3$. From Table 3, it is seen that the adjacent values for the pair of selected pixel values are high (close to one) indicating a very strong correlation for both the original images and the stego images. However, the lower values (close to zero) recorded for the encrypted images indicates a weak correlation among the selected pixels. This reinforces the point that whilst the stego image looks just like the original image for the purpose of deception and concealment, the encrypted images on the other hand look very chaotic even with a concealed message when compared to the original.

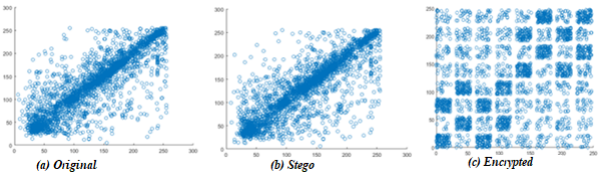

FIGURE 10. Distribution graphs for correlations among the adjacent pixels of image "Lena".

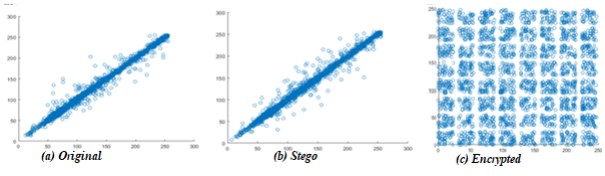

FIGURE 11. Distribution graphs for correlations among the adjacent pixels of image "Peppers".

Figures 10 and 11 depict the correlation distributions of the horizontal adjacent pixels for plain and the corresponding cipher images used for experimentation in this paper. The figures confirm the fact that whilst the adjacent pixels in stego images are strongly correlated, the adjacent pixels in the encrypted images are indeed very weakly correlated.

TABLE 3. Correlation coefficient values of pairs of adjacent pixels, Scheme.

Image	Correlation								
	Plain			*Stego*			*Cipher*		
	Hor	*Vert*	*Diag*	*Hor*	*Vert*	*Diag*	*Hor*	*Vert*	*Diag*
Lena	0.8319	0.9236	0.7814	0.8311	0.9231	0.7807	0.0099	0.0031	0.0002
Peppers	0.9943	0.9903	0.9854	0.9941	0.9902	0.9854	0.0146	0.1110	0.0078

TABLE 4. Execution speed of proposed scheme on different images.

Image/Dimension	*Length of text*	*Encoding time (sec)*	*Decoding time (sec)*
Lena (128×128)	26 char	10.61043	5.91326
Peppers (512×512)	90 char	114.39228	87.56873

TABLE 5. Hardware requirements (Components) of proposed scheme.

S/N	*Component*	*No. of Hardware Units*	*Area-*(Δ_{FA})	*Delay-*(Δ_{FA})
1.	Forward Converter (F/C)	4 Full Adders	$4n-2$	$2n$
2.	Fusing Operations	Nil	Nil	Nil
3.	Crossover	1 XOR	1	1
4.	Mutation	Nil	Nil	Nil
5.	Reverse Converter (R/C)	5 Full Adders	$7n-4$	$5n-1$
Total		***10 units***	$11n-5$	$7n$

E. SPEED TEST

The speed test measures the execution time (i.e. throughput rate) of the proposed scheme. The complexity of the proposed scheme will also be put to test here since a complex scheme will also take a longer time to execute. The execution time (in seconds) as shown in Table 4 shows that despite the layers of encoding decoding embedded in the proposed algorithm, it does not seem to be complex thus yielding the lower runtimes.

F. HARDWARE REQUIREMENTS

The proposed scheme is made up of a forward conversion component that processes pixel/ASCII values into RNS form, fusing of the text with the image, crossover and mutation operations as well as a reverse conversion process in order to get back their decimal equivalent forms. The forward converted adopted from Scheme I requires four modulo adders – two $(n-1)$-bits and two n-bits adders; the crossover operation requires just a XOR unit; the mutation operation requires no hardware unit; and the Reverse Converter (R/C) requires three $(n-1)$-bits full adders, an n-bit full adder and a $(3n-1)$-bit full adder as shown in Table 5. From Table 5, it is clear that there can be an implementation of the proposed scheme without necessarily employing expensive hardware resources thereby leading to a cheaper scheme.

