A Novel Approach for Medical Image Encryption Using Multiple Chaotic Maps and DNA Diffusion Operations

Sumangala Biradar[a,*], **Prema T. Akkasaligar**[b,**], **and Sunanda Biradar**[a,***]

[a] *Department of CSE(Artificial Intelligence and Machine Learning), BLDEA's V.P. Dr. P. G. Halakatti College of Engineering and Technology, Vijayapur, Karnataka, 586103 India*

[b] *Department of Computer Science and Engineering, KLE Technological University's Dr. M.S. Sheshgiri College of Engineering and Technology, Belagavi Campus, Belgaum, Karnataka, 590006 India*

** e-mail: biradarsumangala@gmail.com*

*** e-mail: premasb@rediffmail.com*

**** e-mail: sunanda_biradar@rediffmail.com*

Abstract—Due to advancement in electronic interaction, the broadcast of a medical image is very common. The electronic interaction is open to very one and hence, it is risk for medical image communication. The communication of medical image through opensource network adds uncertain risk of undesirable effect and causes important disease related facts in the image being lost or corrupted. For medical practitioner, diagnosing the correct disease from the lost or corrupted medical image. Hence high-level security and verifying integrity is very essential. A new cryptosystem based on DNA cryptography and multiple high dimensional chaotic maps and SHA-256 is proposed to deliver high-level security and verify integrity. The medical image is divided into two subimages. The subimages are converted into DNA synthesis using dynamic DNA coding rules. The hash keys are generated for both DNA synthesis using SHA-256. The Chen's chaotic sequences are utilized to permute the pixels of DNA synthesis of subimage one. Another DNA synthesis of subimage two are permuted using Lorenz chaotic sequences. The hash keys are XORed with chaotic sequences. The DNA diffusion operation diffuses the pixels of the DNA synthesis. The dynamic DNA decoding rules are used to get cipher image. The simulation outcomes prove that the proposed cryptosystem is suitable to provide high-level security and integrity. The cryptanalysis confirms that proposed system is invulnerable to various types of attacks.

Keywords: DNA cryptosystem, Chen's hyperchaotic map, Lorenz system, medical images, SHA-256

DOI: 10.1134/S1054661825700026

1. INTRODUCTION

The broadcasting medical images via a wireless network is vital in e-health system. The wireless network is a public network, hence exposed to crypto attacks. The medical image security is crucial to avert these attacks. Hence, providing high-level security and verifying integrity are major issues in digital medical health systems. The new medical image encryption system is necessary to fulfil the security, confidentiality and integrity requirements of medical records.

The traditional cryptography methods based on mathematical procedures are secure for text and for normal images and insecure for medical images. The medical image pixels are highly correlated and very large in data volume. Hence, chaos theory-based encryption methods appeal to researchers widely. The chaos theory has good confusion and diffusion property. The chaos theory produces pseudo random sequence and very sensitive to initial conditions [19]. The chaotic sequence generation depends on initial conditions. Hence it is inadequate to brute force attack. The new emerging technique called deoxyribonucleic acid (DNA) method is founded in cryptography.

DNA cryptography is an emerging field in cryptography. It is attracting researcher due it is nonbreaking uniqueness property. Hence it is appropriate for secure broadcast of medical images [26]. The computational cost for the construction of biological DNA structure is very complex. Hence only DNA sequences are in use to provide security, which is not satisfactory. To overcome from these inconsistencies, proposed system concentrates on a blend of chaotic system and DNA cryptography.

The main objectives of the proposed cryptosystems are as follows.

Enhancement of security for medical images. The complex confusion of multiple chaotic maps and uniqueness of DNA operations will enhance the security. We have proposed high-level encryption method

Received December 13, 2021; revised December 28, 2024; accepted February 3, 2025

based on multiple chaotic maps and DNA operations to enhance the security of medical images.

Integrity and confidentiality for medical images. The hash key is used to provide the integrity and confidentiality for medical images.

2. RELATED WORK

The DNA cryptography and chaotic systems to communicate a medical image securely through insecure channel is in immature stage.

