International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-6S, August 2019

Secure Medical Image Processing Using Chaos And Dna Encryption Enhanced Using Reversible Data Hiding

Smita Khond, Bellamkonda Vijayakumar

Abstract:- Paper In the field of medication, information security is central. The photographs that are dealt with in the information base and those that are transmitted over the web ought to be shielded from threatening exercises. This paper proposes a novel picture encryption plan helped with reversible information covering framework to improve the nature of the shielded picture transmission. Confusion and DNA encoding norms are utilized for the encryption philosophy. Piecewise Linear Chaotic Map (PWLCM) and Logistic Map are related with produce all parameters the demonstrated calculation needs and DNA encoding headway fills in as an accomplice instrument. The information disguising and extraction process in the blended area submits mistake during the unraveling framework. This is in light of the way that the pixel estimations of the blended spread picture change during the information concealing technique. Thusly the usage of reversible information covering structure rather than the standard information masking methods helps in recuperation of the spread picture, acknowledging immaculate unscrambling. The test results display that the proposed procedure beats the current secure picture transmission approachs.

Keywords: Chaos, Logistic Map

I. INTRODUCTION

Because of the great development of telecommunications and manufacturing, the throughput of new type of unique intelligent gadgets is becoming more. The resolution in the digital images which are captured from those unique intelligent devices is high and also engages vast storage space. As they are having the capability of storing the cumbersome information, high repetition, and powerful algorithms like Data Encryption Standard (DES) [1], Advanced Encryption Standard (AES) [2], Rivest-Shamir-Adleman (RSA).The encoding of the digital images will not be done with these algorithms. They are highly dependent on the conditions which are given initially, counter fight - volatility, periodicity, and recreation are the major lineaments for chaos system[3], and one can achieve all the necessities by using this primary features. Many portrait encryption innovations are produced during the past few decades on the basis of chaos. These innovations will be seen in [2, 9, 12, and 14]. The portrait encryption innovations which had developed on the basis of DNA encoding and Chaos are showing up in any case in the moved field [4, 10, and 13]. The ordinary depiction encryption movements which are made through agitation essentially include two stages, one is shambling and the other is spread [4-5], both the techniques are managed at the same time [1, 3, 11, and 15]. Where the types of progress utilizing DNA encoding technique [6] will also contain two stages, explicitly encoding and deciphering stages. In the basic express, the reasonable depictions are encoded through the DNA rules, all the while; a basic picture is passed on and blended. By at that point, couple of DNA cutoff points are managed on the encoded fundamental depiction and the blended clear picture. At long last, the required picture is picked up by unscrambling the transitional picture. The presentation of the whole framework variation from the norm is polished through confusion. The standard of encryption relying on unsettling influence produces pictures by utilizing arithmetical procedures, yet the standard related for DNA encryption framework [7] will be in the characteristic blueprint. Enayatifar et al. advised a depiction encryption rule arranged on GA and DNA gathering. This examination says, the decided maps and DNA encryption measures are acknowledged to make essential DNA exterior; the manager picks the helpful façade for making encoding through GA rule. Liu et al. built up a standard by utilizing Chaos and DNA [8] basic standard. During the experimentation, each image piece is encoded and upset into base pair after the course toward permuting the lines and zones normally through the packs made by part capable covered puzzled guide. Wang et al. passed on a hard to miss picture encryption strategy reliant on DNA sales and fierce guide. In this assessment, a sort of spatiotemporal issue alliance, where the coupled guide work is adjusted for making the conceivable depiction perplexed. After the strategy for encryption the obfuscated picture, permute its lines and fragments to make the encoded clear depiction. Huang et al predicted a remarkable depiction encryption rule where hyper-perplexity and DNA request [9] is utilized for the strategy of encryption [10]. During this projection, the fake abstract requesting, which has acquired through the four-spatial hyper-issue plot, is balanced into DNA sales to intertwine the plain depiction. The figure is amassed in the wake of performing different rounds of changes. In the proposed paper, definite DNA guidelines or actions are aimlessly pronounced by chaos, which is enough theoretically.

Manuscript published on 30 August 2019.
***** Correspondence Author (s)
Smita Khond, Research Scholar, Computer Science Engineering, Pacific Academy of Higher Education and Research University, Udaipur, Rajasthan, India (Email: smitakhond2009@gmail.com)
Dr. Bellamkonda Vijayakumar, Professor and HOD, Computer Science Engineering,Vidya Jyothi Institute of Technology, Hyderabad, Telangana, India.(Email: vijaysree.b@gmail.com)

Initially, PWLCM is applied for producing the key portrait, then the comprehensible portrait gets encoded and the main portrait respectively through rows by DNA standards [11] which are chosen from eight types; after this procedure, the two encoded portraits are processed row by row for achieving the in-between portrait. Specific activity is pronounced by logistic map; the in-between portraits are decoded as a comprehensible portrait of next mark; at last, all the above process is again processed by the columns for getting the final cipher portrait.

II. PIECEWISE LINEAR CHAOTIC MAP AND LOGISTIC MAP

In this foreseen standard, the Piecewise Linear Chaotic Map (PWLCM) and Logistic guide [12] are used for developing the specifications which are needed for the principle. If observed in ref [10], there are a number of better qualities in PWLCM which supports the developers for designing the main portrait during logistic map performing few secondary works like selecting the method of function or DNA rules. The description of PWLCM is shown with an equation below:

$$x_{n+1} = F_q(x_n) = \begin{cases} x_n/q, & 0 < x_n < p \\ (x_n - q)/(0.5 - p), & p \le x_n < 0.5 \\ F_q(1 - x_n), & 0.5 \le x_n < 1 \end{cases} \quad \ldots\ldots (1)$$

Where x_n in (0, 1) and q in (0, 0.5)

Applying q value as 0.25678900

$$x_{n+1} = \mu(1 - x_n) \ldots\ldots (2)$$

If observed in the extension of coordination map, the user can estimate that, if μ in (3.9, 4), the pseudorandom sequence will be in 0 and 1. The μ value is assigned as 3.9999999 [4] in the projected principle.

Prepare Your Paper Before Styling

Before you begin to format your paper, first write and save the content as a separate text file. Complete all content and organizational editing before formatting. Please note sections A-D below for more information on proofreading, spelling and grammar.

Keep your text and graphic files separate until after the text has been formatted and styled. Do not use hard tabs, and limit use of hard returns to only one return at the end of a paragraph. Do not add any kind of pagination anywhere in the paper. Do not number text heads-the template will do that for you.

III. DEOXYRIBONUCLEIC ACID SERIES

Deoxyribonucleic harming (DNA) is a sort [13, 14] of particles which are sure around four sorts of nucleotides. Adenine (A), Thymine (T), Cytosine (C) and Guanine (G) and various necessities are standard peripherals of nucleotides. With respect to the DNA drives, an and T, C and G are poor sets. 8allowable mixtures present with respect to DNA interdependent rules. It is a type of interdependent rule which consists of something in similar with the binary combination. In detail, ‘0’ and ‘1’ are interdependent and also ‘00’ and ‘11’, ‘01’ and ‘10’ in the binary combination. In the gray-scale-portrait every pixel consists of 8 bits, in simple, it is applied as ‘00’, ‘01’, ‘10’, ‘11’ as Meta information. For encoding the plain image, 4 types of nucleases are applied with 8 standards. For example: the pixel value is taken as 201 in decimal format; its interrelated binary assessment is ‘11001001’. If this assessment is encoded by using the DNA rules, then the user can acquire 8 types of consolidations: 'TACG', 'TAGC', 'ATCG', 'ATGC', 'CGTA', 'CGAT', 'GCTA' and 'GCAT'. A brief range later, different bits of DNA arrangements are utilized with a total target of depiction encryption. The match measures and segments of DNA are recorded in the tables underneath, table 1 to table 4.

Table 1: rules of Encoding and Decoding

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

Table 2: Exclusive OR (XOR) operation

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

IV. PRINCIPLES OF ENCRYPTION & DECRYPTION

A. Encryption principle

The principle of encryption is shown in fig-1. The details of the principle are as below:

Step 1: the key portrait is produced by using the equations 1 and 4

Pixel = [x x 256] …… (4)

Pixel is nothing but the picture element of the main portrait. X in (0, 1) and this is represented as the emphasis value of the PWLCM. The equations 1 and 2 are emphasized for getting the main portrait. The primary value of equation 1 is computed through equation 3. Neighbor picture are believed to be desolately differentiated and one another. For achieving all these requirements, the picture

elements which are acquired by chaos map are the better choice of selection. The picture elements which are produced later will not have any relation with the present one.

Table 3: Addition (+) operation

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

Table 4: Subtraction (-) operation

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

Step 2: The key portrait and the plain portrait are encrypted with respect to the rows along with DNA rules which are pronounced by equation 2 and equation 5.

Rule = $\lfloor x \times 8 \rfloor + 1$ …… (5)

Here rule is the particular arrangement, through which the encoding momentum is dominated. The basic value of the second equation is given by equation 3. The explanation of DNA rules are shown in the first table. Each picture element is encrypted by detailed rules of DNA; distinct rows have distinct rules, as far as all the picture elements of the portrait are encrypted. The number of bits present in each picture element of the gray-scale plain portrait is 8. If taken from the encoding rules of DNA, these 8 bits are partitioned and then encrypted into 4 types of nucleo bases. MxN is assumed as the size of the primary plain portrait, then M is considered as the width, and N is considered as the height. Once the encoding is done row by row, then a new portrait is produced with the size of 4 x M x N.

Step 3: A row by row DNA operations are performed between the plain portrait which is encoded and the encoded key portrait. The described method of DNA functions are persisted by equation 2 and equation 6. Specifications of DNA functions are described in Table 2 to Table 4.

Function= $\lfloor x \times 3 \rfloor + 1 \lfloor x \times 3 \rfloor + 1$ …… (6)

Here the function is the chosen class of DNA function. The verifying operation is accomplished row by row until and unless the encrypted transitional portrait is generated. The three types of DNA functions which are accomplished by preference are (XOR, +, -). The intensity of the in-between picture is 4 x M x N.

Step 4: An encoded in portrayals are decoded for getting the decoded midway picture. The disentangling rule is made with respect to condition 5.By these steps, the user can obtain the basic cipher portrait. Randomly the process of encoding and decoding improve the functioning of the synthesis of the proposed principle. The size of the basic cipher portrait is M x N.

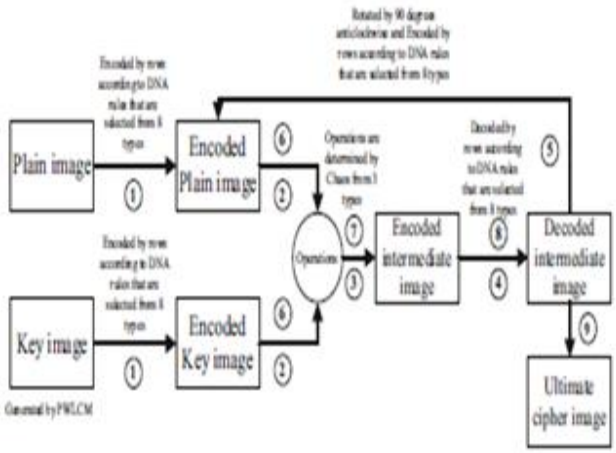

Fig 1: Block diagram of Encryption principle

Step 5: The main cipher portrait is circulated anticlockwise with a degree of 90°. By this anti-clockwise process, one can achieve the latest plain portrait which can be applied for the next step. Through this functioning, the principle proposed can be simplified effectively.

Step 6: Continue the step 4 and 5 until and unless the final cipher portrait is obtained.

B. Decryption principle

The inverse method of encryption principle is mentioned as decryption principle. The user has to concentrate on various methods while doing the process of decryption. Mainly directions to play out the turn around movement of the subtraction. Before the figure portraits are decoded by the receivers, they shall include previously possess the keys which are applied for encrypting the plain portraits, which can diffuse prior than the cipher portraits. The steps which are taken for decoding the portraits are:

Step 1: The cipher portrait is encoded with respect to the accurate inverse operation which attributes to conditions chronicled in step 4 of "Encryption principle".

Step 2: The user has to produce the key portrait and Encoded cipher portrait. For clear understanding refer to initial step and second step in the "Encryption Principle".

Step 3: The encoded key portrait and the encoded cipher portrait are applied for producing the in-between portrait. The particular working is chronicled in the third step of the "Encryption Principle". The three major operations applied in this process are DNA XOR, DNA Addition, and DNA subtraction. The faultless tasks which are significantly connected in the decoding rule are DNA XOR and DNA addition. The DNA XOR and DNA Addition matrices are symmetric matrices. The refinement should be done for the DNA Subtraction for achieving the specifications of DNA rules.

Step 4: The encoded in-between portrait is decoded by using step 3 for obtaining the decoded portrait.

Step 5: The decoded portrait which is obtained from step 4 is rotated anti-cock wise with an angle of 90°. Then the required cipher portrait is obtained from the plain portrait which is encrypted one circle by rows.

Step 6: The stage 1 to stage 4is done continuously until the plain portrait is obtained.

V. REVERSIBLE DATA HIDING BY HISTOGRAM MODIFICATION

A. Reversible data hiding process

The principle to be conferred is majorly for the gray-level portraits but they are protracted effectively to color portraits [15]. The gray level portrait is present with a bit rate of 8 and that portrait is represented. The calculation of portrait histogram is done by computing the picture element by using a gray-level value j for $j \in \{0, 1, 2 \dots 254, 255\}$. h_i is used for representing the count of picture elements with a value j. assuming that, I is having N different picture element characters. Then N nonempty bins are observed in h_I, through which the two highest bins are selected and the complimentary low and high values are represented with I_S and I_R, cooperatively. For a picture element which is tallied in h_I with the charge I, data sinking is accomplished with,

$$i' = \begin{Bmatrix} i-1 & for\ i < I_s \\ I_s - b_k & for\ i = I_s \\ i & for\ I_s < i < I_r \\ I_r + b_k & for\ i = I_r \\ i+1 & for\ i > I_r \end{Bmatrix}$$

i' = the modified picture element value

b_k = k-th message hidden information

By implementing the above equation on each picture element value is counted in h_I, finally, the binary elements which are embedded are $h_I(I_S) + h_I(I_R)$. The bounding values are absent in I, N+2 bins are present in the altered histogram. The bins which are present in between the two summits remains unaltered while the external ones have fluctuated outwards so that each of the summits is divided into two opposite bins (i.e I_S-1 and I_S, I_R and I_R-1) respectively.

The summit values I_S and I_R required to be implemented to excerpt the embedded information. One way of maintaining them is to refuse the 16 picture elements in I from the histogram ascertaining. The least critical bits are to be hidden. After using the equation to each picture element which are processed in h_I for data which is embedded, the peak values are used for the purpose of replacing the least significant bits of the 16 refused picture elements through bitwise functioning. For getting the data which is embedded, the summit values are to be recollected and the marked image i' histogram value is calculated by eliminating the 16 picture elements which are mentioned before. Then the operation below is performed on any picture element which is counted in the histogram with the values of $I_S - 1$, I_S, $I_R, and\ I_R - 1$:

$$b'_k = \begin{Bmatrix} 1 & for\ i' = I_s - 1 \\ 0 & for\ i' = I_s \\ 0 & for\ i' = I_r \\ 1 & for\ i' = I_r + 1 \end{Bmatrix}$$

b_k^I = k-th parallel worth which is taken from the checked picture

The operation which worked on every picture element calculated in the histogram for the purpose of recovering the authentic portrait is shown below. This original image will not have 16 picture elements of least significant bits which are produced from the derived binary values. The forbidden picture elements are reestablished by scripting them back for the purpose of recovering the primary portrait.

$$i = \begin{Bmatrix} i'+1 & for\ i' < I_s - 1 \\ I_s & for\ i' = I_s - 1\ or\ i' = I_s \\ I_r & for\ i' = I_r\ or\ i' = I_r + 1 \\ i'-1 & for\ i' > I_r + 1 \end{Bmatrix}$$

B.Preprocess for the entire recovery

The pixel values of 0 and 255 are to be modified as the data range of uint8 does not support numbers less than 0 and more than 255. The common procedure is to make all the pixel values from 0 to 1 and 255 to 254 respectively. But this process results in errors while decryption of the data. Hence, in this paper, the algorithm is modified by ignoring the pixels having the values 0 and 255. The data hiding through histogram modification is done on the third and fourth highest peaks. This makes the exact recovery of the encrypted cover image.

VI. EXPERIMENTAL RESULTS

The input medical images selected for the analysis are presented in figures 2 (a) – (d).

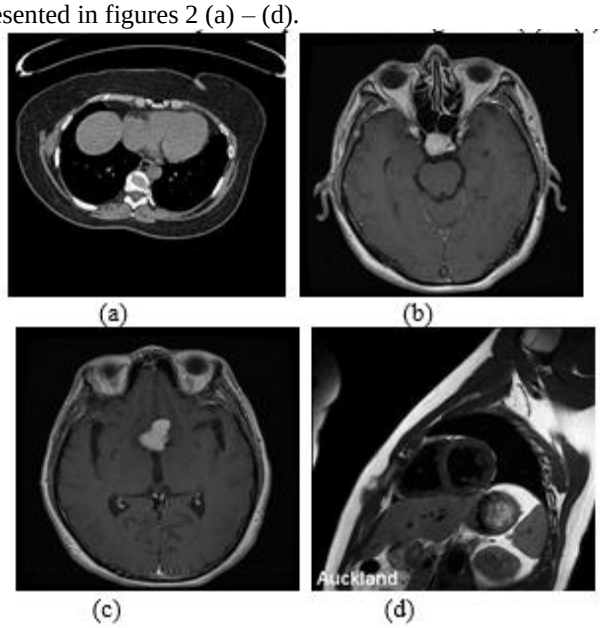

Fig. 2. Input Images

The histogram of the images shown in figure 2 (a) to (d) are presented in figure 3 (a) – (d).

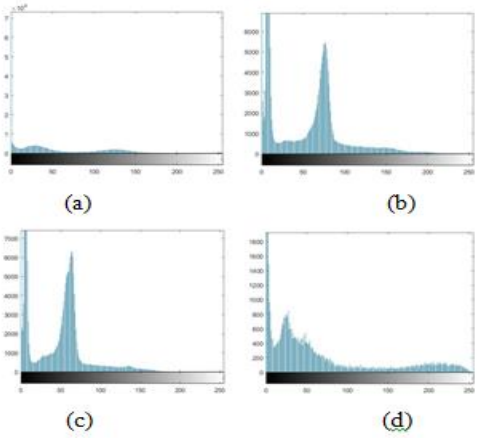

Fig. 3. Input Image histogram

The encrypted outputs are displayed in the figure 4: (a) – (d).

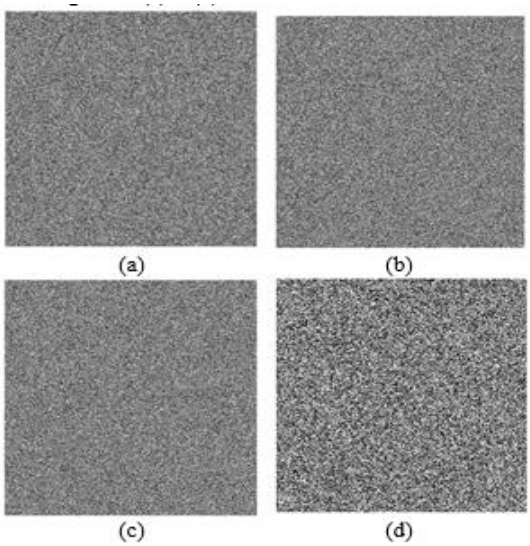

Fig. 4. Encrypted image output

The histogram of the encoded pictures is appeared in the figure 5 (a) – (d). The change in the pictures is exceptionally high contrasted with ordinary calculations.

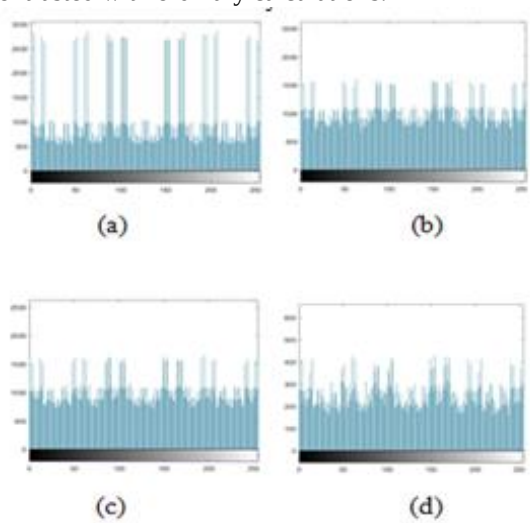

Fig.5 Histogram of encrypted images

The final Decrypted images are shown in figure 6.

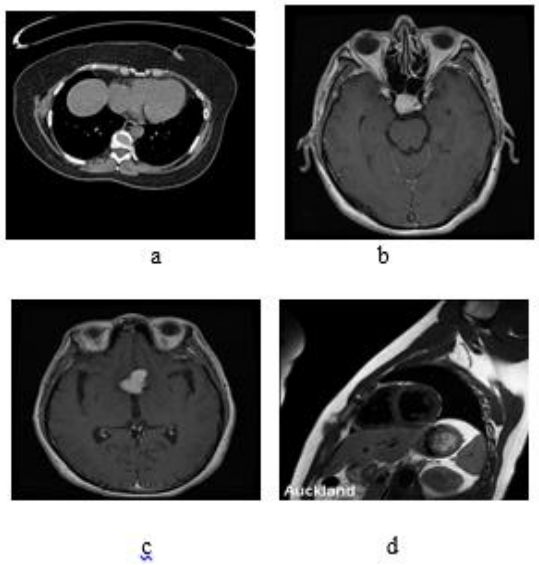

Fig. 6. Decrypted output Images

The correlation index (Corr2) measures the similarity of the input images with the output encrypted images. The table 1 represents the correlation index of the images considered for experiments. The proposed algorithm provides better encryption compared to the existing algorithms.

S.No.	Image	SHA256	Chaotic encryption	Proposed Method
1	2 (a)	0.0013	0.0029	0.000435
2	2 (b)	0.004	0.0038	0.0010
3	2 (c)	0.0029	0.003	0.000869
4	2 (d)	0.0023	0.005	0.0017

VII. CONCLUSION

The paper presents a robust medical image encryption scheme with reversible data hiding. When conventional data hiding techniques are employed with encryption algorithms, the quality of the resultant decrypted image degrades if the cover data is not recovered with complete accuracy. The novel concept employed in this paper fuse the concept of PWLCM is fused with DNA encryption and reversible data hiding. This increases the security of the image along with providing robustness in recovering the cover media perfectly.

REFERENCES

1. Çavuşoğlu, Ü.,Kaçar, S., Zengin, A., Pehlivan, I.: A story cross breed encryption figuring reliant on clamor and S-AES estimation. Nonlinear Dyn. 92(4), 1745–1759 (2018)
2. Akash Kumar Mandal, Chandra Parakash and Mrs. Archana Tiwari, "Execution Evaluation of Cryptographic Algorithms: DES and AES", IEEE Students' Conference on Electrical, Electronics and Computer Science, pp. 1-5, 2017.
3. Zhou, N.R., Chen, W.W., Yan, X.Y., Wang, and Y.Q.: Bit-level quantum covering picture encryption plot with quantum cross-exchange movement and hyper-scattered system. Quantum Inf. Technique. 17, 1–24 (2018)

4. Zhu, H., Zhang, X., Yu, H., Zhao, C., Zhu, Z.: An image encryption count subject to compound homogeneous hyper-confused structure. Nonlinear Dyn. 89(1), 61–79 (2017)
5. Li, C., Luo, G., Qin, K., Li, C.: An image encryption plan subject to furious tent guide. Nonlinear Dyn. 87(1), 127–133 (2017)
6. X. Chai, Y. Chen, and L. Broyde, "A Novel Chaos-based Image Encryption Algorithm using DNA Sequence Operations," Optics and Lasers in Engineering, Vol. 88, pp. 197-213, 2017
7. X.Wang and C. Liu, "An epic and rational picture encryption estimation subject to unrest and DNA encoding," Multimedia Tools Appl. 1–17 (2017).
8. D. Ravichandran, P. Praveenkumar, J. B. B. Rayappan, and R. Amirtharajan, "DNA perplexity blend to check therapeutic security," IEEE Trans. Nanobiosci., vol. 16, no. 8, pp. 850–858, Dec. 2017, doi: 10.1109/TNB.2017.2780881.
9. K. Zhan, D. Wei, J. Shi, and J. Yu, "Cross-utilizing hyperchaotic and DNA groupings for picture encryption," J. Electron. Imag., vol. 26, no. 1, p. 013021, Jan. 2017.
10. Y. Zhang and Y. Tang, "A plaintext-related picture encryption estimation reliant on perplexity," Multimedia Tools Appl., vol. 77, no. 6, pp. 6647–6669, Mar. 2018.
11. Suri S, Vijay R (2018) A synchronous weaving chose control DNA approach for covering picture encryption. J Ambient Intell Hum Comput. DOI: 10.1007/s12652-018-0825-0
12. Ghebleh M, Kanso A, Stevanović D (2017) A story picture encryption figuring reliant on piecewise straight perplexed maps and least squares prompt. Sight and sound Tools Appl 77:1–22
13. Anusudha K, Venkateswaran N, Valarmathi J (2016) Secured suffering picture watermarking with dna codec. Multimed Tools Appl:1–22
14. X. Wang and C. Liu, "A story and effective picture encryption computation reliant on confusion and DNA encoding," Multimedia Tools Appl., vol. 76, no. 5, pp. 6229–6245, 2017.
15. H.- T. Wu,J.- L Dugelay, Y.- Q. Shi, "Reversible picture data stowing away with remarkable perfection improvement", IEEE Signal Process Lett., vol. 22, no. 1, pp. 81-85, Jan.

AUTHORS PROFILE

Smita Khond, Research Scholar, Computer Science Engineering, Pacific Academy of Higher Education and Research University, Udaipur, Rajasthan.
Email Id: smitakhond2009@gmail.com
Dr. Bellamkonda Vijayakumar, Professor and HOD, Computer Science Engineering, Vidya Jyothi Institute of Technology, Hyderabad, India.
Email Id: vijaysree.b@gmail.com