G. SECURITY ANALYSIS OF THE PROPOSED SCHEME

The proposed scheme combines steganography with cryptography; therefore, any attacker would have to apply tools of steganalysis and cryptanalysis in order to discover the existence of message within the stego image and/or discover the scrambled text or image. Most of these attacks are subjective, which makes use of human eye or statistical methods, where mathematical analysis are performed in order to find statistical differences between the altered and non-altered messages, [19]. From the above analysis outlined in Section IV, it is obvious that it will be nearly impossible to notice differences in the stego and original or similarities in the encrypted and original images using either subjective or statistical methods.

In addition, the use of the RNS and GA will render the proposed scheme as an NP-Hard problem for an attacker to break through without having knowledge of the value of n, the moduli set used, the number of moduli and the order used, as well as the crossover and mutation keys. This is because he/she has a positive infinity $(+\infty)$ times of guessing the value of n, after which he has $2^{M!} \times N$ (N is number of moduli) chance of getting the moduli set used, $N!$ for the order before the modulo operations to get the residues, [30]. The attacker has to continue to obtain the crossover and mutation keys in order to have a complete breakthrough of the proposed scheme at different stages. Thus, the proposed scheme is robust against most steganographic and cryptographic attacks.

TABLE 6. PSNR and MSE comparison of proposed scheme on Stego image.

Scheme	*PSNR (db)*	*MSE*
[22]	44.7836	2.1613
[31]	39.4011	0.7940
Proposed	**13.0036**	**0.3683**

TABLE 7. Performance evaluation of the proposed scheme using encrypted (with covered message) image.

Scheme	*Entropy*	*Correlation coefficients*			*NPCR*	*UCAI*	*Time (ms)*
		Vertical	*Horizontal*	*Diagonal*			
[32]	7.9997	0.0007	0.0017	0.0001	0.997103	0.336297	3284
[33]	7.9994	-0.0022	0.0007	0.0149	0.996427	0.335615	28.3
Proposed	**7.9987**	**0.0099**	**0.0031**	**0.0002**	**99.8767**	**0.18155**	**591.26**

V. COMPARISON OF THE PERFORMANCE OF THE PROPOSED SCHEME WITH EXISTING SCHEMES ON KEY PARAMETERS

We compare the performance of the proposed scheme to existing schemes on key parameters; first, on a stego image and second, on an encrypted image using 128 × 128 'Lena' image. Table 6 is a measurement of the amount of noise or alteration that is introduced into or made to the stego image. Here, the scheme is compared with schemes by [22] and [31] whose works are on steganography without encryption. From the table, it is clear that the Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE) values of the proposed scheme are low. Thus, it is an indication that minimal errors were introduced into the stego image using the proposed scheme when compared to the other existing schemes. Table 7 compares the performance of the proposed scheme to other existing schemes by [32] and [33], this time, on the encrypted image. The encrypted image by the proposed scheme contains a hidden message which is unknown to an adversary. The scheme by [33] employed a single layer of encryption during the encryption process; this explains the low runtime values for this scheme. However, the scheme by [32] does a DNA masking in addition to the use of GA operators, this is done in a two-layered manner. But from Table 7, whiles the proposed scheme is a three-layered scheme with a steganographic layer, and encrypts every bit stream of the plain image, its execution time is still faster than that of (Enayatifar *et al.*, 2014). This attest to the fact that the complexity of the proposed algorithm is low and very suitable for images with high intensity. The NPCR and UCAI values of the proposed scheme clearly also show the total scrambling of the pixel values into the cipher image.