In [22], Ismail et al. have put forth a generalized double humped (GDH) method for pseudorandom number key generation (PRNG). This key is combined with a chaotic map range to obtain a cipher image. The AES algorithm uses too simple algebraic structure and uses a short key of size 56 bits. In [15], the 1D chaotic map with lightweight operations are used to get cipher image. An inward spiral scanning pattern (round-robin fashion) is utilized to shuffle the index of the pixels. Because of the limited key space, the 1D chaotic map is vulnerable to exhaustive search attacks.

In [9], Chen et al. have presented both encryption and compression methods simultaneously. The secret compressed sensing (CS) is obtained from structurally random matrix (SRM) method to compress the medical image. The 3D Arnold cat map generates a keystream to confuse and diffuse the pixels of the compressed medical images. In [6], Brindha has suggested "AES-GCM (Advanced Encryption Standard-Galois Counter Mode)" method for encryption and validation. This method produces cipher images for confidentiality. The whirlpool hash function generates 512-bit hash code and embeds in images to check the integrity.

In [20], the chaotic logistic map and DNA mapping rules generates a DNA mask. A genetic algorithm is used to get a best DNA mask. The patient electronic reports are embedded in a DNA mask to get the watermark image. In [23], the medical image pixels are rearranged using a hybrid chaotic shift transform and diffused using a modified Henon map. In [16], Li et al. have presented "Hybrid Chaotic Shift Transform" (HCST). It performs permutation diffusion operation using sine map. In [14], Hua et al. have proposed the bitwise XOR along with modulo operations for pixel adaptive diffusion. The diffused pixels generate a cipher image. In [1], Ahmad and Hwang have presented XOR and ADD logical methods to jumble the image pixels, and affine transformation to get a cipher image. In [7], Chai et al. have presented the memristive hyperchaotic process to generate a cellular automaton. The hash function SHA-256 generates a hash key and provides preliminary values for the hyperchaotic system. The dynamic DNA mapping rules are applied to create a DNA encoded structure. A memristive hyperchaotic sequence shuffles the pixels of the DNA structure. The cellular automata method generates the encrypted image.

In [10], Chen and Hu have presented Arnold mapping and wavelet transform to shuffle the pixels of the image. The Kent mapping generates control parameters for Arnold mapping. The shuffled image pixels are XORed with control parameters of Arnold mapping to encrypt an image. In [11], Enayatifar et al. have suggested a DNA rules to get a DNA encoded matrix and the 3D chaotic map to shamble the pixels. The DNA XOR operation is utilized to generate an encrypted image.

The overview of a few additional existing techniques are emphasized in Table 1. Most of the encryption techniques specified in above survey, does not ensure the high-level security, integrity, and confidentiality for medical images. Therefore, this survey motivates us to propose a new cryptosystem using SHA-256 for integrity, DNA for security, Chen's hyperchaotic system, and Lorenz's chaotic system for shuffling pixels of the medical image.

The key contribution of the proposed cryptosystem are as follows.

(i) **Highlevel security for medical images.**

The good confusion property of a heterogenous chaotic map, dynamic DNA coding rules, and DNA operations are utilized to provide multilevel security.

(ii) **Increase in the number of secret keys.**

Generation of different keys at each level of the encryption algorithm leads to increase in the key size.

(iii) **Integrity and confidentiality.**

The medical images contain sensitive disease-related information. Hence computation of integrity and confidentiality in the encryption algorithm is provided using SHA-256 function.

(iv) **Security analysis of cryptosystem.**

The security analysis of developed high-level encryption approach for medical images is depends on invulnerabilities to various types of attacks, such as statistical attacks, differential attacks and exhaustive attacks. The image quality is also measured using MSE, PSNR, and entropy.

In the proposed system, the original medical image is transformed into a DNA synthesis using dynamic DNA coding rules to enhance the security. The multiple high dimensional chaotic maps, namely Chen's hyperchaotic map and Lorenz chaotic maps are used to confuse the pixels of DNA synthesis. The pixels of DNA synthesis are altered utilizing DNA XOR operation. The proposed system is resistant against known plaintext, chosen-ciphertext, and known ciphertext attacks. It also invulnerable against brute force attacks due to multiple high dimensional chaotic maps.

