International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8, Issue-1C, May 2019

Robust Image Encryption Model using Hyperchaotic System and Deoxyribose Nucleic Acid Sequence

Swetha T N, G M Sreerama Reddy

Abstract— Recently, 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 existing model most digits of each pixel are not altered. For enhancing security for encrypting high dimensional images, this work use both hyperchaotic and DNA sequence. Firstly, pseudorandom sequence is generated using hyperchaotic system. This is done to use hyperchaotic sequence for nearly entire process of the encryption where intensity parameters of a high dimensional image are transformed to a serial binary digit stream. Then, this stream of bits is scrambled using hyperchaotic sequence. DNA complementation and algebraic function are conducted among the DNA and the hyperchaotic sequences to attain efficient and robust image encryption performance. Experimental outcome shows proposed image encryption model attain superior performance than stat-of-art model in terms of robustness against cropping attack and noise.

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

I. INTRODUCTION

Recent growth of internet, information and communication technology, has resulted in paying more attention to information security. Since it affects national and personal security, economy growth, and socio-welfare strength. Measure must be taken to promise the confidentiality, integrity, reliability and availability of information resources. The traditional cryptography mechanism such as Data encryption standard, Feistel, Advanced encryption standard and RSA, do not fulfill or suitable for performing image encryption due to their low encryption efficiency and secureness [1], [2]. Chaotic system is well-known for setting preliminary setup and parameters, pseudo arbitrariness, stochasticity and reproduction [3]. As a result, number of chaotic image encryption models have been modeled in recent times. In [4], presented number of chaotic image encryption schemes for encrypting both partial and complete bio-medical images. In [5], presented an image arbitrariness measure utilizing Shannon entropy over a blocks of image. In [6] presented a color image encryption with correlated chaos and heterogeneous bit-permutation. Correlated chaos is used to fully utilize chaotic maps and heterogeneous bit-permutation is used to enhance permutation efficiency and reduce cost.

Revised Manuscript Received on May 21, 2019.

Prof. Swetha T N, is Assistant Professor department of Electronics & Communication Engineering, S.J.C.I.T

Dr. G M Sreerama Reddy Principal & Pr ofessor in the department of Electronics & Communication Engineering, C.B.I.T, Kolar

In [7], presented a two-dimensional (2-D) modulation map by combining both diffusion and confusion methods. Chaotic shift transformation was presented in some model to efficiently change the position of image pixel. In [8], proposed a fast high dimensional image encoding model which designed using row and column switch. 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 fragment the plain high dimensional image into sub-segment size of four. Thus, the cipher text cannot be created without possession of these sub-segment.

DNA based encryption approach have been proposed in recent times due to high parallelism, storage and low power dissipation it offers. In [11], presented a steganography approach using deoxyribose nucleic acid complementary and Playfair 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 with using sub-segmented corresponding cipher textual high dimensional images and chosen plain high dimensional images. 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 each block is encrypted with diverse methodologies. In [15], a dynamic high dimensional grey scale image encoding model utilizing logistic chaotic maps and deoxyribose nucleic acid. encoding is designed. The input high dimensional image was first encoded using deoxyribose nucleic acid and a mask was constructed with one dimension chaotic system. Deoxyribose nucleic acid complementary and addition was also used. In [16] presented a high dimensional image encoding model utilizing chaotic map and deoxyribose encoding operations. In [16], firstly the plain high dimensional grey scale image is scrambled using pseudoarbitrariness sequences. Secondly, deoxyribose nucleic acid encoding rules is applied for construction of deoxyribose nucleic acid matrix. Then, the row and column of deoxyribose nucleic acid matrix are permutated. 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.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

In [18], presented high dimensional image encoding methodology using Feistel network and dynamic deoxyribonucleic acid encoding technology, using the "permutation–diffusion–scrambling" structure. In [19], presented an image encoding security model using bit and pixel level scrambling, and later deoxyribose nucleic acid encoding operation is performed. Experiment outcome shows the state-of-art model can fight against known plain text attack, strong plaintext sensitivity, differential, and statistical attacks. However, these model are not efficient (robust) against noise and cropping attack. Since, in existing model most digits of each pixel are not altered.

For overcoming research challenges, robust image encryption method by jointly using both DNA sequence and hyperchaotic sequence is proposed in this manuscript. The hyperchaotic system sequence is used in process such as bit scrambling, deoxyribose nucleic acid complement, deoxyribose nucleic acid addition, and the XOR's binary operation. The pixel value substitution and pixel position scrambling are met by the bit scrambling method proposed in this work simultaneously. With bit scrambling, the correlation among the adjacent pixel is very low. For improving/enhancing efficiency the binary XOR, DNA addition, and the DNA complement is used. This superiorly aid proposed approach in increasing the sensitivity to the given high dimensional grey scale images. The importance of presented approach is that it can decrypt the image correctly even with presence of noise or in spite of cropping attacks. The proposed model attains superior image encryption performance than existing models.

Research Contribution are as follows:

- 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 decrypt a image efficiently even with presence of noise.
- Proposed model attain superior performance in terms of correlation coefficient and UACL when compared with state-of-art models [18], [22]. Thus, it is efficient against various kind of attacks such as cropping, noise, plain and differential attack.