VI. CONCLUSION

An end-to-end steganographic and cryptographic scheme is presented using genetic algorithm and residue number system on text and images for digital communication. The proposed scheme is an image encryption and decryption scheme where the encrypted image served as cover medium for hiding text (also encrypted). The proposed scheme can be deployed partly for only the steganography part where a stego image containing a hidden text can be transmitted or deployed fully to include the encryption of the stego image. At this point, the content and existence of the message is hidden from unauthorised persons. A simulation was done using the proposed algorithm and an analysis of the results show that the proposed scheme can withstand various forms of steganalysis and cryptanalysis that include subjective and statistical methods. An evaluation of the proposed scheme in terms standard metrics for steganography and cryptography vis-à-vis existing schemes showed that it performs favourably better. In future, this work can be scaled up to include other forms of digital data such as audio and video. An error correcting scheme using the redundant residue numbers system to detect and correct errors during the encryption and decryption processes is also very crucial in order that the full potentials of the RNS can be utilised for this purpose.

REFERENCES

[1] A. K. Lenstra and E. R. Verheul, "Selecting cryptographic key sizes," *J. Cryptol.*, vol. 14, no. 4, pp. 255–293, Sep. 2001. [Online]. Available: https://infoscience.epfl.ch/record/164526/files/NPDF-22.pdf

[2] H. D. Phaneendra, "Identity-based cryptography and comparison with traditional public key encryption: A survey," *Int. J. Comput. Sci. Inf. Technol.*, vol. 5, no. 4, pp. 5521–5525, 2014.

[3] D. Stinson, *Cryptography: Theory and Practice*. Boca Raton, FL, USA: CRC Press, 1995.

[4] G. C. Kessler. (Apr. 26, 2020). *An Overview of Cryptography*. Garykessler.net. Accessed: May 26, 2020. [Online]. Available: https://www.garykessler.net/library/crypto.html

[5] A. Kumar and M. K. Ghose, "Overview of information security using genetic algorithm and chaos," *Inf. Secur. J., Global Perspective*, vol. 18, no. 6, pp. 306–315, Dec. 2009.

[6] G. C. Kessler. (Feb. 2015). *Steganography for the Computer Forensics Examiner*. Garykessler.net. Accessed: May 26, 2020. [Online]. Available: https://www.garykessler.net/library/fsc_stego.html

[7] D. E. Goldberg, *Genetic Algorithm in Search Optimization and Machine Learning*. Boston, MA, USA: Addison-Wesley, 1989.

[8] C. W. Wu and N. F. Rulkov, "Studying chaos via 1-D maps-a tutorial," *IEEE Trans. Circuits Syst. I. Fundam. Theory Appl.*, vol. 40, no. 10, pp. 707–721, Oct. 1993.

[9] R. Afarin and S. Mozaffari, "Image encryption using genetic algorithm," in *Proc. 8th Iranian Conf. Mach. Vis. Image Process. (MVIP)*, Sep. 2013, pp. 441–445.

[10] V. A. Cicirello and S. F. Smith, *Modeling GA Performance for Control Parameter Optimization*. Las Vegas, Nevada, USA: Morgan Kaufmann, 2000.

[11] P. A. Agbedemnab and E. K. Bankas, "A novel RNS overflow detection and correction algorithm for the moduli set $\{2^n - 1, 2^n, 2^n + 1\}$," *Int. J. Comput. Appl.*, vol. 110, no. 16, pp. 30–34, Jan. 2015. [Online]. Available: http://research.ijcaonline.org/volume110/number16/pxc3900925.pdf

[12] M. I. Daabo and K. A. Gbolagade, "RNS overflow detection scheme for the Moduli set $\{M - 1, M\}$," *J. Comput.*, vol. 4, no. 8, pp. 39–44, 2012.