The succeeding fragment of the paper is structured as: Section 3 covers the multilevel encryption technique suitable for medical images. Section 4 covers the proposed multiple high dimensional chaotic map

Table 1. Overview of existing techniques

References	Method	Remarks
Sebastian and Delson [5]	RSA method is used to encrypt the MRI image K-means and watershed segmentation are employed to extract tumor details	RSA method takes more time for massive databases, and it requires a third party to verify the reliability
Vallathan et al. [25]	Linde, Buzo, and Gray (LBG) process is employed to obtain an encrypted embedded image	The single-level encryption method
Al-Haj et al.	The electronic codebook (ECB) mode of advanced encryption standard (AES)	The AES algorithm uses too simple algebraic structure and uses a short key of size 56 bits
Anusudha et al. [4]	The wavelet transform method embeds the patient record and logistic map to get a cipher image	The limitation of key size of logistic map

cryptosystem specifications and working process. The simulation outcomes of the proposed system are in Section 5. Section 6 illustrates the cryptanalysis of the medical image encryption method, and the comparison work is carried out in Section 7. The conclusion of the proposed cryptosystem is in Section 8.

3. HIGHLEVEL ENCRYPTION SCHEME

The main fundamentals for the transmission of medical images are security, confidentiality, and integrity. Single-level encryption methods fails in fulfilling the requirements of medical images. Hence, a high-level encryption system is necessary. In high-level cryptosystem, the hash function SHA-256 is employed to verify the integrity and confidentiality requirements. The multiple high dimensional chaotic maps such as Chen's hyperchaotic system, Lorenz chaotic system, and DNA cryptography techniques are used to fulfill the high-level security requirement.

3.1. SHA-256

The medical images contain disease related sensitive disease related facts and the slight variation in medical image produces a critical problem. Hence, integrity is the main requirement for the medical image. The hash function SHA-256 is used for integrity. The SHA-256 is also act as a digital signature which proves confidentiality. The hash function creates a fixed size 256-bit hash key for varying size medical images. The medical image is run by 16 cell blocks with 32 bits in each building block and each cell block involves 64 cycles of operations to produce a fixed length hash key.

A medical image M is divided into (M_1, M_2, ..., M_{16}) each of size 32-bit. The hash key is acquired by using the XOR operation between each cell blocks defined in Eq. (1)

$$\Delta(M) = M_1 \oplus M_2 \oplus \ldots \oplus M_{16}, \tag{1}$$

where $\Delta(M)$ is a hash key of size 256-bit. This hash key is useful in verifying the integrity of the medical image during the transmission through internet.

3.2. Multiple High Dimensional Chaotic Maps

The high dimensional chaotic maps, namely, Chen's hyperchaotic map and Lorenz chaotic maps are suitable to deliver the high-level security for the medical images.

3.2.1. Chen's hyperchaotic map. The Chen's hyperchaotic map generates an extremely complex sequence. Hence, has good confusion property and it is extremely not possible to predict these sequences. Hence, Chen's hyperchaotic map is suitable to secure medical images. The Chen's hyperchaotic system is specified using Eqs. (2)–(5):

$$X_1 = \alpha_0(Y_0 - X_0), \tag{2}$$

$$Y_1 = X_0 Z_0 + d_0 X_0 + \gamma_0 Y_0 - W_0, \tag{3}$$

$$Z_1 = X_0 Y_0 - \beta_0 Z_0, \tag{4}$$

$$W_1 = X_0 + l, \tag{5}$$

where X_0, Y_0, Z_0, and W_0 are state parameters and α_0, β_0, γ_0, and d_0 are control factors. The value of l varies from –0.7 to 0.7.

3.2.2. Lorenz chaotic system. The Lorenz chaos system produces a nondeterministic chaotic sequence. These complex sequences are appropriate to convey high-level security for medical images. The Lorenz chaotic map is specified using Eqs. (6)–(8)

$$p_1 = \sigma(q_0 - p_0), \tag{6}$$

$$q_1 = \rho p_0 - q_0 - p_0 u_0, \tag{7}$$

Table 2. DNA coding rules

Coding rules	G	C	T	A
R_1	01	10	11	00
R_2	10	01	11	00
R_3	00	11	10	01
R_4	11	00	10	01
R_5	00	11	01	10
R_6	11	00	01	10
R_7	01	10	00	11
R_8	10	01	00	11

Table 3. DNA XOR function

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

Table 4. Dynamic selection of DNA coding rules

LSB	000	001	010	011	100	101	110	111
Rules	R_1	R_2	R_3	R_4	R_5	R_6	R_7	R_8

$$u_1 = p_0q_0 - t_0u_0, \tag{8}$$

where p_0, q_0, and u_0 are system variables and $\sigma = 10$, $\rho = 28$, $t = 8/3$ are positive coefficients.

The chaotic sequences generated using multiple chaotic maps depends on initial conditions of system parameters. The variance of initial conditions generates a different chaotic sequence. All chaotic sequences are unique; hence these complex chaotic sequences are suitable to provide security for medical images.

3.3. DNA Diffusion Operations

The DNA synthesis is formed of four nucleotides namely, "Adenine (A)," "Thymine (T)," "Guanine (G)," and "Cytosine (C)" [18]. In DNA synthesis, A and T are complement; also, G and C are complements. In binary 0 and 1 are complement, based on this perception the nucleotides are signified in binary form as '00' and '11'. Hence, we can get 4! = 24 various encoding rules. Due to the computational complexity, only eight encoding rules indulge the complementary base pairing rules as shown in Table 2. These coding rules are used to generate the DNA synthesis for medical images.

The DNA diffusion operation DNA XOR is utilized to diffuse the pixels of DNA synthesis. The DNA XOR operation is illustrated in Table 3.

4. PROPOSED HIGH-LEVEL MULTILPLE CHAOTIC MAP CRYPTOSYSTEM

A high-level multiple high dimensional chaotic map cryptosystem is proposed to offer high-level security, confidentiality and the integrity. The medical images encryption scheme is processed using SHA-256, Chen's hyperchaotic system, Lorenz's chaotic system, and DNA diffuse operations.

In the proposed cryptosystem, the medical image is separated into subimages. The two-hash keys are obtained using hash function SHA-256 for both subimages. The subimages are renovating into an 8-bit binary images. The all DNA coding rules are utilized to attain a DNA synthesizes for both binary images. The DNA coding rules are dynamically selected depending on the value of the pixels of binary image.

4.1. Generation of DNA Synthesis

The DNA synthesis is produced using all DNA coding rules. The least significant bits of 8-bit binary images are utilized to select DNA coding rules dynamically as shown in Table 4.

If the pixel value is "10110110" three LSB is "110," the rule R_7 is chosen. Correspondingly depending on pixel values, all DNA coding rules are employed to obtain a unique DNA synthesis for each medical image.

The multiple chaotic maps are used to permute the pixels of DNA synthesizes. The permuted pixels are diffused using DNA diffusion process.

4.2. Multiple Chaotic Permutation and DNA Diffusion Process

The multiple chaotic permutation process confuses the pixels of a DNA synthesizes. The Chen's chaotic sequences and Lorenz chaotic sequences are assembled in increasing order. The indexes of the sorted sequences are used to confuse the pixels of both DNA synthesizes.

The DNA diffusion process changes the pixel value of DNA synthesizes. The chaotic sequences are also modified using logical XOR between hash keys and chaotic sequences. The DNA XOR operation is applied between the diffused chaotic sequences and permuted DNA synthesizes.

The DNA decoding rules are utilized to renew the DNA synthesizes into a binary image.

Table 5. Dynamic selection of DNA decoding rules

LSB	AA|GA	AT|GT	AG|GG	AC|GC	TA|CA	TG|CG	TC|CC	TT|CT
DNA coding rules	R_1	R_2	R_3	R_4	R_5	R_6	R_7	R_8

4.3. DNA Decoding Rules

The inverse of DNA coding rules are used as a DNA decoding rules. These rules are dynamically applied depending on the least significant bits of the DNA synthesizes, as shown in Table 5.

The binary images are combined and is transformed into a cipher image.

For better understanding the proposed cryptosystem, the encryption scheme is illustrated in detail steps of Algorithm 1.

Algorithm 1: High-level multiple chaotic map cryptosystem

```
//Input: Original medical image O($m \times n$) of size $m$ rows and $n$ columns
//Output: Cipher image E($m \times n$)
Step 1: Start
Step 2: The original medical image O is separated into two subimages $O_1$ and $O_2$.
Step 3: The hash key $k_1$ is produced for $O_1$ and hash key $k_2$ is generated for $O_2$.
Step 4: The subimages $O_1$ and $O_2$ are transformed into 8-bit binary images $B_1$ and $B_2$, respectively.
Step 5: The DNA coding rules are used to convert $B_1$ and $B_2$ into DNA synthesizes $D_1$ and $D_2$, respectively.
Step 6: The hyper chaotic sequences $X$ and $Y$ are produced using Chen's chaotic map.
        The logical XOR is applied between chaotic sequences $X$ and hash key $k_1$.
Step 7: The chaotic sequences $X$ and $Y$ are sorted in increasing order. The index of sorted sequences $\overline{X}$ and $\overline{Y}$ are utilized
        to confuse the pixels of $D_1$.
Step 8: The chaotic sequences $p$ and $q$ are generated using Lorenz chaotic map. The logical XOR is applied between $p$ and
        hash key $k_2$.
Step 9: The Lorenz chaotic sequences $p$ and $q$ are arranged in increasing order. The index of ordered sequences $\overline{p}$ and $\overline{q}$
        are utilized to confuse the pixels of $D_2$.
Step 10: The DNA XOR is used between Chen's chaotic sequence and $D_1$ to diffuse the pixels. Similarly, DNA XOR is
         used between Lorenz chaotic sequence and $D_2$.
Step 11: Renovated DNA synthesizes into a binary image using DNA decoding rules.
Step 12: Binary images are combined to get the cipher image.
Step 13: Stop
```

The medical image is decrypted from the cipher image using the inverse process of Algorithm 1.

The DNA coding rules are used as a secret key at the first level to generate a unique DNA synthesizes. The initial values of state parameters of multiple high dimensional chaotic maps are represented as a secret key in the second and third levels. Further, the DNA XOR and logical XOR operation alter the pixels of a medical image in the fourth level. The hash key is also used as a secret key. The multiple keys are used in multiple levels in the proposed cryptosystem for the enhancement of the security level of medical images.

5. EXPERIMENTAL RESULTS

The experiment is carried out on 9th generation Intel CoreT M i7 7500U CPU @ 2.70 GHz, 2901 MHz, 2 Core(s), 4 Logical Processor(s). The 500 medical images of size 512 × 512 of five different categories (100 medical images from each category) like Ultrasound, MRI, X-ray, and CT from the "National Library of Medicine's Open Access Biomedical Images Search Engine" [17]. The ECG images from "ecgeducator.blogspot.com." The Matlab (R2015b) tool is used to implement the propose cryptosystem. The sample medical images are shown in Fig. 2.