The manuscript is structured as follows. In section II, the proposed robust image encryption model using hyperchaotic system and deoxyribose nucleic acid sequence is presented. Experiment evaluation along with result and discussion is presented in section III. Lastly, the conclusion along with future research direction is described.

II. ROBUST IMAGE ENCRYPTION MODEL USING HYPERCHAOTIC SYSTEM AND DEOXYRIBOSE NUCLEIC SEQUENCE

This section present a novel 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.

a) System model:

Hyperchaos system is generally modeled using chaos system. The major difference among them is that the hyperchaotic based method possesses minimum of two 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 chaotic system is high dimensional in nature poses lager key size. Then, these chaotic sequences 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 sequence is self-possessed of nucleic acid bases such as adenine (A), Cytosine (C), Thymine (T), Guanine (G). In this work, we consider 'A' and 'T' are complement of each other. Similarly, 'G' and 'C' are complement of one another. 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 meets Watson-Crick rule [18], [19], [21]. The rule is composed of 8 rules. Further, DNA computing such as subtraction and addition are carried using old-fashioned binary operation.

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_0 times to remove the adverse effects. Secondly, post completion of iteration O_0 times, 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

Retrieval Number: A10250581C19/19©BEIESP
Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

$(t_j^b)^k \in [0,255], (j = 1,2,3,4)$ and $t_j^c \in [0,255]$, respectively. These keys can be computed as follows

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

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

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

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

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 that has a intensity outcome in array of $[0, 255]$ possessing8 bits. The intensity outcome of high dimensional images is then bit by bitscrambled. This is done for minimizing correlation among neighbouring pixel. The intensity outcome of every pixels is affected or altered in proposed bit scrambling model. This process infers the 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, using l^y , c^0 is scrambled to obtain one dimensional binary sequences as follows

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

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

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

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.

III. EXPERIMENT ANALYSIS

This section discusses experiment analysis of proposed image encryption model over existing model [18]. The proposed high dimensional image encryption model is evaluated in terms of correlation coefficient (CC) and uniform average changing intensity (UACL). For experiment analysis and executing algorithm Matlab 2017 tool. Further, the standard 256∗256 Lena grayscale image is selected as the high dimensional image for performing encryption.

a) Correlation coefficient performance evaluation:

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

$$r_x = \frac{cov(x,y)}{\sqrt{D(x)\,D(y)}} \tag{10}$$

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

$$cov(x,y) = \frac{1}{N}\sum_{i}^{N}(y_i - E(x))(y_i - E(y)), \tag{11}$$

$E(x)$ is computed as follows

Retrieval Number: A10250581C19/19©BEIESP
Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

$$E(x) = \frac{1}{N}\sum_{i}^{N} x_i, \tag{12}$$

And $D(x)$ is computed as follows

$$D(x) = \frac{1}{N}\sum_{i}^{N} \left(x_i - E(x)\right)^2. \tag{13}$$

The CC among input original image and the encrypted grayscale image is computed using Eq. (10). The performance attained by proposed method over existing method is depicted in Table I. From experiment analysis, it is seen proposed encryption method attain superior correlation coefficient performance when compared with existing model.

Table 1: Correlation coefficient

Algorithm	Horizontal	Vertical	Diagonal
Existing model [18]	0.0039	-0.0314	0.0158
Existing model [22]	0.0163	-0.0029	0.0309
Proposed model	0.0018	-0.00298	0.0018

b) Differential attack performance evaluation:

This section present differential attack (DA) performance attained by proposed high dimensional image encryption method over existing encryption method. A differential attack is a process to perform trivial modification to the input or source high dimensional images and then perform encryption on source high dimensional image and alter the high dimensional image. The association among the source high dimensional image and the encrypted high dimensional images is attained by associating the two encrypted high dimensional images. The UACL is utilized to quantify whether the encryption technique used resisted DA [23]. The UACL is computed as follows

$$UACL = \frac{1}{W * H}\left[\sum_{i,j}\frac{|C(i,j) - C'(i,j)|}{255}\right] * 100 \tag{14}$$

The UACL performance is computed using Eq. (14) and performance attained by proposed encryption method over existing encryption method is shown in Table II. From experiment analysis it is seen proposed method can resist to plain text and differential attack when compared with existing model.

Table 2: UACL performance

Algorithm	UACL (%)
Existing model [18]	28.73
Proposed model	49.75

IV. CONCLUSION

This work presented an efficient image compression technique using both hyperchaotic sequences and DNA sequences. 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 model. Experiment are conducted to assess performance of proposed security (encryption) method over exiting encryption method. The outcome shows proposed model attain superior correlation coefficient and UACL performance when compared with existing model. Thus, the proposed model can resist different attack due to large key size. Along with, using proposed bit scrambling method and the nonlinearity of the DNA algebraic process, the proposed model can resist noise, cropping attack and linear attack more efficiently. Future, we will conduct experiment analysis considering varied images and other security performance metric.

REFERENCES

1. P 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 and mutation 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 medical privacy," 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 with statistical 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 random number," 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 chaos map," 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 sequence operations," 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 DNA complementary 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

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Retrieval Number: A10250581C19/19©BEIESP

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 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.

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.

.

Retrieval Number: A10250581C19/19©BEIESP
Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication