Turkish Journal of Computer and Mathematics Education Vol.12 No.2 (2021), 2754-2764

Research Article

Secure and Efficient Image Cryptography Technique using Choas and DNA Encoding Methodology

Bahubali Akiwate[1], Latha Parthiban[2]

[1]Visvesvaraya Technological University, Karnataka, India
[2]Pondicherry University, Pondicherry,India
[1]bahubalimakiwate@gmail.com,[2] lathaparthiban@yahoo.com

Article History: Received: 11 January 2021; Accepted: 27 February 2021; Published online: 5 April 2021

Abstract*:* In this era of the digital world, handling digital data with a secure passion is more important. At the height of maximum interest with the attainment of the data confidentiality with the miniature information is the tedious and most challenging concern of the system with the data handling and operating in the real-time environment. With the latest data confidentiality security model, such as image encryption over the communication networks in the distributed data environment, advanced hacking efforts such as cropping attack, brute force, differential, mathematical, and many more need to be addressed. In terms of bit scrambling, the security function plays a vital role in the pixel-based approach with minimum pixels are followed in the current security model for a better correlation with the available pixels with the continued higher runtime complexity. In this research paper, along with the DNA encoding process, an efficient image cryptographic technique is shown with the reduced runtime complexity. The discussion in the article begins with the chaotic sequence EIIS (Efficient Image Information Scrambling) method. Progressed with the DNA (Deoxyribo Nucleic Acid) encoding is done with the data for resistance against different kinds of attacks by considering the suitable parameters from the existing security models.

keywords: Cryptography, Chaotic System, Confusion, Diffusion, DNA Encoding

1. Introduction

In the rapid era of digitization, data handling and its security are the main concerns in the modern world as it is very crucial to secure complex digital data such as image [1,2] from the unauthorized mode of access over the open networks. Current traditional algorithms can encounter few design principles failures with the small key size, with the obvious consequence of unwanted protection. At the outset, a broad range of security techniques to satisfy privacy and data secrecy have been addressing in this article. Encryption and decryption is the combo procedure to be planned and implemented on the input data to enhance data protection. Encryption is the process that will be conducted at the transmitter node with the efficient requirements for effective action to secure the input data image. This process of encryption can be described as asymmetric and symmetric depending on the key usage. In detail, the asymmetric method of encryption is essential to complete the process by using a public key [3] and in pertaining to the SKE (Symmetric Key Encryption) the common key will be exchanged among the transceiver nodes. When compared between both the kind of encryption techniques, SKE criteria is found to be effective, simple, and faster for the macro image size, but the key management is crucial for SKE, as the key among the sender and receiver need to be safely communicated in the communication system defending with the untrusted intruder [7,8,9]. Whereas on the other side of the PKE (Public Key Encryption) will ensure the various issues by addressing a pair of keys such as private and public keys that are securely used for decryption and encryption activities respectively. The main design issue will rely on selection of keys in the PKE system by satisfying the strict mathematical policies, thereby avoiding the need for the key exchange among the processes of cryptography. It additionally can give DS (Digital Signature) administration, which cannot complete using SKE. DS provides information about non-repudiation, authenticity, and data integrity.

As discussed in [10] ECC (Elliptical Curve Cryptography) utilizes smaller parameter contrasted with state-of-art similar methodologies, but with proportional degrees of security. The most widely accepted mathematical computations used in PKE are discrete IF (Integer Factorization) and DL (Discrete Logarithm). These two mathematically difficult computations are utilized in RSA and DSA (Digital Signature Algorithm) cryptography methodologies, respectively. In [10] presented another PKE known as the EC (Elliptic curve) that enhances the productivity of different systems. Cryptanalysts have discovered that they can accomplish computational effectiveness in execution, with a better security level, minimal key size contrasted with different methodologies. There is no sub-exponential method for tackling the DL issue on an appropriately selected EC curve that makes the ECC progressively appealing.

It attracts enormous kinds of attacks including suspicious activities is mentioned in [26]. One solution for minimizing computation overhead (i.e., reduce runtime) to provide image security (i.e., image encryption) using such an algorithm and realize a low-cost security framework is by employing selective encryption. It chooses a segment with the image for carrying out encryption operations [13]. In the case of clinical research data for the

cryptographic behavior in the nearest future, special encryption to function for the decreasing computing time to preserve the security is needed. It has gathered the interest for the research experts to opt for the more encryption schemes selectively for the biomedical image processing that can be employed even for the wireless clinical data in real-time and in decentralized healthcare for the diagnostic data. Recently, several CS (Chaotic Sequence) based image encryption methods are presented [14]. This CS based image security method offers good security features because of chaos properties such as sensitivity to an initial state and pseudo-randomness [4]. However, such CS has certain drawbacks for providing security because of its simplicity and smaller key space [5,15].

ECDH (Elliptic Curve Diffie-Hellman) management methodology used in numerous applications. In recent times, a significant amount of image security methods using ECC have been modeled. The image security approach using the elliptical curve and discrete CS methods are used in [11] where the parameter and keys are gathered using elliptical curve, whereas CS is used for scrambling images. The source image will convert into DNA codes in [12] ECDH and DNA-based image protection methods, then DNA addition is done, and finally, ECDH is used to get the cipher image. Results show that a large key space by their model and is effective against various attacks. In any case, such a method induces higher runtime that takes a more amount of time for the secure image because of high redundancy, the massive size of data, a higher correlation among neighboring pixels [25].