[13] L. Sousa and P. Martins, "Sign detection and number comparison on RNS augumented 3-moduli sets $\{2^n - 1, 2^{n+x}, 2^n + 1\}$," *Circuits, Syst., Signal Process.*, vol. 36, no. 3, pp. 1224–1246, Mar. 2017.

[14] P. A.-N. Agbedemnab, E. Y. Baagyere, and M. I. Daabo, "A novel text encryption and decryption scheme using the genetic algorithm and residual numbers," in *Proc. 4th Int. Conf. Internet, Cyber Secur. Inf. Syst.*, vol. 12, K. Njenga, Ed. London, U.K.: EasyChair, 2019, pp. 20–31. [Online]. Available: https://easychair.org/publications/paper/kzG7

[15] A. Azizifard, M. Qermezkon, and R. Farshidi, "Information steganography within 3D images using residue number system," Islamic Azad Univ., Dezfoul, Iran, Tech. Rep., Feb. 2015.

[16] R. Chowdhury, N. Dey, and S. Ghosh, "Design and implementation of RNS model based steganographic technique for secured transmission," *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 2, no. 3, pp. 132–136, 2012.

[17] P. P. Bhangale, A. Gawad, J. Maurya, and R. S. Raje, "Image security using AES and RNS with reversible watermarking," *Int. J. Innov. Sci., Eng. Technol.*, vol. 4, no. 5, pp. 350–355, 2017.
[18] R. Tavoli, M. Bakhshi, and F. Salehian, "A new method for text hiding in the image by using LSB," *Int. J. Adv. Comput. Sci. Appl.*, vol. 7, no. 4, pp. 126–132, 2016.
[19] B. M. Amine and S. El Mamoun, "Introduction to steganography in RRNS based communications," in *Proc. 2nd Int. Conf. Netw., Inf. Syst. Secur.*, 2019, pp. 1–7.
[20] C. K. Mulunda, P. W. Wagacha, and A. O. Adede, "Genetic algorithm based model in text steganography," *Afr. J. Inf. Syst.*, vol. 5, no. 4, pp. 131–144, 2013.
[21] R. J. Essa, N. A. Z. Abdullah, and R. D. Al-dabbagh, "Steganography technique using genetic algorithm," *Iragi J. Sci.*, vol. 59, no. 3A, pp. 1312–1325, 2018.
[22] A. Khamrui and J. K. Mandal, "A genetic algorithm based steganography using discrete cosine transformation (GASDCT)," *Procedia Technol.*, vol. 10, pp. 105–111, Dec. 2013, doi: 10.1016/j.protcy.2013.12.342.
[23] P. Sethi and V. Kapoor, "A proposed novel architecture for information hiding in image steganography by using genetic algorithm and cryptography," *Procedia Comput. Sci.*, vol. 87, pp. 61–66, 2016, doi: 10.1016/j.procs.2016.05.127.
[24] E. Castillo, L. Parrilla, A. Garcia, A. Lloris, and U. Meyer-Baese, "Watermarking strategies for RNS-based system intellectual property protection," in *Proc. IEEE Workshop Signal Process. Syst. Design Implement.*, Oct. 2005, pp. 160–165.
[25] F. L. Bauer, *Decrypted Secrets: Methods Maxims Cryptology*, 3rd ed. New York, NY, USA: Springer-Verlag, 2002.
[26] A. Omondi and B. Premkumar, *Residue Number Systems: Theory and Implementation*, vol. 2. Singapore: World Scientific, 2007. [Online]. Available: http://www.worldscientific.com/worldscibooks/10.1142/p523
[27] M. Hosseinzadeh and K. Kia, "Effective reverse converter for general three moduli set(2^n)-1,(2^n)+1,$(2^{(pn+1)})$-1," *Int. J. Image, Graph. Signal Process.*, vol. 4, no. 9, pp. 37–43, 2012.
[28] K. A. Gbolagade, R. Chaves, L. Sousa, and S. D. Cotofana, "An improved reverse converter for $\{2^n+1-1, 2^n, 2^n-1 moduliset\}$," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, May 2010, pp. 2103–2106.
[29] P. A.-N. Agbedemnab, E. Y. Baagyere, and M. I. Daabo, "A new image encryption and decryption technique using genetic algorithm and residual numbers," in *Proc. IEEE AFRICON*, Accra, Ghana, 2019.
[30] M. Abdallah and A. Skavantzos, "A systematic approach for selecting practical moduli sets for residue number systems," in *Proc. 27th Southeastern Symp. Syst. Theory*, 1995, pp. 445–449.
[31] G. Prema and S. Natarajan, "Steganography using genetic algorithm along with visual cryptography for wireless network application," in *Proc. Int. Conf. Inf. Commun. Embedded Syst. (ICICES)*, Feb. 2013, pp. 727–730.
[32] R. Enayatifar, A. H. Abdullah, and I. F. Isnin, "Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence," *Opt. Lasers Eng.*, vol. 56, pp. 83–93, May 2014, doi: 10.1016/j.optlaseng.2013.12.003.
[33] Y. Wang, K.-W. Wong, X. Liao, and G. Chen, "A new chaos-based fast image encryption algorithm," *Appl. Soft Comput.*, vol. 11, no. 1, pp. 514–522, Jan. 2011.

EDWARD YELLAKUOR BAAGYERE (Member, IEEE) received the B.Sc. degree (Hons.) in computer science from the University for Development Studies (UDS), Tamale, Ghana, in 2006, the M.Phil. degree in computer engineering from the Kwame Nkrumah University of Science and Technology, Kumasi, Ghana, in 2011, and the Ph.D. degree in computer science and technology from the University of Electronic Science and Technology of China, in 2016. He is currently a Senior Lecturer with the Faculty of Mathematical Science, C. K. T. University of Technology and Applied Sciences, Navrongo, Ghana. He teaches with the Department of Computer Science. He is also a Postdoctoral Research Fellow with the School of Information and Software Engineering, University of Electronic Science and Technology of China. His current research interests include machine learning, mobile sensor networks, cryptography, and social networks. He is a member of the International Association of Engineers.

PETER AWON-NATEMI AGBEDEMNAB (Graduate Student Member, IEEE) is currently pursuing the Ph.D. degree in computational mathematics with the University for Development Studies (UDS). He is currently a Lecturer with the Department of Computer Science, C. K. T. University of Technology and Applied Sciences, Navrongo, Ghana. His current research interests include computer arithmetic and architecture, and information security.

ZHEN QIN (Member, IEEE) received the B.Sc. degree in communication engineering from the University of Electronic Science and Technology of China (UESTC), in 2005, the M.Sc. degree in electronic engineering from the Queen Mary University of London, in 2007, and the M.Sc. and Ph.D. degrees in communication and information system from UESTC, in 2008 and 2012, respectively. He is currently an Associate Professor with the School of Information and Software Engineering. His current research interests include network measurement, wireless sensor networks, and mobile social networks.

MOHAMMED IBRAHIM DAABO received the B.Sc. degree in computer science and the M.Sc. and Ph.D. degrees in computational mathematics from the University for Development Studies, Tamale, Ghana. He is currently a Senior Lecturer with the Department of Computer Science, Faculty of Mathematical Sciences, C. K. T. University of Technology and Applied Sciences, Navrongo, Ghana. His current research interests include computer arithmetic, residue number systems, digital logic design, and mathematical modeling.

ZHIGUANG QIN (Member, IEEE) is currently a Professor and the Retired Dean of the School of Information and Software Engineering, University of Electronic Science and Technology of China, where he is also the Director of the Key Laboratory of New Computer Application Technology and the UESTC-IBM Technology Centre. His research interests include computer networking, information security, cryptography, information management, intelligent traffic, electronic commerce, distribution, and middleware.