TEST Engineering & Management

November-December 2019
ISSN: 0193-4120 Page No. 3857 - 3869

An Efficient Hyperchaotic based Image Encryption Model based on DNA Encoding and Bit Scrambling

Swetha. T. N[1], Dr. G.M. Sreerama Reddy[2]
Assistant Professor & Research Scholar - VTU, Dept. of Electronics & Communication Engg.
SJC Institute of Technology, Chickaballapur-562101, Visvesvaraya Technological University , India
E-mail: swethareddy.t.n@gmail.com
Professor & Principal, C Byregowda Institute of Technology, Kolar-563101, Visvesvaraya Technological University, India
E-Mail: sreeramareddy90@gmail.com

Article Info
Volume 81
Page Number: 3857 - 3869
Publication Issue:
November-December 2019

Abstract:
In recent times data security has been given more attention in communication and storing data, especially multimedia data/image. Digital data has been utilized in wide range of application services such as for providing secure access control mechanism, payment gateway service, in providing border security control system, forensic, fraud detection and prevention and so on. Subsequently, wide interest has been shown in providing or enhancing degree of security of multimedia data. Thus, efficient cryptography model for multimedia image is most desired. The traditional cryptography mechanism such as Data encryption standard (DES), advanced encryption standard (AES) and asymmetric encryption method such as RSA are not efficient in meeting digital image security requirement due to their low encryption security efficiency. Recently, deoxyribose nucleic acid (DNA) sequences and hyperchaotic sequence are jointly used for building secure and efficient image encryption model. However, the state-of-art model are not efficient (robust) against noise and cropping attack. Since in existingmodel most digits of each pixel are not altered. For enhancing security for encrypting high dimensional images, this work use both hyperchaotic and deoxyribose nucleic acid sequence. Firstly, pseudorandom sequence is generated using hyperchaotic system. This is done to use hyperchaotic sequences for each possible cases of the cryptography process where intensity parameters of a high dimensional images are transformed to a serial binary digit stream. Then, this stream of bits is scrambled using hyperchaotic sequence. Deoxyribose nucleic acid complementation and algebraic function are conducted among the deoxyribose nucleic acid sequences and the hyperchaotic sequences for attaining a dynamic and efficient image encoding outcomes. The experimental outcome shows proposed image encryption model attain superior performance than stat-of-art model in terms of robustness against entropy, statistical, cropping, noise, plain and differential attack.

Article History

Article Received: *5 March 2019*
Revised: *18 May 2019*
Accepted: *24 September 2019*
Publication: *19 December 2019*

Keywords: *Bit-level scrambling, DNA encoding, Hyperchaotic system, Image encryption, bit-level scrambling.*

I. INTRODUCTION

The use of multimedia data such as text, images and videos is massively increasing in different application such as web, military, medicine so on. The secure transmission of data over the web by protecting data from unauthorized users is still a challenging aspect. The popularity of multimedia technology encourages the digital images to perform a huge part as compared to state-of-art textual content, that prerequisite to preserve privacy of subscribers for different applications. Further, cheap availability of bandwidth has let to growth of

November-December 2019
ISSN: 0193-4120 Page No. 3857 - 3869

internet, information and communication technology (ICT), providing data security has been given wide importance. Since it affects security of a country, economy progress, personal and socio-economics wellbeing. Measure must be taken for assuring privacy, integrity, reliability and availability of information resources. Encryption and steganography methods of multimedia data are utmost critical and must be utilized to block malicious activity from illegal admittance. But steganography consumes more redundant information rather than actual data. Cryptography plays an important role to secure the data from unauthorized access. Cryptography is one of the mathematical based techniques used for data security. Different services of the cryptography include integrity, confidentiality and authentication of information. Encryption is one of the basic principal of cryptography; encryption is used to convert the information into unreadable format to protect the information from alteration. Cryptography are of different kinds considering application requirement, algorithm, key size, and amount of keys utilized to perform encoding and decoding process. There are two major different kinds of security or encryption methods, that is, (i) Symmetrical key based encryption methods and (ii) Public key based encryption methods. These are classified based on number of keys used both in encryption and decryption. The traditional symmetrical based cryptography mechanism such as data encryption standards, Feistel, advanced encryption standards, and asymmetrical based encryption method such as RSA, does not meet or suitable for performing cryptography operation on multimedia due to its low security and encryption efficacy [1], [2].Chaotic system is well-known for initial conditions and parameters, pseudorandomness, ergodicity and reproduction [3].Thus, in recent times number of chaotic based multimedia cryptography models has been modelled.

In [4], presented number of chaotic image encryption schemes for encrypting both partial and complete diagnostic multimedia data. In [5], presented a multimedia data arbitrariness quantization utilizing Shannon entropy of confined images patch sets. In [6] presented a cryptography method for encoding RGB data with correlated chaos and mixed bit-permutation. Associated chaotic sequences is used to fully utilize chaotic maps and heterogeneous bit-permutation is used to enhance permutation efficiency and reduce cost. In [7], presented a 2-D modulation map by combining both diffusion and confusion operations. Transformation of Chaos shift was presented in some model to resourcefully modify pixel position of a multimedia images. In [8], proposed a multimedia image encoding model for enhancing encoding speed using row and column switching operation. In [9], proposed an image encoding model based on true random number and knight's travel path. In [10], using quaternary coding presented an image encoding technique. They used quaternary coding to segment a multimedia image into set of segment (they considered four sub-segment). Thus, the cipher data cannot be reconstructed without possessing all segments (i.e., the image can be reconstructed post obtaining all sub-segments).