The DNA encoding approach and chaotic systems are used as hybrid forms to concentrate on these complicated issues [16,17]. The clinical data memory is more efficient at the time of storage at the beginning for more processing, the low power implications working for power reduction and concurrent processing operations to enable greater parallelism, thus interpreting the device requirements for the DNA-based encryption system. The approaches in [18,21] for the replacement of DNA and its chaos are summarized. But in the [19] has discussed the protocols for the DNA based encryption systems with the feature-based and block approach. The technical discussion on DNA for the complementary approach is highlighted in the [20] for the data protection operation. Nevertheless, advanced rules are discussed in the PRS (Pseudo-Random Sequence) to result in the necessary plain text [22]. For a highly secure analysis of medical data, the relative challenges are posed in the [6]. Given the article [22] that came with the implementation of the "permutation-diffusion-scrambling" model with the conventional FN (Feistel Network), as an interesting matter of fact [22]. Primarily, the SHA-3 algorithm was made use of to find the hash value for the plaintext image as the preliminary assessment of the CS method. For scrambling pixel positions and obtaining Hill Cipher Matrix (HCM), CS is used.

Secondly, a key, K in FN, is used as the DNA encoding process. FN also assists in understanding the distribution of the image pixel position. Further, three rounds of chaos scrambling DNA encryption-Feistel changes-DNA decoding, making sure the cipher data is much safe and guaranteeing resistance against various attacks. However, it induces higher computational overhead for providing security. Thus, for reducing computational overhead in [27] using chaos sequence security method and DNA encoding method that composed of coupled map lattice chaos model and optical chaotic sequence security model, a new security and communication model pertaining to the medical image data is discussed and similar to the model presented in [28] is applied for providing better security. In an extensive survey [24], the study shows that hybrid design does not guarantee effective security performance. However, the model's safety can suffer significantly in the presence of noise. Because in existing security methodologies, first pixel values will change and scatter (i.e., diffuse) with slight variation within the input image to entire pixels of the cipher image. Second, the method scatters the changed pixel value column by column and row by row using fixed rule sets. Thus, an intruder can get enough information for carrying out a wide range of security attacks. For addressing the research issues in the next section, proposed work secure and efficient image cryptography for future communication environments can resist various kinds of attacks [22,23]. The SEIC (Secure and Efficient Image Cryptography) model presents an efficient pseudorandom substitution method using logistic sine cosine chaotic maps. The substitution depends on the indexes of the matrix are constructed using chaotic sequences. Using these substitutions, utilizing its preceding value and chaotic sequences, the model randomly changes the current pixel value. Finally, the scrambled pixel applies the DNA coding rule, and the encoded image is stored remotely [32, 33].

2. The research contributions

The contribution of the research can be classified broadly into three different categories, namely the following:

- It presents an effective image data scrambling technique with chaotic maps that can withstand multiple security attacks.
- The SEIC-based image ciphering provides a limited correlation between the nearest pixels and can decode the image with or without noise.

- SEIC resulted in an enhancement in parameters such as UACI (Unified Average Changing Intensity), NPCR (Number of Pixels Change Rate), Histogram, Entropy, Runtime, and Processing time performance than existing image security methods.

The articulation of the manuscript can be summarized as different sections, in the first section; it is narrated with the chaotic system for data encryption and DNA encoding. Further, the article is preceded by focusing on research challenges and issues in presenting an efficient security method for protecting the image. The second section presents information required for the proposed secure and efficient image cryptography method for securing images for future generation communication networks. The last section of the paper covered the practical studies with supportive conclusions are drawn with the recommendations for continued efforts.

3. A Secure and Efficient Image Cryptography (SEIC) Technique Using Choas and DNA Encoding Methodology

This section covers the discussion and narration about the SEIC strategy pertaining to the communication networks. This SEIC will make use of different strategies of DNA encoding and its chaos for betterment in the security needs with the combined tradeoff among the computational overheads and its security. Below, Figure 1 shows the architecture of a secure and efficient image cryptography approach in which the input image will first convert to binary form with chaos-based data scrambling followed by DNA encoding. A chaotic based key generated will be then combined to produce a ciphered image. It uses DNA rule sets.

