

## An efficient data masking for securing medical data using DNA encoding and chaotic system

Siddhartha B. K.<sup>1</sup>, Ravikumar G. K.<sup>2</sup>

<sup>1</sup>BGS Institute of Technology, India

<sup>2</sup>Department of Computer Science and Engineering, BGS Institute of Technology, India

---

### Article Info

#### Article history:

Received Jun 26, 2019

Revised May 5, 2020

Accepted May 27, 2020

---

#### Keywords:

Bit-level scrambling

Chaotic system DNA encoding

Cryptography

Steganography

---

### ABSTRACT

Data security is of utmost importance for ubiquitous computing of medical/diagnostic data or images. Along with that must consider preserving the privacy of patients. Recently, deoxyribose nucleic acid (DNA) sequences and CSs are jointly used for building efficient data masking models. However, the state-of-art method is not robust against cropping attack (CA) and noise. Since in the existing model most of the digits of each pixel are not changed. This work represents efficient-data-masking (EDM) using chaos and the DNA based encryption technique for securing the healthcare data. For overcoming the research challenges the effective-bit-scrambling technique is needed. At first, this work represents an efficient bit-scrambling using the logistic-sin-map, and the PS-utilizing the chaotic system. Then the substitution is carried out between them to resist against SA, DA, and CA. the experiments are conducted on the standard assuming the diverse images. The gained result represents that the introduced model is very efficient when compared to the existing models.

*Copyright © 2020 Institute of Advanced Engineering and Science.  
All rights reserved.*

---

### Corresponding Author:

Siddhartha B. K.,

BGS Institute of Technology,

Karnataka, India.

Email: siddharthbk7@gmail.com

---

## 1. INTRODUCTION

A recent development in information and communication technology and the health care domain has increased the sharing of diagnostic data such as scanning, X-ray report, etc. the increased usage of diagnostic digital data over the online environment has resulted from researchers in providing secure processing and compressing of diagnostic data. Further, in recent times most of the eminent research is going to processing, handling, and sharing the larger amount of collected data from different sources [1-3]. Anyways, preserving the privacy of digital data like videos and images shared via the internet has been the main concern. In most of the applications, these data are the privacy-sensitive information. Thus, it can be abused if improper management and handling of these stored data in the plaintext on the environment of cloud storage. As an outcome, more attention can be paid to preservice privacy [4]. Anyways, with the rapid development of communication and information technology, the multimedia information is prone to the security attacks data can be modified and re-distributed without knowing the data owner. Furthermore, security risk may induce copyright violation, information theft and privacy, and different kind of statistical and differential attacks [5-7]. For instance, the medical pictures, healthcare and data's are used in the electronic patient record, diagnostic picture-information is sent to the concerned person who is located by the means of non-safety-internet channels [8-12]. The smaller information to these diagnostic would outcome in wrong diagnosis and life-loss.

Data masking (DM) using cryptography is an area of mathematics and computer science that offers several methodologies and algorithms that overcome the challenges in providing security for different kinds of data such as multimedia data, textual data, and medical data, etc. The number of cryptography approaches

using a digital signature (DS) and encryption has been discussed in the literature. The existing security method such as Feistel, advanced-encryption standard, and RSA are insufficient for giving the scalable and robust security for diagnostic/image data [13]. This model needs image modification visually and statically. Due to massive data size, a high correlation between higher redundancy and neighboring [14]. Thus, this leading to various types of invite attacks and suspicious [15]. However, in recent time selective encryption has been used to protect medical data that minimize computation time and maintain a high level of secureness. This has led the researcher to model various selective encryption methods for securing digital medical images that can be used for provisioning various real-time wireless medical and mobile health care services for safeguarding diagnostic information.

Chaotic system (CS) is well-known for initial conditions and parameters, pseudorandomness, ergodicity, and reproduction [16]. Thus, in recent times the number of chaotic based multimedia cryptography models has been modeled for provisioning security to medical data [17-20]. However, the existing chaotic based security method has certain limitations for example non-uniform information distribution, intermittent chaotic behavior, and so on. For addressing the aforementioned problems, Zhou et al., [21] presented a chaos-based security method with enhanced chaotic behavior. DNA based cryptosystem has emerged as an efficient mechanism in recent for provisioning security for multimedia and digital data. The major benefit of using DNA based security method provides an unbreakable cryptosystem, low power consumption, huge data storage, and low power consumption [22]. Further, in literature few works have shown that some chaotic based security models are prone to attacks [23, 24]. In [24], showed chaotic cryptography (CC) method might remove the diffusion effect and reconstruct the key structure by applying known/chosen plain text (PT) analysis. For overcoming, some work has combined both CSs with DNA cryptographic mechanisms [25-27]. Furthermore, [28] came up with dynamic deoxyribonucleic-acid encoding-technology and Feistel network utilizing the structure of “permutation-diffusion-scrambling”. In [29], represented the model of image-encoding security utilizing pixel and bit-level scrambling and performed the encoding operation of nucleic-acid. The experimental result represents the state art of model that can fight against the PTA (plain-text-attack), statistical and differential attacks and SPS (strong-plaintext-sensitivity), extensive performed in [30] shows each model has cons and pros. They showed representing the hybrid-design may nor ensure the high security. As an outcome, for providing an effective and fast security model, it is very eminent to represent the encryption method and bit-scrambling utilizing the DNA encoding technique and chaotic system.

For overcoming research challenges, this work represents a new data masking technique for securing the medical data based on DNA encoding technique and chaotic system. Firstly, it represents the effective bit-scrambling-technique to achieve a lower correlation between the neighboring pixels. Then, the bit-randomization is carried out. Then, the given image is encoded by using the substitution of DNA to resist the different types of security attacks like differential and statistical. Along with it can resist the cropping attack. The introduced image encryption method achieves a better performance of image encryption than the existing models of image-encryption.

The research contribution is described below

- Represented an efficient BSM (bit-scrambling method) by using CS (chaotic sequence) and PS (PS) that has a lower correlation among all neighboring pixels.
- The proposed model can allow the decryption of images efficiently even with the presence of noise.
- Proposed model attain superior performance considering information entropy (IE), correlation coefficient (CC), histogram (H), UACI, and NPCR when compared with state-of-art models [17, 28, 29, 31]. Thus, it is efficient against various types of attacks for example entropy, statistical, cropping, noise, plain, and differential attack.

This manuscript is defined as Section 1 provides the introduction of image-encryption utilizing chaotic-system and the DNA encoding. Further, it highlights research challenges, issues, and problems are representing the efficient data masking technique. Section 2 describes different state-of-art methods represented to give secure image encryption utilizing the chaotic system, DNA encoding. In section 3 the introduced an efficient data masking technique for securing the medical image utilizing the CS and the DNA. The experiment analysis and outcome are discussed in section 4. Lastly, the conclusion with the future research direction of this work is discussed.

## 2. LITERATURE SURVEY

This section conducts an extensive survey of the various existing model for provisioning security to information (images) shared over the internet. In [31], aimed at addressing the patient’s safety and confidentiality through the refuge of medical media. They have proposed a model using CS (CS) and quantum encryption for preserving the privacy of health care images. In this context, encrypted images are

sent to the environment of CC (cloud computing) by the healthcare-staff in the respective area. The image from the cloud is received with the help of healthcare-staff in their location. The staff of healthcare can securely support the users' by decrypting the image content. They have suggested a novel technique for enhanced quantum (EQ) of image encryption of the healthcare-media. The CS and gray code set are utilized in their method. The quantum gray-code and quantum images are scrambled. Formerly, the image of scrambled-quantum has encrypted the operation of quantum XOR that built on the key generator by LSCSS (logistic sine-CS-set). Based on the NEQR-quantum image-demonstration, the projected decryption/encryption circuit's algorithm is planned. The encryption method of the quantum image is robust, realizable and it has better efficiency when associated with the classical-counterpart that are represented by the simulation and numerical analyses.

In paper [7], the author aimed at addressing the chaos-encryption based on the blind digital image-watermarking technique that is applicable for color and grayscale images. Before embedding a watermark in the host-image of DCT must be utilized. Former to the allocation of DCT (Discrete-cosine-transform), the host image is parted into  $8 * 8$  non-overlapping blocks via modifying the difference between adjacent blocks of DCT-coefficient of watermark-bit is embedded. To add the double-layer of security, which is utilized to the WAT (watermark Arnold-transform). The introduced algorithm has been analyzed and tested by 3 various dissimilar variances. The outcomes represent that their method is robust to maximize the operations of image processing like joint picture-expert group, sharpening, and median filtering and cropping. The experimental result is related to the state-art-of method to authorize the efficiency of their method. The outcome represents better performance in terms of security, robustness, and imperceptibility.

In paper [32], aimed at addressing double-chaos-system and DNA-encryption algorithm that covers coupled-sequence set of lattice-chaos system and Optical-chaos-injection, novel image encryption then the transmission system is introduced with same chaos injection form laser with 2-optical responses, two (SL2 and SL1) can output the same chaotic signals can be served as one of the chaotic-carrier to pass on the given image and utilized to generate the encryption method. The rule of DNA complementary can be generated by 128-bit-key which is utilized original-value of dual-chaotic-system, therefore the key is one of the hypersensitive in the process of encryption and decryption process. The chaotic synchronization amid SL1 and SL2 is desired through numerical experimental outcomes of the cross-correlation function.

In [29], aimed at addressing a novel image encryption scheme has been projected with the help of pixel-level scrambling (PLS), DNA encoding, and bit-level scrambling (BLS). Hyper-chaos system is computed and chaos sequence is generated using initial conditions of five-dimensional. It is proved that their scheme is very safe and can resist known PTA, DA, and SA by conducting experiments and theoretical analysis. It is suitable for practical application.

In paper [28], aimed at addressing dynamic-DNA-encoding technology and FN (Feistel-network), an image encryption method is estimated by the help of PFS-structure (permutation-diffusion-scrambling). The algorithm of SHA-3 is used to calculate hash-value of plain-text as preliminary-value of hyper-system of chaos and generated the sequence of chaotic is utilized to crate HCM (Hill-cipher-matrix) to substitute the pixel of an image. Whereas in [17], the author aimed to protect digital-media data from counterfeit and fraud as they are sent over public-channel. It is very hard to send all larger medical data with improvised the data-traffic. Different novel methods have come into the image to minimize traffic while upholding adequate security-level. This algorithm consists of three phases like permutation, encoding, and diffusion. In all of the phases, the precise assortment of the ruleset is depends on key-sequence that produced from joined-method. The experimental result is carried out to validate developed resistance algorithms to DA, SA, and BFA.

From an extensive survey carried out, it can be seen using deoxyribose nucleic acid sequence and hyperCS for performing encryption on image aid security performance. The existing encryption model for the image using both hyperCS and DNA sequences can fight against DA types for example BFA, DA, EA, and SA. However, no prior work can resist against CA. This is a due correlation among the adjacent pixel is very high. Thus, the bit and pixel scrambling technique are not efficient. Thus, there is a requirement to develop a new image encryption model that overcomes the above-mentioned research problem. This paper presents such a security model in the next section below namely, an efficient data masking method for securing the medical-image using the chaotic system and deoxyribose-nucleic acid encoding.

### **3. AN EFFICIENT DATA MASKING METHOD FOR SECURING MEDICAL DATA USING DEOXYRIBOSE NUCLEIC ACID ENCODING AND CHAOTIC SYSTEM**

This section presents an efficient-data-masking (EDM) method for securing the medical image and multimedia. Firstly, the new-chaotic-sequence of the generation-model is represented. Then, the system model is defined for performing the encryption on the medical image and multimedia. Then, it represents

a bit-scrambling-method and key generation. Finally, it represents an encryption technique for securing the medical image and multimedia. The below-given block diagram of the introduced data masking technique for securing the medical image, which is represented in Figure 1.

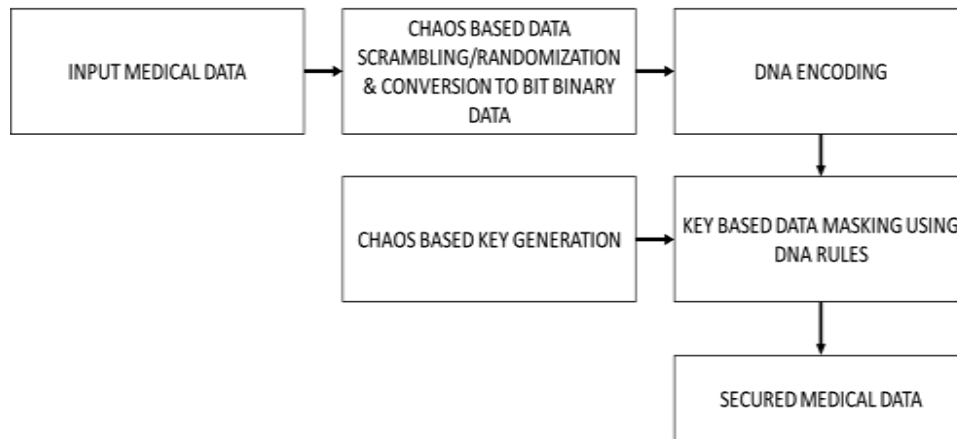


Figure 1. The architecture of proposed efficient data masking method using DNA encoding and chaotic system

### 3.1. Novel CS method

EDM-model overcomes the disadvantage of existing-CS based security technique. The introduced new NCS (novel-chaotic-sequence) is defined as follows:

$$y_{j+1} \cos(\pi(G(b, y_j) + H(c, y_j) + \gamma)), \quad (1)$$

where,  $H(c, y_j)$  and  $G(b, y_j)$  represents the sets of CS (chaotic-sequence) defined as the sets of seed-sequence,  $c$  and  $b$  represent the sets of control-parameters' seed-sequence and  $\gamma$  is defined as the parameter that depicting the shifting constantly.

From (1), it can be seen that our model associates the result of  $H(c, y_j)$  and  $G(b, y_j)$  with  $\gamma$ . After that, it performed the cosine-transformation for generating the result. The function of association aid in efficiently shuffle-CS and scramble dynamics of 2-seed-sequence sets. Furthermore, utilizing the cosine-transformation that aid in getting the higher complex nonlinearity. As an outcome, the sets of a chaotic system achieved by utilizing the introduced technique and exhibit the complex-behavior. This is due to the sets of seed-sequence  $H(c, y_j)$  and  $G(b, y_j)$  in introduced CS that can be the sets of existing CS, the service subscriber and provider can utilize various combinations of the existing CS-sets to generate the various sets of CS flexibly.

### 3.2. A system model of proposed data masking model for performing encryption of multimedia image

When the sets of CS used in performing the encryption operations, the complexity-feature of CS dominates security features of the cryptography-mechanism. Here, we represent a new encryption technique using introduced the sets of LSCCS created by utilizing the NCS. For achieving a high level of encryption-standard, this work mainly utilizes the organization of confusion-diffusion. The secure-key  $L$  creates the sets of preliminary state for the set of SCCS to generate the CS that provides better EBS (efficient bit scrambling) and ASS (arbitrary sequence substitution). The EBS can be modeled in such a way that it separates the neighboring-pixel into a distinct position. Whereas, ASS is used to optimize the value of a pixel based on the PS that is established by CS. After that, the diffusion and EBS process for a certain iteration, the image of plain-multimedia is encrypted by using the rule of DNA coding to get the secure-cipher image.

### 3.3. DNA encoding and binarization

The sequences of DNA are generated as Guanine (G), Thymine (T), Cytosine (C), and adenine (A) by utilizing nucleic-acid-bases. The adenine and thymine are complements to each other. Same as, 'C' and 'G' are also complementing to other each other. Since, we utilize 20bit-binary (i.e., '1' and '0') to depict the DNA base that also complements to each other. This work also utilizes the rules that satisfy the rule of Watson-

Crick [28, 29, 33], which consisting 8-rules in below given Tables 1 and 2. Furthermore, DNA computing like XOR, subtraction, and addition operation is performed by using the operation of old-fashioned as represented in Tables 3-5 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
11	T	T	G	C	G	C	A	A
01	C	G	A	A	T	T	C	G
10	G	C	T	T	A	A	G	C

Table 2. Encoding rule set

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

Table 3. Deoxyribose nucleic acid sequence

subtraction function					
---	A	C	G	T	
G	G	C	A	T	
C	C	A	T	G	
A	A	T	G	C	
T	T	G	C	A	

Table 4. Deoxyribose nucleic acid sequences

addition function					
+++	A	C	G	T	
G	G	T	A	C	
C	C	G	T	A	
A	A	C	G	T	
T	T	A	C	G	

Table 5. Deoxyribose nucleic acid sequence

XOR function					
<b>XOR</b>	A	C	G	T	
T	T	G	C	A	
G	G	T	A	C	
C	C	A	T	G	
A	A	C	G	T	

### 3.4. Key generation and efficient BSM:

The secure key generates a set of LSCCS-preliminary. The size-length of secure-key is introduced in LSCCS based on the image-encryption method, which is fixed to 25-bits where  $2^{256}$ key-space is. EBS is modeled to remove and minimize the pixel correlation among neighboring-pixels. It is performed within the block of square-matrix as follows:

$$M^2 * M^2,$$

Where  $M$  is represented as the size of the block. Such as, considered the size of the multimedia-data  $N * O$  to be encrypted then block-size  $M$  is computed by using the following.

$$M = \min\{\lfloor \sqrt{N} \rfloor, \lfloor \sqrt{O} \rfloor\}, \quad (2)$$

Where,  $\lfloor \sqrt{\mu} \rfloor$  shows floor-function to possess the high integer which is higher than  $\mu$ . In this EBS, the image is encrypted into the blocks  $M^2$ . Then based on CS, it can be generated pixel in each of the rows that are permuted into distinct-blocks. Afterward. In each-block their-position is established by utilizing the other-CS.

### 3.5. Proposed bit-scrambling-model

The multimedia-image can be rotated as clockwise by the help of right-angle then EBS is carried out with the limit of  $M^2 * M^2$  and the size of a block is obtained by (2). This image has  $N * O$  size, all of the pixels will be given and scrambled as  $M = \sqrt{N} = \sqrt{O}$ . All of the given pixels are scrambled for ensuring the image angle which is varied by right-angle in the clockwise-direction with successive-EBS.

### 3.6. High dimensional image encryption methodology

The EBS aid in getting a lower correlation between neighboring pixels. It is an aid in achieving the complex correspondence of non-linear between cipher pixel and input pixel that aid in maximizing the security level. Firstly, ASS and EB is carried out on  $Q$  image with size  $N * O$  to get the binary sequence  $B_1$ . Then, encoded  $B_1$  by utilizing the sequence  $D_1$ . Then, the operation of DNA addition is performed on every single sequence of  $B_1$  to posses  $D_2$ . Lastly,  $L_T$  the sequence is removed for  $L$  chaotic-

sequence. Post that,  $L_T$  the sequence is transformed into the binary form  $B_L$ .  $B_L$  can be encoded to get  $D_L$  utilizing 3<sup>rd</sup> encoding rule. Then, forgetting the sequences  $D_3$  the DNA addition between  $D_L$  and  $D_2$  is performed. Then the threshold function is expressed as:

$$\mathbb{T} = \begin{cases} 0, & 0 \leq \frac{K}{Z} \leq A, \\ 1, & 0 < \frac{K}{Z} \leq B. \end{cases} \quad (3)$$

For achieving the sequence of DNA  $D_4$ . For achieving the binary-sequence  $B_1$ , the first rule of DNA coding is used to  $D_4$  decode. Then for achieving the sequences of cipher binary  $B_3$  bitwise XOR operation is performed between  $B_L$  and  $B_2$ . Finally,  $B_3$  is converted to the cipher image  $R$ . Same, to the operation of decryption and encryption is performed in a reverse manner. The outcome achieved represents the EDM model to attain better performance than the existing security model that is proven experimentally below.

#### 4. RESULTS AND DISCUSSION

This section evaluates the achieved outcome by the introduced EDM model over existing security-model [28, 29] in terms of the correlation coefficient (CC), histogram analysis (HA), a number of pixel change rate (NPCR), and uniform average changing intensity (UACI), and Information entropy (IE). The model is implemented by using Matlab 2018-framework tool. For the analysis, we use the obtained medical image from [34]. Further, we utilize standard 256\*256 Lena, aerial image, Pepper for the analysis. All the given image utilized for the experiment analysis is presented in below given Figure 2.

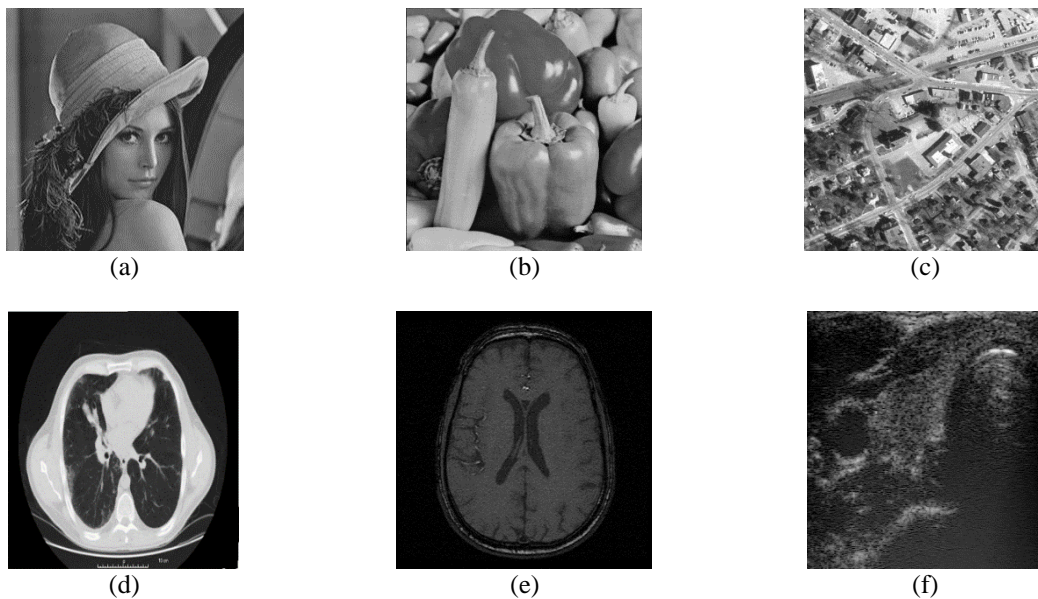


Figure 2. Images used for experiment analysis

##### 4.1. Histogram performance evaluation


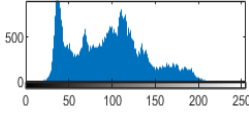

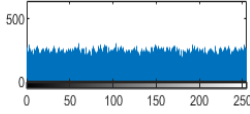

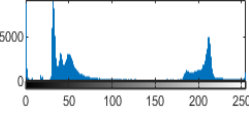

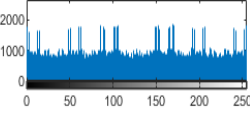

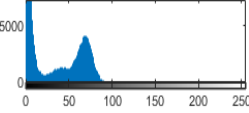

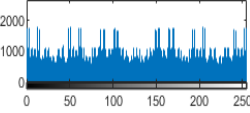

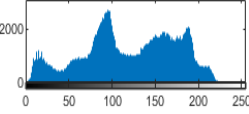

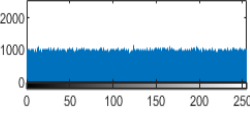
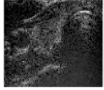
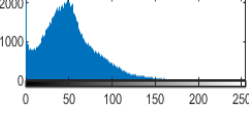

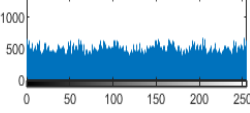

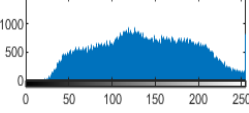

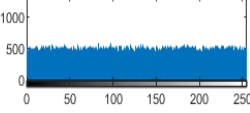
The statistical properties of medical data show the distribution properties of gray parameters of the input medical content to an assured level. Further, the histogram metric is considered to be a significant factor in performing encryption on medical data to see if it modifies the statistical distribution (SD) properties of the input multimedia data. The objective of our grayscale encryption methodology is to resist against statistical attack. Table 6 shows the experiment outcome attained by the proposed encryption model. Experiments are conducted for the image case study shown in Figure 2. From the analysis, it can be seen the proposed image encryption model can resist against greyscale statistical analysis (SA) in a manner where the intruder can't decode the input image or gray parameter distribution properties. Since the proposed encryption model makes the grayscale distribution of the encoded input picture element very flat. Moreover,

to measure the pixel distribution uniformity of the 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 the same image, the variance of these cipher images is computed using (4). If the respective cipher text is close, then the cipher image has higher histogram uniformity. The histogram variance is computed as follows:

$$V(Z) = \frac{1}{n^2} \sum_{i=0}^1 \sum_{j=0}^{n-1} \frac{(z_i - z_j)^2}{2} \tag{4}$$

where  $Z$  is the histogram parameter vector  $Z = \{z_0, z_1, z_2, \dots, z_{256}\}$  of a 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 the proposed model

	Input image	Histogram of the input image	Cipher image	Histogram of cipher image
Case (a) : Lena				
Case (b): Chest CT Scan				
Case (c): Brain MRI				
Case (d): Pepper				
Case (e): Ultrasound Image				
Case (f): Aerial Image				

**4.2. Correlation coefficient performance evaluation**

This section evaluated the performance of CC, which is achieved by the introduced security model over the existing model. The experimental is performed for images and represented in Figure 2. The CC  $r_x$  between the neighboring pixel is calculated by utilizing the below;

$$r_x = \frac{cov(x, y)}{\sqrt{D(x)D(y)}} \tag{5}$$

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

$$cov(x, y) = \frac{1}{N} \sum_i^N (y_i - E(x)) (y_i - E(y)), \tag{6}$$

$E(x)$  is calculated as follows

$$E(x) = \frac{1}{N} \sum_i^N x_i \quad (7)$$

And  $D(x)$  is calculated as follows

$$D(x) = \frac{1}{N} \sum_i^N (x_i - E(x))^2 \quad (8)$$

The CC between encrypted medical/multimedia image and the input-original image is calculated by (5). The performance achieved by introduced the EDM-security model over the existing model which is represented in Tables 7 and 8. From the experimental analysis, it can be seen that the introduced EDM technique achieves much better performance than the existing model for the image.

Table 7. Correlation coefficient attained by proposed EDM over the existing model for Lena images

Algorithm	Horizontal	Vertical	Diagonal
Existing model [28]	0.0039	-0.0314	0.0158
Existing model [29]	0.0068	-0.0054	0.001
Existing model [33]	0.0211	0.0412	-0.0016
EDM model	0.0019	-0.0030	0.0018

Table 8. Correlation coefficient attained by EDM model considering a diverse set of images

Images	Horizontal	Vertical	Diagonal
Pepper	0.0009	0.004058	0.00079
Aerial	-0.00098	0.003369	0.002243
Chest CT	-0.000713	0.0076	0.00034
Brain MRI	0.0013	0.00814	0.00118
Ultrasound	0.003078	0.00055	-0.00039

### 4.3. Information entropy performance evaluation

IE metric is a measurement to compute the degree of insecurity which is computed using the following

$$H(m) = - \sum_{k=0}^{2^N-1} p(m_i) \log_2 p(m_i) \quad (9)$$

where  $p(m_i)$  shows the probability that data  $m_i$  appears. For grayscale images, data  $m_i$  is collected 256 states, the max and min (maximum and minimum) value are 0 and 255, respectively. With the help of (9), entropy is random, whenever the size of entropy is 8 that represents high entropy of the cipher image is secure and the model of encryption is utilized. The entropy performance of cryptographic images obtained by performing encryption on Lena and Pepper image using the proposed and various state-of-art encryption methods is presented in Table 8. From a result, it is inferred that the proposed EDM method achieves superior performance than the existing image encryption method [28, 29]. Thus, shows the information leakage (IL) of cipher image are significantly less. Thus, it proves the security of the proposed image encryption model. Below given Table 9 shows the performance evaluation of information entropy.

Table 9. Information entropy performance evaluation

Algorithm	Lena	Pepper	Aerial	Chest CT	Brain MRI	Ultrasound
Existing model [18]	7.978	-	-	-	-	-
Existing model [19]	7.9967	7.9967	-	-	-	-
EDM model	7.9964	7.9992	7.998	7.955	7.9422	7.9895

### 4.4. Differential attack performance evaluation

This section represents differential attack-performance obtained by introduced the EDM technique over the image encryption technique, A DA is to perform a trivial modification to the input 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 NPCR and UACI are utilized to measure whether the encryption technique resisted differential attack [35]. The UACI is calculated as follows:

$$UACI = \frac{1}{W * H} \left[ \sum_{i,j} \frac{|C(i,j) - C'(i,j)|}{255} \right] * 100 \quad (10)$$

Similarly, the NPCR is computed as follows

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W * H} * 100 \quad (11)$$

where,  $W$  and  $H$  represents the length and width of the gray-scale image, respectively,  $C'$  and  $C$  represents cipher picture elements with regards to two-picture elements with the variation of single-pixel. For pixel  $(i,j)$ , if  $C(i,j) = C'(i,j)$ , then  $D(i,j) = 0$ , otherwise  $D(i,j) = 1$ . The performance of NPCR and UACI is calculated by using (10) and (11) respectively, and performance achieved by introduced the EDM model over the existing method, which is represented in Tables 10 and 11. From the experiment analysis, it can be inferred that the introduced EDM technique can resist the plain-text and the differential attack when compared to the existing model. From achieved outcome it can be seen introduced model achieves the same performance of UACI when compared to the existing model. Anyways, in terms of the NPCR, the introduced EDM model achieves superior performance than the existing model.