DNA based encryption approach have been proposed in recent times because of low energy dissipation, superior parallelization, and huge storage it offers. In [11], presented a steganography approach using Deoxyribose nucleic acid complement and Play fair cipher rules. In [12], conducted extensive analysis on RGB based image encoding model designed using chaos map and DNA encoding. They showed that their model could not be cracked by using 4 corresponding cipher data's and chosen plain data's. In [13], proposed a hybrid design for encrypting image using DNA encoding and 2-D chaotic sequence. In [14], presented a model for encrypting gray images using DNA complementary rules and chaos system. The main and least important segments in every patches is encoded using various techniques. In [15], a robust image encryption model using logistic chaotic maps

and DNA encoding is designed. The input multimedia data is first encoded using deoxyribose nucleic acid encoding method. Post that a mask is constructed using one dimension chaos sequence map. Deoxyribose nucleic acid complementary and Deoxyribose nucleic acid addition was used. In [16] presented acryptography method for encrypting multimedia data utilizing chaos sequences and Deoxyribose nucleic acid sequences operations. In [16], firstly they used pseudorandom sequences for mixing the plain multimedia data. Secondly, Deoxyribose nucleic acid encoding rules is applied for constructing Deoxyribose nucleic acid matrix. Then, permutation operation of row and column of Deoxyribose nucleic acid matrix are performed. In [16], presented an image encryption model adopting chaotic maps and DNA addition. The DNA sequence matrix is segmented into equal size of multiple blocks. Then, DNA addition process is performed on these blocks. Along with that DNA complementary process was also applied in their model. In [18], presented cryptography method for performing encryption on multimedia image using dynamic deoxyribonucleic acid encoding technology and Feistel network and, using "permutation–diffusion–scrambling" structure. In [19], proposed image encryption model using bit-level permutation, pixel level permutation, and deoxyribonucleic acid encoding. Experiment outcome shows the state-of-art model can fight against known statistical attacks (SA), plain text attack (PTA), strong plaintext sensitivity (SPS), and differential attacks (DA). However, these model are not efficient (robust) against noise and cropping attack. Since, in existingmodel most digits of each pixel are not altered.

For overcoming research challenges, this work present an efficient hyperchaotic based image encryption method using deoxyribose nucleic acid encoding and bit scrambling method. The hyperchaotic sequence is used across bit scrambling, deoxyribose nucleic acid complement, deoxyribose nucleic acid addition, and the binary XOR operation for enhancing efficiency and increasing the sensitivity to the input image. The pixel value substitution and pixel position scrambling are met by the proposed bit scrambling method simultaneously. Using proposed bit scrambling, the correlation among the adjacent pixel is very low. The importance of proposed encryption image model is that it can decrypt the image correctly even with presence of noise or cropping attacks. The proposed image encryption model attains superior image encryption performance than existing image encryption models.

The research contribution are described below

- Presenting an encryption where the proposed bit scrambling technique is used in each step of hyperchaotic sequence. Thus, correlation among adjacent pixel is less and aiding superior security performance.
- The proposed model can allow decryption of image efficiently even with presence of noise.
- Proposed model attain superior performance considering information entropy (IE), correlation coefficient (CC), histogram (H), UACL, and NPCR when compared with state-of-art models [10], [18], [19], [22], [26], [27], [28], [29], [30], and [31]. Thus, it is efficient against various types of attacks for example entropy, statistical, cropping, noise, plain and differential attack.

The manuscript is articulated as described: Section I, provide introduction of image encryption using hyperchaotic system and DNA encoding. Further, highlights research problem, issues and challenges in presenting secure image encryption. Section II describes about the various state-of-art method presented to provide secure image encryption using hyperchaotic system, DNA encoding, pixel scrambling and bit scrambling. In section III the proposed an efficient hyperchaotic based image efficient encryption method using deoxyribose nucleic acid and bit scrambling method. Experiment result and analysis is discussed in

November-December 2019
ISSN: 0193-4120 Page No. 3857 - 3869

section IV. Lastly, the conclusion with future research direction of work is discussed.

II. LITTERATURE SURVEY

This section conduct extensive survey of various existing model for provisioning security to information (images) shared over internet. In [4], showed it is very important to provision security to digital medical information (image) from forgery and fraud as they are communicated over internet. Further, to reduce congestion due to bulky nature of medical images, new method have been employed while maintaining security feature aspects. Partial encryption is one widely used encryption model which selectively perform encryption on huge medical image. In other case for performing diagnosis the entire medical is encrypted. Here they presented a hybrid security model using chaotic sequence and deoxyribonucleic acid. The hybrid security model is adaptive in nature for performing encryption on both partial and entire medical image. For generating efficient arbitrary key to perform encryption on color multimedia image they used multiple chaotic map sequences. The hybrid security model is composed of three stage such as permutation, encoding, and diffusion. In each of these stages, the rule set selection depends on key sequences generated by the combined chaotic maps. Experiment outcome shows their model can resist against brute force attack, differential attack and statistical attack. In [24], presented an image encryption model namely Beta chaotic map. The Beta chaos maps is used for carrying out diffusion and confusion and of multimedia data. Then, these encryption model is again used for multiple secret sharing. The state-of-art multiple secret sharing scheme used XOR and Chinese remainder theorem for converting secret image into set of shared images. The existing model yielded good outcome when secret haring is even. However, when secret haring is odd it has some limitation. In [1], they overcome these problems by using three multiple secret sharing scheme. Firstly, by performing *k* image encryption. Secondly, by incorporating as added arbitrary images. Lastly, by utilizing two varied masking coefficient. Experiment outcome shows their model improves the secureness of multiple secret sharing scheme.

In [25], presented an image encryption and transmission model using double-chaotic sequences map. The double-chaotic map is composed of map lattice chaotic sequences and coupled with optical chaos map. Here, they used matching chaotic sequence map from root laser with two optical responses. The two slave laser (S1 and S2) can obtains identical chaotic sequences for transmitting image. Along with, it is used construct the main part of encryption operation. Further, 128 bit key size is used to construct the original parameter of double-chaotic method for deciding which DNA complementary rules to be used. Thus, the key used here is hypersensitive for performing encryption and decryption operation. Further, they used chaos masking for modulating and demodulating optical message. The outcome attained by them show their model has capability to fight against different attack types for example entropy attacks, statistical attacks, brute force attack (BFA), and differential attacks. In [20], presented an encryption model using hyperchaotic system. They used Ikeda system which is an infinite dimensional chaotic based image encryption method. Thus, can offer dynamic resistances against intruder task. Further, they showed state-of-art method was exposed to chosen plaintext attack. For enhancing security of state-of-art encryption method they presented two method. Firstly, permutation operation is performed on plain image using chaotic map sequence prior to vector segmentation. Thus, aiding in protecting the size of the preliminary sub-vector from being illegitimately exposed by chosen the plaintext attack. Secondly, for resisting against differential attack, two times the crossover diffusion operation is carried out at the completion of encryption operation.

In [18], presented a security model using dynamic deoxyribonucleic acid encoding and Feistel network.

November-December 2019
ISSN: 0193-4120 Page No. 3857 - 3869

The security model is designed using permutation–diffusion–scrambling structure. Firstly, for initializing parametric of hyperchaotic system, the hash parameter of plain multimedia is computed. Then, the image pixel is replaced by constructing Hill cipher matrix using generated chaos sequence. Secondly, the Deoxyribose nucleic acid sequence function are utilized as the Feistel network operation F. The Deoxyribose nucleic acid sequence reference is utilized as the key K. Post that, the multimedia pixel parameter distribution realization are done using Feistel cipher. Lastly, additional distribution is done using ciphertext feedback information. Then, using the cipher text confusion and distribution of iteration of chaos scrambled deoxyribose nucleic acid encoding and Feistel cipher transformation deoxyribose nucleic acid decoding makes the cipher increases randomness. Thus, aid in resisting to attacks and guarantees more security for encoded data. Their model can efficiently encrypt the image and provide superior security features, such as large key space, strong plaintext sensitivity, and excellent ciphertext statistical properties. In [19], presented an image encryption model using deoxyribose nucleic acid encoding, bit level permutation and pixel level permutation. Firstly, they constructed a chaotic sequence using five dimensional (5-D) hyperchaotic system. Post completion of sequence generation, bit and pixel level scrambling are done plain images to permute them. Further, pseudorandom sequence are generated for enhancing security. DNA complementary, encoding and XOR operation rules are used to enhance safety (secureness) of cryptography mechanism. The result obtained by them shows, they can resist against statistical, known plain text and differential attacks. Thus, it provides enough secureness and are suitable for practical application requirement.

From extensive survey carried out it can be seen using deoxyribose nucleic acid sequence and hyperchaotic sequence for performing encryption on image aid security performance. The existing encryption model for image using both hyperchaotic sequence and DNA sequences are able to fight against different attack types for example brute force attack, differential attack, entropy attacks and statistical attack. However, no prior work can resist against cropping attack. This is due correlation among the adjacent pixel is very high. Thus, the bit and pixel scrambling technique is not efficient. Thus, there is requirement to develop a new image encryption model that overcomes the above mentioned research problem. This paper present such security model in next section below namely, an efficient hyperchaotic based image encryption model based on deoxyribose nucleic acid encoding and Bit scrambling method.

III. AN EFFICIENT HYPERCHAOTIC BASED IMAGE ENCRYPTION MODEL USING DEOXYRIBOSE NUCLEIC ACID ENCODING AND BIT SCRAMBLING METHOD

This section present an efficient encryption model using both hyperchaotic sequence and DNA sequences. Firstly, the system model for attaining efficient image encryption is presented. Then, DNA encoding and binarization method adopted for encrypting sequence is described. Then, the model to perform encryption on high dimensional images is given. Further, the proposed bit scrambling method is described. Lastly, the proposed encryption model step is given. The architecture of proposed efficient hyperchaotic based image encryption model using deoxyribose nucleic acid encoding and bit scrambling methods.

November-December 2019
ISSN: 0193-4120 Page No. 3857 - 3869

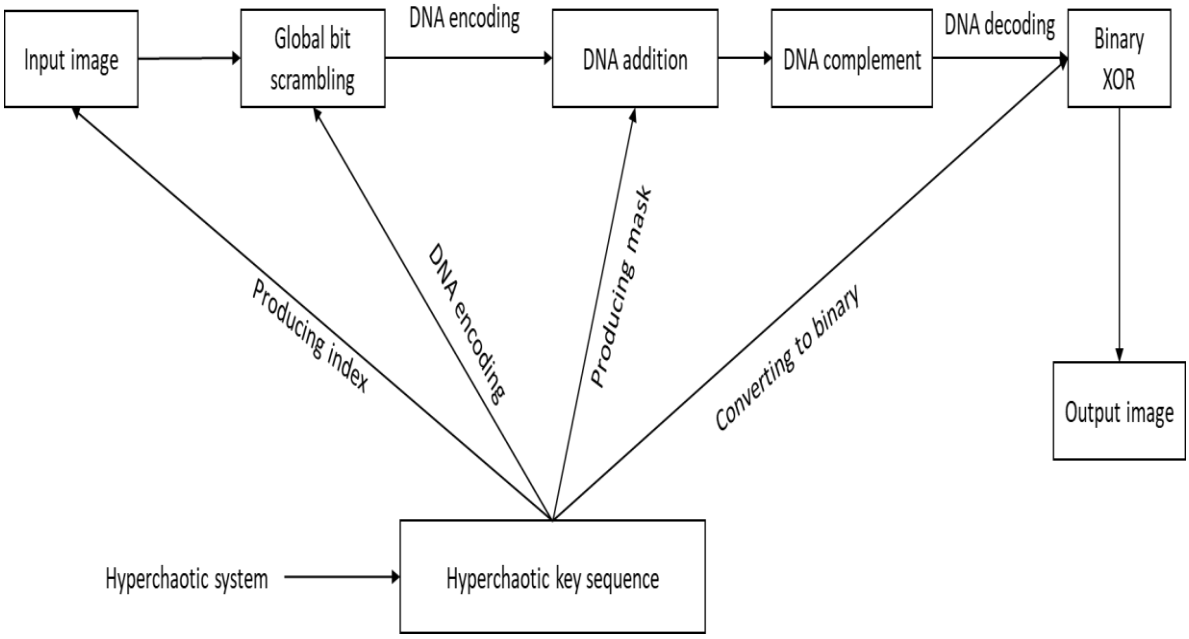


Figure 1: Architecture of proposed efficient hyperchaotic based image encryption model based on DNA encoding and bit scrambling methods.

A. *System model*

Hyperchaos system is generally modelled using chaos system. The major difference among them are hyperchaotic based system have minimum of at least 2 or higher Lyapunov exponent [20]. Further, hyperchaotic system poses more dynamic behavior and they exist in high-dimensional non-linear system. Along with, the uncertainty and arbitrariness are superiorly improved in hyperchaotic based system. However, chaotic based system attain higher efficiency and is simpler. Thus, the key size is smaller with less system complexity. As a result, offers lower security protection. However, hyperchaotic system has more state variables. Thus, a high-dimensional (HD) chaos sequences method poses lager key size and its non-linear characteristics is unpredictable and complex. Thus, the hyperchaotic system can be described or established using non-linear equation as follows

$$\begin{cases} Y_1 = \omega(y_2 - y_1) + \varphi_1 y_4, \\ Y_2 = \delta y_2 - y_1 y_3 + \varphi_2 y_4, \\ Y_3 = -\mu y_3 + y_1 y_2 + \varphi_3 y_4, \\ Y_3 = -\gamma y_1, \end{cases} \quad (1)$$

where ω, δ, μ, γ, φ_1, φ_2, and φ_3 are the present hyperchaotic behavior (control parameters) of the system.

B. *DNA encoding and binarization*

Deoxyribose nucleic acid sequences are constructed adenine (A), Cytosine (C), Guanine (G), Thymine (T) using nucleic acid bases. The adenine and thymine are complement to each other. Similarly, ‘G’ and ‘C’ are complementary to each other. Since we use two-bit binary variable (i.e., ‘0’ and ‘1’) to depict a DNA base which is also complementary to each other. This work uses rules that satisfy Watson-Crick rule [18], [19], [21] which is composed of 8 rules as shown in Table 1 and 2. Further, DNA computing such as subtraction, addition and XOR operation are carried using old-fashioned binary operation as shown in Table, 3,4, and 5, respectively.

Table 1: Encoding/DNA coding rule set

Rule	1	2	3	4	5	6	7	8
00	A	A	C	G	C	G	T	T
01	C	G	A	A	T	T	C	G
10	G	C	T	T	A	A	G	C
11	T	T	G	C	G	C	A	A

November-December 2019
ISSN: 0193-4120 Page No. 3857 - 3869

Table 2: Encoding rule set

Rule	1	2	3	4	5	6	7	8
A	00	00	01	10	01	10	11	11
C	01	10	00	00	11	11	01	10
G	10	01	11	11	00	00	10	01
T	11	11	10	01	10	01	00	00

Table 3: Deoxyribose nucleic acid sequence subtraction function

---	A	C	G	T
A	A	T	G	C
C	C	A	T	G
G	G	C	A	T
T	T	G	C	A

Table 4: Deoxyribose nucleic acid sequences addition function

+++	A	C	G	T
A	A	C	G	T
C	C	G	T	A
G	G	T	A	C
T	T	A	C	G

Table 5: Deoxyribose nucleic acid sequence XOR function

XOR	A	C	G	T
A	A	C	G	T
C	C	A	T	G
G	G	T	A	C
T	T	G	C	A

C. *High dimensional image encryption model*

Using hyperchaotic based system aid in providing stronger security for protecting high dimensional images due to pseudo randomness and good statistical properties. The hyperchaotic sequence construction is composed of following steps. Firstly, to enhance security, the hyperchaotic scheme is iterated priory O_0times to remove the adverse effects. Secondly, post completion of iteration O_0times, the model is further iterated for another set of $n * o$ times. This work use k to depict the index of iteration. In each k, four states outcomes $(y_1^k, y_2^k, y_3^k, y_4^k)$ is stored/kept. In each iteration, each state outcome y_j^k is utilized to construct two different key outcomes such as $(t_j^b)^k \in [0,255], (j = 1,2,3,4)$ and $t_j^c \in [0,255]$, respectively. These keys can be computed as follows

$$(t_j^b)^k = mod\left\{\left\lfloor \frac{[|y_j^k| - \lfloor [y_j^k] \rfloor * 10^{15}]}{10^8} \right\rfloor, 256\right\}, \quad j = 1,2,3,4, \tag{2}$$

$$(t_j^b)^k = mod\left(\lfloor mod\{[(|y_j^k| - \lfloor |y_j^k| \rfloor) * 10^{15}], 10^8\} \rfloor, 256\right), \quad j = 1,2,3,4, \tag{3}$$

where$\lfloor . \rfloor$ depicts flooring function, i.e., its rounds the component closer to integer towards negative infinity and $mod(.)$ depicts the modulo function. Then, these keys i.e. (Eq. (2) and (3)) are combined with below equation to be respective vector t^k as follows

$$t^k = \left[(t_1^b)^k, (t_2^b)^k, (t_3^b)^k, (t_4^b)^k, (t_1^c)^k, (t_2^c)^k, (t_3^c)^k\right] \tag{4}$$

Lastly, post completion of all iteration, these sequences are combined with below equation to posses l, as follows

$$l = [t^1, t^2, \dots, t^{n*o}]. \tag{5}$$

One component in l can be represented by$l_j, j \in [1, 8no]$.

D. *Proposed bit scrambling model*

Let consider a high dimensional image Q with intensity outcome ranging from $[0, 255]$possess8 bits. Post that scrambling operation is performed bit by bit on the intensity outcome of high dimensional images. This is done to minimize the correlation

November-December 2019
ISSN: 0193-4120 Page No. 3857 - 3869

among neighbouring pixels. Further, the intensity outcome of every pixelare modified/optimized in proposed bit permutation/scrambling model. This operation infers pixel substitution is met by proposed bit scrambling model at the same instance as follows. Firstly, the intensity outcome of every pixel is stated as binary parameter one-after-other to possess one dimensional binary sequencesc^0. Then, to achieve the index sequencel^y, the hyperchaotic sequence l is organized in ascending order. Secondly, usingl^y, c^0 is scrambled to obtain one dimensional binary sequences as follows

$$c_j^1 = c_{l_1^y}^0, \qquad i \in [1, 8no]. \tag{6}$$

E. High dimensional image encryption methodology

The proposed bit scrambling methods results in complex non-linear association among cipher image and input image, which aid in enhancing security. The proposed encryption model is described as follows. Firstly, let us consider $n * o$ as the size of high dimensional input image Q. Then, bit scrambling is performed on this image Q to possess binary sequencec^1. Secondly, using DNA coding rule, $c^1$is encode to a DNA sequencee^1. Then, addition operation is performed on each component of e^1 to obtain e^2 by

$$\begin{cases} e_1^2 = e_0 + +e_1^1, \\ e_j^2 = e_{j-1}^2 + +e_j^1, \qquad j \in [2, 4no], \end{cases} \tag{7}$$

where$e_0$is a stated initial parameter and ++ depicts the DNA addition function. Thirdly, a sequence l^t is extracted from l as follows

$$l^t = [l_1, l_2, \dots, l_{no}] \tag{8}$$

and then l^t is converted to binary representation c^l. Then, using DNA encoding rule, c^l is encoded toe^l. Post encoding DNA addition is performed among e^2 and e^l in order to possess a sequencee^3. Fourthly, a weight function $f(a)$ is described as follows

$$f(a) = \begin{cases} 0, & 0 \le \frac{a}{255} \le 0.5, \\ 1, & 0.5 < \frac{a}{255} \le 1. \end{cases} \tag{9}$$

A cut sequence of l,$[l_1, l_2, \dots, l_{4no}]$, is transformed to a mask sequence x using Eq. (9). For constructinge^4, $e^3$and the masked sequence x are utilized, i.e., if$x_j = 1$, the respective e_j^3 is optimized to possess e_j^4, otherwise it's kept same and not altered. Thus, the DNA sequence e^4 is obtained. Fifthly, using DNA coding rule, e^4 is decoded to possess a binary sequencec^2. Then, bitwise XOR operation is performed among c^2 and c^l to possess binary sequencec^3. Lastly, c^3 is converted to a cipher image Q. In similar manner to encryption, decryption operation is performed in reverse order. In next experiment analysis is presented for performing image compression. The result attained shows proposed encryption model attain superior performance than existing model which is experimentally proven below.

IV. Experimetal Result And Analysis

This section present experiment evaluation of proposed image encryption model over existing model [18]. The proposed image encryption model is evaluated in terms of histogram, correlation coefficient, information entropy, uniform average changing intensity(UACL), and number of pixel change rate (NPCR). For experiment analysis and executing algorithm Matlab 2017 tool. Further, the standard 256∗256 Lena and Pepper grayscale images is used as the input data for performing encryption.

A. Histogram perforamcne evaluation

The statistical properties of an image shows distribution properties of gray parameters of the input multimedia content to an assured level. Further, the histogram metric is considered to be a significant factor of performing encryption on multimedia data to see if it modifies the statistical distribution (SD) properties of the input multimedia data. The objective of our grayscale encryption methodology is to resist against statistical attack. The table 6 shows the experiment outcome attained by proposed encryption model. Two case study (image) are considered for histogram analysis. From analysis it can be seen the proposed image encryption model can resist against grey scale statistical analysis (SA) in a manner where the

November-December 2019
ISSN: 0193-4120 Page No. 3857 - 3869

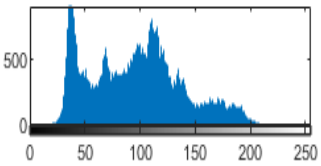
intruder can't decode the input image or gray parameter distribution properties. Since, the proposed encryption model makes grayscale distribution of the encoded input picture element very flat. Moreover, to measure the pixel distribution uniformity of cipher image variance of the histogram is used. More uniformity the pixel distribution property is when variance or closer. Different key size is utilized for performing encryption on same image, the variance of these cipher images is computed using Eq. (10). If the respective cipher text are close, then the cipher image has higher histogram uniformity. The histogram variance is computed as follows:

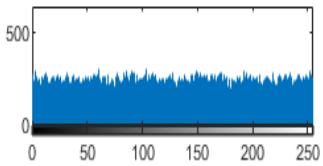
$$V(Z) = \frac{1}{n^2}\sum_{i=0}^{1}\sum_{j=0}^{n-1}\frac{(z_i - z_j)^2}{2} \quad (10)$$

where Z is the histogram parameter vector $Z = \{z_0, z_1, z_2, \ldots, z_{256}\}$of greyscale image, and z_i and z_j are the total pixel size with grey parameters i and j, $n = 256$.

Table 6: Histogram performance evaluation of proposed model

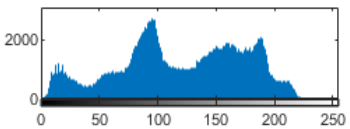
Case 1: Lena

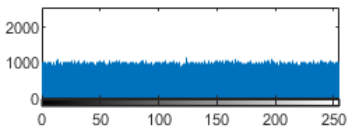



Input Image | Histogram of input image | Cipher image | Histogram of cipher image

Case 2: Pepper

Input Image | Histogram of input image | Cipher image | Histogram of cipher image

B. *Correlation coefficient perforamcne evaluation*

This section present correlation coefficient performance achieved by proposed image encryption method over existing image encryption method. For experiment analysis standard 256∗256 Lena grayscale image is used as input to perform encryption and evaluate correlation coefficient performance. The correlation coefficientr_x performance among two neighbouring/adjacent pixel $(x, y)$is computed as follow

$$r_x = \frac{cov(x,y)}{\sqrt{D(x)D(y)}} \quad (11)$$

where$cov(x, y)$ is computed as follows

$$cov(x,y) = \frac{1}{N}\sum_{i}^{N}\big(y_i - E(x)\big)\big(y_i - E(y)\big), \quad (12)$$

$E(x)$is computed as follows

$$E(x) = \frac{1}{N}\sum_{i}^{N} x_i, \quad (13)$$

And $D(x)$ is computed as follows

November-December 2019
ISSN: 0193-4120 Page No. 3857 - 3869

$$D(x) = \frac{1}{N}\sum_{i}^{N}\left(x_i - E(x)\right)^2. \quad (14)$$

The correlation coefficient among input original and encrypted image is computed using Eq. (11) and performance attained by proposed image encryption method over existing image encryption method is shown in Table 5. From experiment analysis it can be seen proposed model attain superior correlation performance when compared with existing model.

Table 7: Correlation coefficient

Algorithm	Horizontal	Vertical	Diagonal
Existing model [18]	0.0039	-0.0314	0.0158
Existing model [22]	0.0163	-0.0029	0.0309
Existing model [26]	0.152	0.014	0.0218
Existing model [19]	0.0068	-0.0054	0.001
Existing model [27]	0.0211	0.0412	-0.0016
Existing model [28]	0.0082	-0.0107	0.0022
Proposed model	0.0018	-0.00298	0.0018

C. *Information entopy perforamcne evaluation*

Information entropy (IE) metric is a measurement to compute the degree of insecurity which is computed using following equation (15)

$$H(m) = -\sum_{k=0}^{2^N-1} p(m_i)\log_2 p(m_i)$$

where $p(m_i)$depicts the probability that the data$m_i$appears. For the grayscale images, the data$m_i$is composed of256 states, the minimum and maximum value is 0 and 255, respectively. Using Eq. (15), the entropy is completely random in nature, when entropy size is 8, which shows higher the entropy of cipher image is more secure the encryption model used. The entropy performance of cryptographic image obtained by performing encryption on Lena and Pepper image using proposed and various state-of-art encryption method is presented in Table 8. From result, it is inferred that the proposed image encryption method achieve superior performance than most of the existing image encryption method From result, [18] attained an average entropy performance of 7.978, [19] attained an average entropy performance of 7.9967, [29] attained an average entropy performance of 7.7895, [30] attained an average entropy performance of 7.99615, and proposed encryption model attained an average entropy performance of 7.9978. Thus, shows the information leakage (IL) of cipher image are significantly less. Thus, proves the security of proposed image encryption model.

Table 8: Information entropy performance evaluation

Algorithm	Entropy performance for Lena	Entropy performance for Pepper
Existing model [18]	7.978	-
Existing model [19]	7.9967	7.9967
Existing model [29]	7.7893	7.7897
Existing model [30]	7.9962	7.9961
Proposed model	7.9964	7.9992

D. *Differential attack perforamcne evaluation*

This section present differential attack performance achieved by proposed image encryption method over existing image encryption method. A DA is to perform a trivial modification to the input

November-December 2019
ISSN: 0193-4120 Page No. 3857 - 3869

multimedia picture elements. Post that, perform encryption on input multimedia picture elements and alter the multimedia picture elements. The correlation among the input multimedia picture elements and the encrypted multimedia picture elements is attained by correlating the two encrypted multimedia picture elements. The uniform average changing intensity (UACI) and number of pixel change rate (NPCR) are used to measure whether the encryption method resisted the differential attack [23]. The UACL is computed as follows

$$UACL = \frac{1}{W * H}\left[\sum_{i,j}\frac{|C(i,j) - C^{'}(i,j)|}{255}\right] * 100 \quad (16)$$

Similarly, the NPCR is computed as follows

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W * H} * 100 \quad (17)$$

where$H$ and W depicts width and length of the grayscale image, respectively, C and $C^{'}$ depicts the cipher picture elements with respect to 2inputpicture elements with a single-pixel variation. For the pixel (i,j), if$C(i,j) = C^{'}(i,j)$, then $D(i,j)$ is equal to one, otherwise, $D(i,j)$ is equal to zero.The UACL and NPCR performance is computed using Eq. (16) and Eq. (17), respectively and the performance attained by proposed encryption model over existing encryption method is presented in Table 8. From experiment analysis it can be inferred that the proposed image encryption method can resist to plaintext and differential attack when compared with existing model. From result attained it can be seen proposed model attain similar (slightly lesser) UACL performance when compared with existing model. However, in term of NPCR proposed encryption model attain superior performance when compared with existing model.

Table 9: UACL performance

Algorithm	UACL	NPCR
Existing model [18]	99.6185	28.7344
Existing model [19]	99.61	33.46
Existing model [10]	99.57	33.45
Existing model [31]	99.54	33.43
Proposed model	99.23	49.7571

E. Result and discussion

From overall result attained shows, the proposed model attain superior performance considering histogram, CC, IE, UACL, and NPCR. The proposed image encryption model makes grayscale distribution of the encoded input multimedia picture elements is significantly flat when compared with existing model [18], [19]. Thus, can resist against statistical attack. The proposed image encryption model attain superior correlation coefficient performance when compared with exiting image encryption model [18], [19]. This is due to the proposed bit scrambling technique is used in each step of hyperchaotic sequence. Thus, correlation among adjacent pixel is less and aiding superior security performance. Further, the proposed image encryption model attain similar UACL performance and superior NPCR performance when compared with exiting image encryption model [18], [19]. Thus, the proposed image encryption model can resist against cropping, noise, plain and differential attack. The overall result attain shows robustness of proposed image encryption model.

V. CONCLUSION

This work presented an efficient hyperchaotic based image efficient encryption method using deoxyribose nucleic acid and bit scrambling method. This work used a four dimensional hyperchaotic sequence to construct the pseudorandom sequence. Pixel scrambling and substitution was realized concurrently using proposed bit scrambling. DNA addition function is used rather than performing binary operation in order to increase efficiency and cipher randomness (unpredictability) of proposed image encryption model. Experiment are conducted to evaluate performance of proposed image encryption model over existing. The outcome shows

November-December 2019
ISSN: 0193-4120 Page No. 3857 - 3869

proposed model attain superior histogram, correlation coefficient, information entropy, UACL, and NPCR performance when compared with existing image encryption model. Thus, the proposed model can resist different attack such differential attack, statistical attack, noise, cropping attack and linear attack more efficiently due to larger key size, using proposed bit scrambling method and the nonlinearity of the DNA algebraic process. Further, proposed image security model can allow efficient decryption even with presence of noise. Therefore it has good security and is reliable or potential for practical application. Future work we will conduct experiment analysis considering varied images and other security performance metric. Along with, would present an enhanced hyperchaotic sequence based security provisioning for encrypting image that is adaptive to external noise interference.

REFERENCES

[1] Z. Zhu, W. Zhang, K. W. Wong, and H. Yu, "A chaos-based symmetric image encryption scheme using a bit-level permutation," Inf. Sci., vol. 181, no. 6, pp. 1171–1186, 2011.

[2] L. Y. Zhang et al., "On the security of a class of diffusion mechanisms for image encryption," IEEE Trans. Cybern., vol. 48, no. 4, pp. 1–13, Apr. 2017.

[3] D. Ravichandran, P. Praveenkumar, J. B. Balaguru Rayappan, and R. Amirtharaja, "Chaos based crossover andmutation for securing DICOM image," Comput. Biol. Med., vol. 72, pp. 170–184, 2016.

[4] D. Ravichandran, P. Praveenkumar, J. B. B. Rayappan, and R. Amirtharajan, "DNA chaos blend to secure medicalprivacy," IEEE Trans. Nanobiosci., vol. 16, no. 8, pp. 850–858, Dec. 2017.

[5] Y. Wu, Y. Zhou, G. Saveriades, S. Agaian, J. P. Noonan, and P. Natarajan, "Local Shannon entropy measure withstatistical tests for image randomness," Inf. Sci., vol. 222, pp. 323–342, 2013.

[6] X. Wang and H. Zhang, "A color image encryption with heterogeneous bit-permutation and correlated chaos," Opt.Commun., vol. 342, pp. 51–60, 2015.

[7] W. Liu, K. Sun, and C. Zhu, "A fast image encryption algorithm based on chaotic map," Opt. Lasers Eng., vol. 84,pp. 26–36, 2016.

[8] X. Wang, Q. Wang, and Y. Zhang, "A fast image algorithm based on rows and columns switch," Nonlinear Dyn., vol. 79,no. 2, pp. 1141–1149, 2015.

[9] T. Sivakumar and R. Venkatesan, "A new image encryption method based on knight's travel path and true randomnumber," J. Inf. Sci. Eng., vol. 32, no. 1, pp. 133–152, 2016.

[10] H. Niu, C. Zhou, B. Wang, X. Zheng, and S. Zhou, "Splicing model and hyper–chaotic system for image encryption," J.Elect. Eng., vol. 67, no. 2, pp. 78–86, 2016.

[11] A. Khalifa and A. Atito, "High-capacity DNA-based steganography," in Proc. 8th Int. Conf. Informat. Syst., 2012, pp. BIO-76–BIO-80.

[12] Y. Liu, J. Tang, and T. Xie, "Cryptanalyzing a RGB image encryption algorithm based on DNA encoding and chaosmap," Opt. Laser Technol., vol. 60, no. 2, pp. 111–115, 2014.

[13] X. Wang, Y. Zhang, and Y. Zhao, "A novel image encryption scheme based on 2-D logistic map and DNA sequenceoperations," Nonlinear Dyn., vol. 82, no. 3, pp. 1269–1280, 2015.

[14] A. Rehman, X. Liao, A. Kulsoom, and S. A. Abbas, "Selective encryption for gray images based on chaos and DNAcomplementary rules," Multimedia Tools Appl., vol. 74, no. 13, pp. 4655–4677, 2015.

[15] A. Jain and N. Rajpal, "A robust image encryption algorithm resistant to attacks using DNA and chaotic logistic maps,"Multimedia Tools Appl., vol. 75, no. 10, pp. 5455–5472, 2016.

[16] X. Wang, Y. Zhang, and X. Bao, "A novel chaotic image encryption scheme using DNA sequence operations," Opt. Lasers Eng., vol. 73, pp. 53–61, 2015.

[17] Q. Zhang, L. Guo, and X. Wei, "Image encryption using DNA addition combining with

November-December 2019
ISSN: 0193-4120 Page No. 3857 - 3869

chaotic maps," Math. Comput. Model., vol. 52, no. 11/12, pp. 2028–2035, 2010.

[18] X. Zhang, Z. Zhou and Y. Niu, "An Image Encryption Method Based on the Feistel Network and Dynamic DNA Encoding," in IEEE Photonics Journal, vol. 10, no. 4, pp. 1-14, Aug. 2018, Art no. 3901014. doi: 10.1109/JPHOT.2018.2859257.

[19] S. Sun, "A Novel Hyperchaotic Image Encryption Scheme Based on DNA Encoding, Pixel-Level Scrambling and Bit-Level Scrambling," in IEEE Photonics Journal, vol. 10, no. 2, pp. 1-14, April 2018, Art no. 7201714. doi: 10.1109/JPHOT.2018.2817550.

[20] M. Li, H. Fan, Y. Xiang, Y. Li and Y. Zhang, "Cryptanalysis and improvement of a chaotic image encryption by first-order time-delay system," in IEEE MultiMedia.doi: 10.1109/MMUL.2018.112142439.

[21] S. Sun, "A novel secure image steganography using improved logistic map and DNA techniques," J. Internet Technol., vol. 18, no. 3, pp. 647–652, 2017.

[22] G. Ye, "A block image encryption algorithm based on wave transmission and chaotic systems," Nonlinear Dyn., vol. 75, no. 3, pp. 417–427, 2014.

[23] X. Wang, L. Teng, and X. Qin, "A novel color image encryption algorithm based on chaos," Signal Process., vol. 92, no. 4, pp. 1101–1108, 2012.

[24] J. Guo, D. Riyono and H. Prasetyo, "Improved Beta Chaotic Image Encryption for Multiple Secret Sharing," in IEEE Access, vol. 6, pp. 46297-46321, 2018.

[25] X. Fu, B. Liu, Y. Xie, W. Li and Y. Liu, "Image Encryption-Then-Transmission Using DNA Encryption Algorithm and The Double Chaos," in IEEE Photonics Journal, vol. 10, no. 3, pp. 1-15, Art no. 3900515, 2018.

[26] H. Liu, X. Wang, and A. Kadir, "Image encryption using DNA complementary rule and chaotic maps," Appl. Soft Comput., vol. 12, no. 5, pp. 1457–1466, 2012.

[27] S. Sun, "A novel secure image steganography using improved logistic map and DNA techniques," J. Internet Technol., vol. 18, no. 3, pp. 647–652, 2017.

[28] S. Sun, "Chaotic image encryption scheme using Two-by-two deoxyribonucleic acid complementary rules," Opt. Eng., vol. 56, no. 11, 2017, Art. no. 116117.

[29] L. Xu, Z. Li, J. Li, and W. Hua, "A novel bit-level image encryption algorithm based on chaotic maps," Opt. Lasers Eng., vol. 78, no. 21, pp. 17–25, 2016.

[30] X. Wang, Y. Zhang, and X. Bao, "A novel chaotic image encryption scheme using DNA sequence operations," Opt. Lasers Eng., vol. 73, pp. 53–61, 2015.

[31] M. Brindha and N. A. Gounden, "A chaos based image encryption and lossless compression algorithm using hash table and Chinese remainder theorem," Appl. Soft Comput., vol. 40, pp. 379–390, 2016.

AUTHORS PROFILE

Prof. Swetha T N is presently working as a Assistant Professor in the department of Electronics & Communication Engineering, S.J.C.I.T, Chickballapur, Karnataka, India. She is having 10 years of teaching experience. Her areas of interest are Communication systems, Cryptography & Network security, Information Theory & Coding, Embedded Systems, Protocol Engineering, Image Processing, Digital Logic Design, Wireless communication.

Dr. G M Sreerama Reddy is presently working as a Principal & Professor in the department of Electronics & Communication Engineering, C.B.I.T, Kolar, Karnataka, India. He is having 27 years of teaching experience. His areas of interest are Communication systems, VLSI, Mixed mode VLSI, Information Theory & Coding, Microelectronics, Protocol Engineering, Image Processing, SOC, Verilog and HDL.