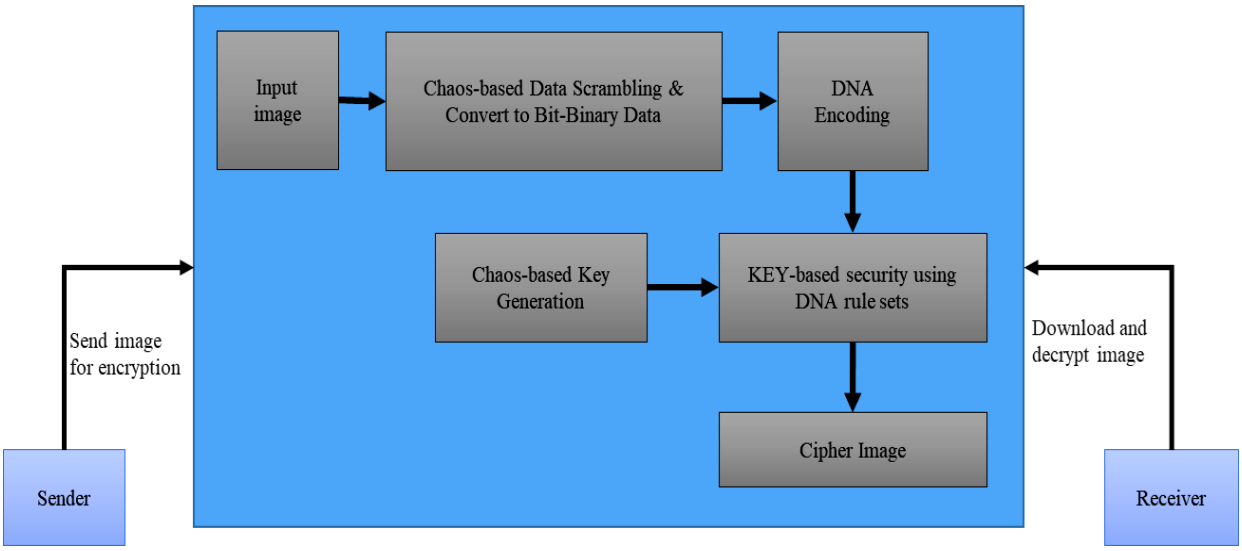


Fig. 1. Proposed architecture of secure and efficient image cryptography approach

2.1 System model and hybrid chaotic sequence generation method

The Chaotic sequence will dominate all the required level of protection for the corresponding data cryptographic mechanism for the encryption process, with the available level of complexity. This subsection is devoted to the discussion of the smart hybrid chaotic sequence's efficient, protected image cryptography. It is introduced with the traditional technique of the confusion and diffusion process to achieve a better level of the encryption standard. As a matter of fact that the key plays a vital role in the process of cryptography which will be denoted as L and it is a set of preliminary states of HCS (Hybrid Chaotic Sequence) to build the CS to gain the operation of EIIS and RSS (Random Sequence Substitution).

The EIIS is shown in a way as needed, is the unique adjacent pixel located in the unique position. Medical image as input is encrypted with the existing rules of the DNA coding style for the efficiently secure cipher image following the successful implementation of the EIIS and for the few iterations to obtain a diffusion process.

The improved chaotic sequence that can overcome problems of existing CS is expressed using following equation (1):

$$y_{j+1} = \cos\left(\pi\left(G\left(b, y_j\right) + H\left(c, y_j\right) + \gamma\right)\right) \tag{1}$$

In the equation (1), it has to be noted that the seed sequences of the CS are $H\left(c, y_j\right)$ and $G\left(b, y_j\right)$.

For the setting, control parameters such as b and c, and shift in the depicting constant in shifting such as γ parameter are used. It is correlated with the trigonometric cosine function for the outcome when the processing of these parameters begins. The function is associated with the secure chaotic sequence for the dynamic seed sets for shuffling or scrambling of the CS. As a preferred outcome, the proposed method uses extremely complex response, increased complexity due to the fact of the parameters such as $G(b, y_j)$ and $H(c, y_j)$ for the complex set of CS with the various combinations of the CS. To show the secureness of proposed SEIC, this work builds three one-dimension (1-D) CS maps using standard Sine ($\mathcal{S}$), Tent ($\mathcal{T}$), and Logistics ($\mathscr{L}$) maps as seed maps which can be mathematically expressed as follows:

$$\mathcal{S}: Y_{j+1} = \mathcal{S}(s, y_j) = s \sin(\pi y_j) \tag{2}$$

If $y_j < 0.5$ then,

$$\mathcal{T}: Y_{j+1} = U(s, y_j) = 2sy_j \tag{3}$$

If $y_j > 0.5$ then,

$$\mathcal{T}: Y_{j+1} = U(s, y_j) = 2s(1 - y_j) \tag{4}$$

$$\mathscr{L}: Y_{j+1} = \mathscr{L}(s, y_j) = 4sy_j(1 - y_j) \tag{5}$$

The parameter s depicts the control factor of the Sine, Tent and Logistic maps, while $s \in [0,1]$. We can obtain three new one dimensional CS by configuring Eq. (2), Eq. (3), Eq. (4) and Eq. (5) of seed maps of Eq. (1).The Sine-Tent-Cosine (STC) CS is built utilizing $\mathcal{S}$ as $G(b, y_j)$ and the $\mathcal{T}$ as $H(c, y_j)$. The Tent-Logistic-Cosine (TLC) CS is built utilizing the $\mathcal{T}$ as $G(b, y_j)$ and the $\mathscr{L}$ as $H(c, y_j)$. Logistic-Sine-Cosine (LSC) CS is built utilizing the $\mathscr{L}$ as $G(b, y_j)$ and the $\mathcal{S}$ as $H(b, y_j)$. This work initialize the parameter b and s as $1 - s$, where s depicts the parameter of the constructed CS.

2.2 Key generation and enhanced image information scrambling method

In the HCS set establishment, a more secure key of encryption of the length 32 bytes each byte of 8 bits resulting in the available key space of 2^{256}. Our key is composed of five elements $L = \{y_0, q_0, e, h, I\}$. The element (y_0, q_0) depicts the original states, e depicts parameter that disturbs its original preliminary state, h depicts the coefficient of preliminary state, and $I = \{I_1, I_2, I_3, I_4\}$ is composed of four coefficients of the disturbing parameter. Each element is composed of 32 bits. The parameter y_0, q_0, e depicts float value within the range [0,1] and every element can be acquired from a 32 bit stream using following equation (6):

$$\mathscr{F}_L = \sum_{j-1}^{32} \mathscr{B}_j * 2^{-j} \tag{6}$$

The coefficients $\mathrm{h}, \mathrm{I}_1, \mathrm{I}_2, \mathrm{I}_3, \mathrm{I}_4$ are integer values which can be computed using the following equation (7):

$$\mathscr{J}_N = \sum_{j-1}^{32} \mathscr{B}_j * 2^{j-1} \tag{7}$$

Post that, the preliminary states for the entire encryption rounds is evaluated using the following equation (8):

$$\begin{cases} y_0^{(j)} = (y_0, h + e * I_j) \; mod \; 1 \\ q_0^{(j)} = (q_0, h + e * I_j) \; mod \; 1 \end{cases} \tag{8}$$

In the above equation (8), the j is the parameter limited to the value 4 starting with the initial value 1 with the one of the building block of $\left(y_0^{(j)}, q_0^{(j)}\right)$, in the HCS system which can build the distributed random sequence of CS for the randomization of the substitution technique. The proposed EIIS model is targeted for the non-maximization of the pixel correlation with the existing adjacent pixel values in the image under consideration. As the EIIS will be carried out for the matrix based approach having the equal number of rows and columns which is represented as M as given by (9):

$M^2 * M^2$

(9)

For an instance, in regard with the multimedia data of size $N * O$ to be encrypted, the block size M is computed using following equation (10):

$$M = \min\{\lfloor\sqrt{N}\rfloor, \lfloor\sqrt{O}\rfloor\} \tag{10}$$

In any digital multimedia image, it will be processed by shifting the digital data pixel with the right angle clockwise rotation then operated with the EIIS operation with the limiting factor of $M^2 * M^2$, and size of the block can be obtained by the equation (10). For an image with the order of the dimension $N * O$, the overall pixel will be altered by the scrambling operation if and only if which meets the criteria $M = \sqrt{N} = \sqrt{O}$. A small shift in the angle of the image by a clockwise right angle of the effective EIIS will be performed to ensure the operation over all the pixels with the scrambling operation.

Further, for improving security, a random optimization method is modeled. The state-of-art method scatters the changed pixel value column by column and row by row using fixed rule sets. Adopting these methods will give enough information for carrying out a wide range of attacks. For addressing the problems and achieve superior security performance, this work presents an efficient pseudorandom substitution method. Let us consider that both have a dimension of the proposed bit scrambling and the constructed chaotic matrix and are a matrix index generated by ordering each column. For obtaining the greatest integer that is not greater than, the function is utilized, depicts the intensity level parameter. The decryption operation substitution will be carried out by inversing operations utilizing the same substitution order.

2.3 DNA encoding and decoding method

For achieving of minimal correlation coefficient among the adjacent and nearest possible pixels it is implemented with the EIIS technique, which is an aid for the attainment of nonlinear complex values with the cipher pixel and input pixel values. For the attainment of increasing the security level and the entire process of DNA encoding is expressed as follows:

- EIIS and RSS are operated on the "Q", where Q is the image format with the dimension $N * O$ for the resultant B_1 which is a binary sequence. The operation of DNA computing is done as discussed in [19,20,22] the binary sequence is encoded with the obtained DNA sequence.
- Addition process in the DNA approach is achieved by the sequences pertaining to the combination of the binary and DNA sequences.
- Then in the successive step, from the chaotic sequence the new sequence of L_T is obtained followed by the binary encoded sequence as obtained with the individual rule.
- For obtaining the D_3 sequence, the addition operation among the previous bits are carried to avoid redundancy with the basic threshold principle given by (11):

$$\mathbb{T} = \begin{cases} 0, & 0 < \dfrac{K}{Z} \leq A, \\ 1, & 0.5 \leq \dfrac{K}{Z} \leq B. \end{cases} \tag{11}$$

For obtaining DNA sequence D_4 and for obtaining a binary sequence B_1, the decoding process of DNA can be summarized as follows:

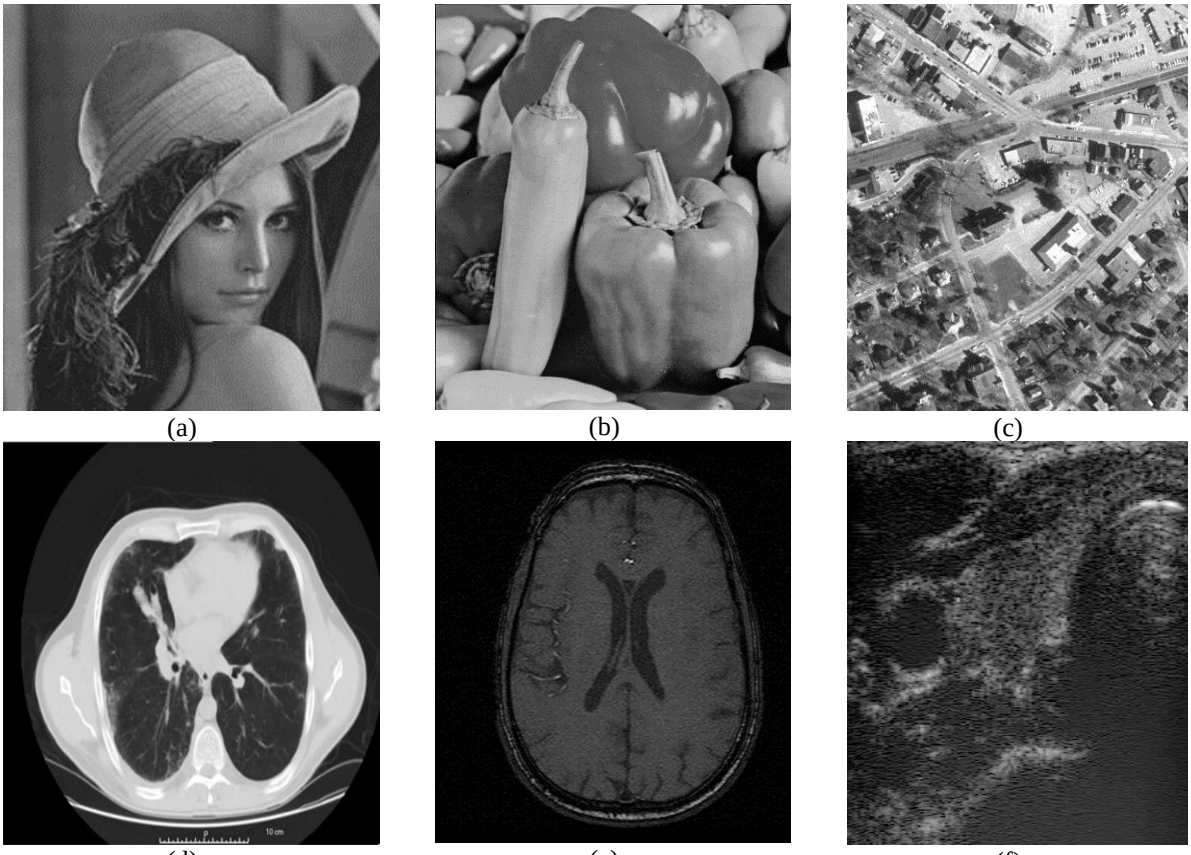
- DNA coding rule is utilized to decode D_4.
- For the cipher text in the binary sequence B_3, it is performed with the logical exclusive OR operation between B_2 and B_1.
- Lastly, B_3 is converted to cipher image R.

In the counter passion of the encryption, suitable decryption is carried out for the reconstruction of the plain text from the ciphertext. The SEIC method is secure and efficient, which is experimentally proven and discussed in the following section.

4. Experimental Results And Analysis

The experimental results of the proposed model of SEIC with the other existing models of image security [22, 23] will be presented in this section. Therefore, different parameters such as UACI (uniform average changing

intensity), NPCR (Number of Pixel Change Rate), Histogram, Information entropy for the two different conditions under consideration, such as the static and dynamic environment, are used to detail the results. The proposed model uses the platform of Visual Studio 2017 with all the necessary toolboxes of MATLAB 2018. The model implemented is carried out on the few standard database images of the size 256∗256 universally accepted. The sample images of Lena, Peppers, and Aerial image are as shown in figure 2, out of which medical data for the evaluation of the model is also considered, surgical data is collected from [28]. These images considered for the experiment are diverse which will aid in validating the robustness of the security model. Figure 2 shows Images used for experiment analysis. Images shown in Figure 2a and 2b namely Lena and Peppers are widely used images in the image processing field. Figure 2c in this work considered satellite image, as a huge amount of satellite data has been collected and stored for security, crop classification, disaster management, etc. All these satellite data require a secure data storage technique with high efficiency. Figure 2d is a CT scan image, Figure 2e is an MRI image, and Figure 2f is an ultrasound image. Among these, the image Figure 2f is very noisy in nature followed by Figure 2e, and Figure 2d. Thus, evaluating security on diverse medical diagnostic data is needed for different treatments, as doctors will use various procedures. Till now, very rarely, the researchers have spotted the implementation of satellite images and medical images for security-related parametric analysis.



(a) (b) (c)

(d) (e) (f)

Fig. 2. Images used for experiment analysis

2.1 Histogram performance evaluation

2.2

Concerning the clinical research data, this exhibits the various properties statistically with the variation of distribution property in the grayscale for the input clinical hidden data for a promised threshold level. In continuation of the previous criteria, a histogram-based analysis is focused on the notable factor for operating the data encryption on the input clinical data on account of futuristic multimedia data for its properties. For the avoidance of statistical attack, the statistical similarity of the histogram representation of the source image and encrypted image should not be symmetrical. Hence, the histogram of the encrypted image should be relatively at or with a uniform statistical distribution, indicating the strength and quality of the encryption system[31]. For validation, variable key size is employed for data image encryption on the particular image, the parameter of variance on the ciphertext of the image is validated as satisfying the equation (12). If the respective ciphertext is

close, then the cipher image has higher histogram uniformity. The histogram variance is computed using the following equation (12):

$$V(Z) = \frac{1}{n^2}\sum_{i=0}^{1}\sum_{j=0}^{n-1}\frac{(z_i - z_j)^2}{2} \quad (12)$$

Where Z is the histogram parameter vector $Z = \{z_0, z_1, z_2, \ldots, z_{256}\}$ of grayscale image, and z_i and z_j are the total pixel sizes with grey parameters i and j, $n = 256$. The histogram performance of SEIC is computed using Eq. (12) and as shown in Figure 3. The image in the first column depicts the source image and its corresponding histogram values are shown in column two. Similarly, the cipher images obtained using SEIC are shown in column 3 and its corresponding histograms are shown in the last column. As a result, it shows that very little correlation has occurred between the cipher images and the source images. Further, identical histogram outcomes of the source and the decrypted images obtained show the SEIC can retain information efficiently even when applying security. From the overall result obtained, it can be seen that the proposed SEIC model attain less correlation among neighboring pixels.

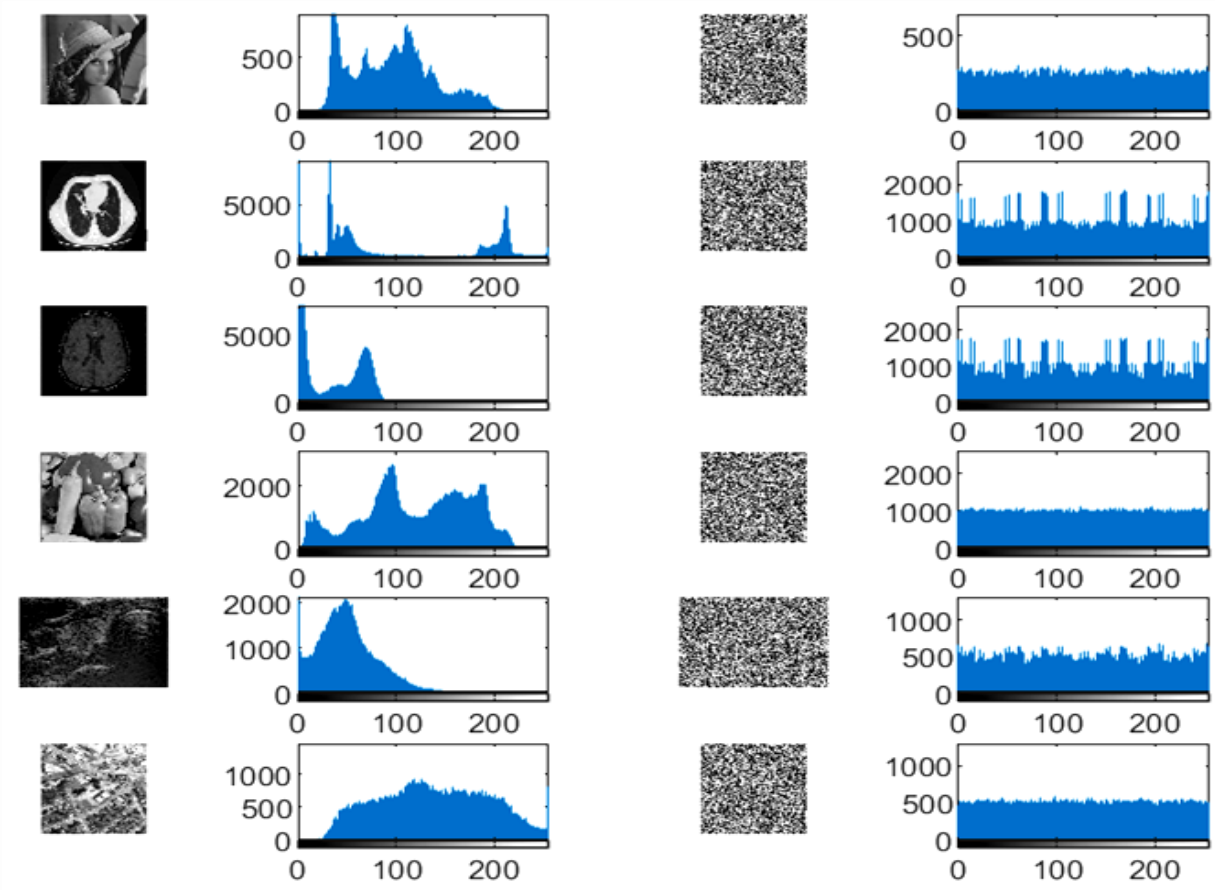


Fig. 3. Histogram performance evaluation of proposed SEIC method

2.3 Differential attack resistivity evaluation

2.4

In this section, the DA (Differential Attack) resistivity evaluation is analyzed for the SEIC security model with the existing security methods. The untrusted users may get insight information of an image by just altering a few pixel positions in the original image. The resistance for such an attack is measured using UACI and NPCR. The NPCR indicates the number of different pixels in two images. In other words, NPCR helps us to understand the effect of change of single-pixel over an image. The UACI describes the difference between two images in average pixel intensity values. A DA is measured in terms of UACI [29] using below equation (13):

$$UACI = \frac{1}{W * H}\left[\sum_{i,j}\frac{|C(i,j) - C'(i,j)|}{255}\right] * 100 \quad (13)$$

Similarly, the NPCR is computed as follows (14):

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W * H} * 100 \quad (14)$$

Where W and H depicts width and length of the grayscale image respectively and C and C' depicts the cipher picture elements with respect to 2 input picture elements with a uni-pixel variation. The UACI and NPCR performance is computed as shown in Eq. (13) and Eq. (14) and performance attained by proposed SEIC security model over existing security model is given in Table 1 and Table 2 respectively. From tabulated result analysis it is observed and noted proposed SEIC model can resist to PT (Plain Text) attack and DA when compared with existing security model (X. Zhang, 2018); (Sun, 2018).