Table 10. UACI performance evaluation considering diverse images

Algorithm	Lena	Pepper	Aerial	Chest CT	Brain MRI	Ultrasound
Existing model [18]	28.7344	-	-	-	-	-
Existing model [19]	33.46	-	-	-	-	-
Proposed model	49.7571	24.9	26.15	49.59	49.77	49.91

Table 11. NPCR performance evaluation considering diverse images

Algorithm	Lena	Pepper	Aerial	Chest CT	Brain MRI	Ultrasound
Existing model [28]	99.6185	-	-	-	-	-
Existing model [29]	99.61	-	-	-	-	-
Proposed model	99.23	99.22	99.23	99.22	99.22	99.22

#### 4.5. Result and discussion

From overall achieved outcome represents that the introduced model achieves good superior performance considering CC, UACI, histogram, NPCR, and IE. The EDM model makes a grayscale distribution of the encoded input multimedia picture elements is significantly flat when compared with the existing model [17, 28, 29, 31]. Thus, it can resist against SA. The model of EDM attains superior-performance for CC when compared with the existing image encryption model [17, 28, 29, 31]. This is because EBS is used in each step of CS. Thus, the correlation among adjacent pixels is less and aiding superior security performance. Further, the EDM model attains similar UACI performance and superior NPCR performance when compared with the existing image encryption model [17, 28, 29, 31]. Thus, the EDM model can against DA, cropping, noise, and plain. The overall achieved outcome shows the robustness of the EDM model.

#### 5. CONCLUSION

This paper is represented an efficient-image method using DNA and CSs. The efficient-BSM utilizing arbitrary of LCMCS and random-sequence. Furthermore, the DNA substitution is utilized to maximize the efficiency and cipher-unpredictability of data masking-method. The experiment is done by using the datasets of diverse medical that ranging from MRI to CT. Further, the used standard Lena, Pepper, and aerial image to perform the analysis of comparative. The outcome represents introduced the model of EDM security to attain the superior performance of CC and UACL when compared to the existing model. Thus, the proposed method of EDM security can resist the DA, linear attack (LA), resist noise, and CA more efficiently because of the large-key-space. In future, we will enhancing the generation of CS to further improve security. Along with we will conduct the experiment analysis considering by the varied images and other metrics of security performance.

## REFERENCES

- [1] Z. H. Hu, Y. Wen, T.-S. Chua, and X. Li, "Toward scalable systems for big data analytics: A technology tutorial," *IEEE Access*, vol. 2, pp. 652-687, 2014.
- [2] Y. Luo, D. Tao, K. Ramamohanarao, C. Xu, and Y. Wen, "Tensor canonical correlation analysis for multi-view dimension reduction," *IEEE Transactions on Knowledge and Data Engineering*, vol. 27, pp. 3111-3124, 2015.
- [3] Y. Luo, Y. Wen, D. Tao, "Heterogeneous multitask metric learning across multiple domains," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 29, no. 9, pp. 4051-4064, 2017.
- [4] M. Lim, and P. Yuen, "Entropy measurement for biometric verification systems," *IEEE Transactions on Cybernetics*, vol. 46, pp. 1065-1077, 2016.
- [5] H. Nyeem, W. Boles, and C. Boyd, "Digital image watermarking: Its formal model, fundamental properties and possible attacks," *EURASIP J. Adv. Signal Process.*, vol. 2014, no. 1, pp. 1-21, 2014.
- [6] N. Zivic, "Watermarking for Image Authentication," *Robust Image Authentication Presence Noise, 1st ed. Cham, Switzerland: Springer*, pp. 43-47, 2015.
- [7] N. A. Loan, N. N. Hurrar, S. A. Parah, J. W. Lee, J. A. Sheikh and G. M. Bhat, "Secure and Robust Digital Image Watermarking Using Coefficient Differencing and Chaotic Encryption," *IEEE Access*, vol. 6, pp. 19876-19897, 2018.
- [8] S. A. Parah, F. Ahad, J. A. Sheikh, and G. M. Bhat, "Hiding clinical information in medical images: A new high capacity and reversible data hiding technique," *J. Biomed. Inf.*, vol. 66, pp. 214-230, 2017.
- [9] Reddy, R. O., Dhruve, K. D., Reddy, R. N., Radha, M., and Vani, N. S., "A Novel Approach in Adopting Finite State Automata for Image Processing Applications," *International Journal of Computer Vision and Image Processing*, vol. 8, no. 1, pp. 59-74, 2018.
- [10] S. A. Parah, J. A. Sheikh, J. A. Akhoun, N. A. Loan, and G. M. Bhat, "Information hiding in edges: A high capacity information hiding technique using hybrid edge detection," *Multimed Tools Appl.*, vol. 77, no. 1, pp. 185-207, 2018.
- [11] S. A. Parah, F. Ahad, J. A. Sheikh, N. A. Loan, and G. M. Bhat, "Information hiding in medical images: A robust medical image watermarking system for E-healthcare," *Multimed Tools Appl.*, vol. 76, no. 8, pp. 10599-10633, 2017.
- [12] K. Muhammad, J. Ahmad, S. Rho, and S. W. Baik, "Image steganography for authenticity of visual contents in social networks," *Multimedia Tools Appl.*, vol. 76, no. 18, pp. 18985-19004, 2017.
- [13] 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, 2017.
- [14] A. Kanso and M. Ghebleh, "An efficient and robust image encryption scheme for medical applications," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 24, no. 1-3, pp. 98-116, 2015.
- [15] K. Muhammad, M. Sajjad, I. Mehmood, S. Rho, and S. W. Baik, "A novel magic LSB substitution method (M-LSB-SM) using multi-level encryption and achromatic component of an image," *Multimedia Tools Appl.*, vol. 75, no. 22, pp. 14867-14893, 2016.
- [16] A. Sambas, M. Mamat, A. A. Arafa, G. M. Mahmoud, M. A. Mohamed, and W. S. MadaSanjaya, "A new chaotic system with line of equilibria: dynamics, passive control and circuit design," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 9, no. 4, pp. 2365-2376, 2019.
- [17] 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, 2017.
- [18] Sharma, S., Kumar, T., Dhaundiyal, R., Mishra, A. K., Duklan, N., and Maithani, A., "Improved method for image security based on chaotic-shuffle and chaotic-diffusion algorithms," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 9, no. 1, pp. 273-280, 2019.
- [19] J. Chandrasekaran and S. J. Thiruvengadam, "A hybrid chaotic and number theoretic approach for securing DICOM images," *Secur. Commun. Netw.*, vol. 2017, no. 3, 1-12, 2017.
- [20] S. El Assad and M. Farajallah, "A new chaos-based image encryption system," *Signal Process., Image Commun.*, vol. 41, pp. 144-157, 2016.
- [21] Y. Zhou, L. Bao, and C. L. P. Chen, "A new 1D chaotic system for image encryption," *Signal Process.*, vol. 97, pp. 172-182, 2014.
- [22] X. Li, L. Wang, Y. Yan, and P. Liu, "An improvement color image encryption algorithm based on DNA operations and real and complex chaotic systems," *Opt.-Int. J. Light Electron Opt.*, vol. 127, no. 5, pp. 2558-2565, 2016.
- [23] Y. Zhang, W. Wen, M. Su, and M. Li, "Cryptanalyzing a novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system," *Opt.-Int. J. Light Electron Opt.*, vol. 125, no. 4, pp. 1562-1564, 2014.
- [24] L. B. Zhang, Z. L. Zhu, B. Q. Yang, W. Y. Liu, H. F. Zhu, and M. Y. Zou, "Cryptanalysis and improvement of an efficient and secure medical image protection scheme," *Math. Problems Eng.*, vol. 2015, no. 2, pp. 1-11, 2015.
- [25] A. Merzoug, A. Ali-Pacha, and N. Hadj-Said, "New Approach of the Playfair's Cipher with A Numerical Value of the Keyword," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 6, no. 3, pp. 695-703, 2017.
- [26] 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.
- [27] 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, 2016.
- [28] X. Zhang, Z. Zhou and Y. Niu, "An Image Encryption Method Based on the Feistel Network and Dynamic DNA Encoding," *IEEE Photonics Journal*, vol. 10, no. 4, pp. 1-14, 2018.
- [29] S. Sun, "A Novel Hyperchaotic Image Encryption Scheme Based on DNA Encoding, Pixel-Level Scrambling and Bit-Level Scrambling," *IEEE Photonics Journal*, vol. 10, no. 2, pp. 1-14, 2018.
- [30] H. Fan and M. Li, "Cryptanalysis and Improvement of Chaos-Based Image Encryption Scheme with Circular Inter-Intra-Pixels Bit-Level Permutation," *Mathematical Problems in Engineering*, vol. 2017, pp. 1-11, 2017.

- [31] A. A. Abd El-Latif, B. Abd-El-Atty and M. Talha, "Robust Encryption of Quantum Medical Images," *IEEE Access*, vol. 6, pp. 1073-1081, 2018.
- [32] X. Fu, B. Liu, Y. Xie, W. Li and Y. Liu, "Image Encryption-Then-Transmission Using DNA Encryption Algorithm and The Double Chaos," *IEEE Photonics Journal*, vol. 10, no. 3, pp. 1-15, 2018.
- [33] 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.
- [34] Mike W., "Standard Test Images," University of Michigan, [Online], Available: [www.ece.rice.edu/~wakin/images/](http://www.ece.rice.edu/~wakin/images/).
- [35] 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.

## BIOGRAPHIES OF AUTHORS



**Siddhartha B. K.** received his Bachelor degree from BGSIT, VTU during the year 2009, M.Tech from SJGIT, VTU during the year 2012. Currently pursuing Ph.D degree in VTU. He is having more than 8 years of Professional experience which includes Software Industry and teaching experience. His areas of interests are Big Data Security, Cloud Computing, AI and Machine Learning. He has published and presented papers in National and International conferences and journals.



**Dr. Ravikumar G. K.** received his Bachelor degree from Bangalore University during the year 1996, M. Tech from Karnataka Regional Engineering College Surthkal (NITK) during the year 2000 and Ph.D from Dr MGR University, Chennai. He is working as a Professor and Research Head in Department of Computer Science Engineering, BGSIT. He had worked with iGATE Global solutions Bangalore, Wipro and also has worked with SJBIT as Prof and HOD of Dept of CSE and ISE, having more than 20 years of Professional experience which includes Software Industry and teaching experience. His areas of interests are Data Warehouse & Business Intelligence, multimedia, Databases, AI, Machine Learning. He has published and presented papers in National and International conferences and journals.