Table 1. UACI performance evaluation considering diverse images

Algorithm	Lena	Pepper	Aerial	Chest CT	Brain MRI	Ultrasound
(X. Zhang, 2018)	28.7344	-	-	-	-	-
(Sun, 2018)	33.46	-	-	-	-	-
SEIC [proposed]	49.75	24.45	26.73	2.85	49.92	24.94

Table 2. NPCR performance evaluation considering diverse images

Algorithm	Lena	Pepper	Aerial	Chest CT	Brain MRI	Ultrasound
(X. Zhang, 2018)	99.6185	-	-	-	-	-
(Sun, 2018)	99.61	-	-	-	-	-
SEIC [proposed]	99.62	99.25	99.24	11.33	99.26	99.21

3.3 Correlation coefficient and Information Entropy analysis

This sub-section of the article is confined to the topic of SEIC performance analysis in terms of information entropy and correlation coefficients when compared with existing models. Correlation coefficient values indicate the relationship between the pixels which are adjacent to each other. The smaller values of correlation co-efficient show the greater security against attacks as resisting ability against them. The performance of the correlation coefficient is given by the following equation (15):

$$r_x = \frac{cov(x,y)}{\sqrt{D(x)D(y)}} \quad (15)$$

Where p and q are adjacent pixels. cov (p, q) is the covariance between two pixels p and q. It is given as follow (16):

$$cov(p,q) = \left(\frac{1}{N}\right)\sum_{i=1}^{N}\left(p_i - E(p)\right)(q_i - E(q)) \quad (16)$$

Where $E(p) = \left(\frac{1}{N}\right)\sum_{i=1}^{N} p_i$

$$D(p) = \left(\frac{1}{N}\right)\sum_{i=1}^{N}(p_i - E(p))^2$$

Table 3. Correlation coefficients performance

Table 3 shows the correlation coefficients performance compared with existing methods. It is observed in the results that the proposed SEIC model has resulted in a comparatively good performance in the coefficient analysis.

In continuity, the proposed work is also extended to the computation of the information entropy, which will be given by the following equation (17):

$$H(m) = -\sum_{k=0}^{2^N-1} p(m_i)\log_2 p(m_i) \quad (17)$$

In the above equation (17), $p(m_i)$ will denote the corresponding value for the probabilistic value for the cipher data given by m_i. With reference to the model discussed in [22], the amount of entropy is 7.9967, whereas on the other hand in the security model described [23] an entropy value of 7.978, and finally in the proposed SEIC model has attained the entropy value of 7.998492 which ensures the supportive value for the saying proposed SEIC is the novel model for the standard images.

5. Results and Discussion

With the obtained results, it is noticeable for the SEIC model for the novel unique performance of the desired system with the consideration of the different parameters such as data entropy, correlation coefficient, NPCR, histogram, and UACI. The proposed model of SEIC can withstand many possible security attacks; this model can perform better than the existing models with validation, such as efficient data image scrambling technique at every step of CS. The proposed model achieves higher values of NPCR and UACI values when compared to existing methods. The security of the system is enhanced due to the fact of the system that the images under consideration are constituted with the pixel values, and every adjacent pixels with the individual correlation coefficients achieved smaller values. The proposed SEIC model has attained the betterment in all the aspects of consideration with all the possible existing models [5,6,22,23] with the salient resistance with the possible attacks.

6. Conclusion

This research article is a novel outcome for the domain of the enhanced smart hybrid data security systems for the data secrecy in terms of the standard image under consideration executed for the near-future environment. This research article progressed initially subjective to the data-efficient handling with the existing strategies such as arbitrary random sequences and HCS technique. Then the approach is continued with the substitution technique of DNA for the suitable improved efficiency with the ciphering technique of the proposed SEIC method. The results ensure and support the unique dataset, with the attainment of the superior SEIC security, regarding the correlation coefficient, NPCR, UACI, and entropy of data under consideration with the proposed image security model. In the later part of the article, the SEIC security model is discussed, which can withstand different types of data attacks, such as cropping attack, brute force attack, linear cryptanalysis attack, differential attack, and noise resistance with the use of a larger encryption key size. With the futuristic research, it is also interpreted for security and limited time complexity with the consideration of real-time data for analysis.

7. Acknowledgment

I Bahubali Akiwate take this opportunity to express my deep sense of gratefulness to my guide and mentor Dr. Latha Parthiban, Pondicherry University, Pondicherry, India for her valuable advice, expert guidance, and unceasing support at all the stages during this research work. I extend my sincere gratitude to Dr. Veena Desai, Gogte Institute of Technology, Belagavi, Karnataka, India for her timely suggestions and encouragement in accomplishing this work.

Algorithm	Horizontal	Vertical	Diagonal
(X. Zhang, 2018)	0.0068	-0.0054	0.001
(Sun, 2018)	0.0039	-0.0314	0.0158
SEIC [proposed]	0.000901	0.004058	0.000790

References

1. Jinsong Wu, Song Guo, Jie Li, Deze Zeng, “Big Data Meet Green Challenges: Big Data toward Green Applications”, IEEE Systems Journal, vol. 10, issue. 3, Sept. 2016.
2. Jinsong Wu, Song Guo, Jie Li, Deze Zeng, “Big Data Meet Green Challenges: Greening Big Data”, IEEE Systems Journal, vol. 10, no. 3, Sept. 2016.

3. Run-Fa Liao, Hong Wen, “Security Enhancement for Mobile Edge Computing through Physical Layer Authentication”, IEEE Access, vol. 7, pp. 116390-116401, August 2019, DOI: 10.1109/ACCESS.2019.2934122.
4. 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.
5. 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.
6. A. A. Abd El-Latif, B. Abd-El-Atty and M. Talha, "Robust Encryption of Quantum Medical Images," in IEEE Access, vol. 6, pp. 1073-1081, 2018.
7. L. Huang, S. Cai, X. Xiong, and M. Xiao, "On symmetric color image encryption system with permutation-diffusion simultaneous operation," Opt. Lasers Eng., vol. 115, pp. 7_20, Apr. 2019.
8. Y. Luo, S. Tang, X. Qin, L. Cao, F. Jiang, and J. Liu, "A double image encryption scheme based on amplitude-phase encoding and discrete complex random transformation," IEEE Access, vol. 6, pp. 77740_77753,2018.
9. C. Zhu and K. Sun, "Cryptanalyzing and improving a novel color image encryption algorithm using RT-enhanced chaotic tent maps," IEEE Access, vol. 6, pp. 18759_18770, 2018.
10. N. Koblitiz, "Elliptic curve cryptosystems". Mathematics of computation. Vol. 48; No. 177; 1987; 203-208.
11. Z. Liu, T. Xia, and J. Wang, "Image encryption technique based on new two-dimensional fractional-order discrete chaotic map and Menezes-Vanstone elliptic curve cryptosystem," Chin. Phys. B, vol. 27, no. 3, pp. 1_16, 2018.
12. M. Kumar, A. Iqbal, and P. Kumar, "A new RGB image encryption algorithm based on DNA encoding and elliptic curve Diffie-Hellman cryptography," Signal Process., vol. 125, pp. 187_202, Aug. 2016.
13. Ayoup A, Hussein A, Attia M, “Efficient selective image encryption”. Multimed Tools Appl. Springer Science+Business Media New York, 2016.
14. Ahmad M, Shamsi U, Khan I, “An enhanced image encryption algorithm using fractional chaotic systems”. Proc Comput Sci 57:852–859, 2015.
15. J. Chandrasekaran and S. J. Thiruvengadam, “A hybrid chaotic and number theoretic approach for securing DICOM images,” Secur. Commun. Netw., vol. 2017, Art. no. 6729896, 2017.
16. X. Chai, Z. Gan, K. Yuan, Y. Chen, and X. Liu, “A novel image encryption scheme based on DNA sequence operations and chaotic systems,” Neural Comput. Appl., pp. 1–19, Apr. 2017.
17. X. Wang and C. Liu, “A novel and effective image encryption algorithm based on chaos and DNA encoding,” Multimedia Tools Appl., vol. 76, no. 5, pp. 6229–6245, 2017.
18. 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.
19. 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.
20. 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.
21. 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.
22. 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, Art no. 3901014. doi: 10.1109/JPHOT.2018.2859257, 2018.
23. 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, Art no. 7201714. doi: 10.1109/JPHOT.2018.2817550, 2018.
24. Haiju Fan and Ming Li, “Cryptanalysis and Improvement of Chaos-Based Image Encryption Scheme with Circular Inter-Intra-Pixels Bit-Level Permutation,” Mathematical Problems in Engineering, vol. 2017, Article ID 8124912, 11 pages, 2017. https://doi.org/10.1155/2017/8124912.
25. A. Kanso and M. Ghebleh, “An efficient and robust image encryption scheme for medical applications,” Commun. Nonlinear Sci. Numer. Simul., vol. 24, nos. 1–3, pp. 98–116, 2015.
26. K. Muhammad, M. Sajjad, I. Mehmood, S. Rho, and S.W. Baik, ``A novel magic LSB substitution method (M-LSB-SM) using multi-level encryptionand achromatic component of an image," Multimedia Tools Appl., vol. 75, no. 22, pp. 14867-14893, 2016.
27. 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.
28. Standard Test Images. Compiled by Mike Waken, University of Michigan--ww.ece.rice.edu/~wakin/images/.Last accessed september 2020.

29. 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.
30. 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.
31. L.-C. Huang, L.-Y. Tseng, and M.-S. Hwang, “A reversible data hiding method by histogram shiftingin high quality medical images,” Journal of Systemsand Software, vol. 86, no. 3, pp. 716-727, 2013.
32. Rachad Atat, Lingjia Liu, “Big Data Meet Cyber-Physical Systems: A Panoramic Survey”, IEEE Access, vol. 6, pp. 73603-73636, 10.1109/ACCESS.2018.2878681, 2019.
33. Luo, R. Zhou, J. Liu, C. Yi, and X. Ding, "A parallel image encryption algorithm based on the piecewise linear chaotic map and hyper-chaotic map," Nonlinear Dyn., vol. 93, no. 3, pp. 1165_1181, Aug. 2019.