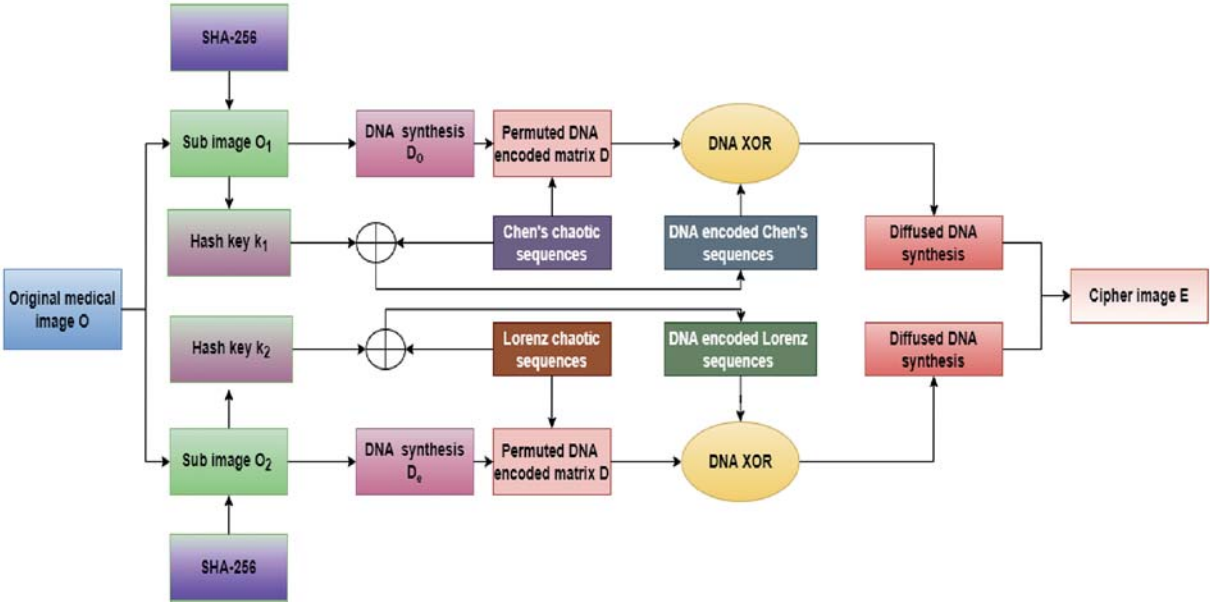


Fig. 1. Proposed high-level multiple chaotic map-based encryption method.

In the proposed method, the original medical image of size 512 × 512 as shown in Fig. 2, is split into a two subimages of size 256 × 256. The hash keys are generated for each subimages. The subimages are renewed into binary images. All eight DNA coding rules are employed to produce a unique DNA synthesis (D_1, D_2) for each subimage separately. The multiple high dimensional chaotic maps, namely Chen's hyperchaotic map and Lorenz chaotic maps, are employed to confuse the pixels of DNA synthesizes. We have considered $X_0 = 0.3$, $Y_0 = –0.4$, $Z_0 = 1.2$, and $W_0 = 1$ as initial values of state parameters in Chen's hyperchaotic map. The primary values of state parameters $\alpha_0 = 0.3$, $\beta_0 = –0.4$, $\gamma_0 = 1.2$, and $d_0 = 1$ are empirically determined to produce a sequence of the chaotic map. In the Lorenz chaos system, $p_0 = 1.2$, $q_0 = 1.2$, and $u_0 = 3.7$ are empirically determined as initial values to get Lorenz chaotic sequence. The multiple chaotic sequences are XORed with hash keys. The sequences of high dimensional chaotic maps are arranged in increasing order, and the DNA synthesizes (D_1, D_2) pixels are shuffled depending on the index of the arranged sequence. The DNA XOR operation is applied to change the pixels of DNA synthesizes. The DNA decoding rules are applied to produce a cipher image as depicted in Fig. 2. The original medical image is decrypted using inverse process of Algorithm 1 depicted in Fig. 2.

To verify the integrity the hash keys of sender are compared with hash keys generated at receiver side. If hash keys of sender is equal to receivers' hash key the integrity is maintained during transmission.

6. PERFORMANCE ANALYSIS

The performance of proposed cryptosystem depends on resistance against different types attacks namely, "statistical attacks," "differential attacks," and "exhaustive attacks." The analysis of correlation coefficient is performed to withstand the statistical attack [24]. The key security and key space analysis performed to resist the exhaustive attack. The entropy analysis is to ascertain the superiority of the medical image. The mean square error (MSE) and peak signal noise ratio (PSNR) are applied to validate the error rate of a medical image.

6.1. Statistical Attack

The statistical attack is performed to evaluate whether it is possible to predict the original image and secret keys by monitoring the dissemination of pixels in the cipher image. The analysis of correlation coefficient and histogram analysis are used to analyze the statistical attack.

6.1.1. Analysis of correlation coefficient. The correlation coefficient analyzes the association among the neighboring pixels of the medical images. The neighboring pixels are strongly associated in the medical images. The attackers study the association between neighboring pixels of cipher image and try to predict the medical image. The coefficient value of the correlation specifies the relation between the neighboring pixels. The smaller value means are inadequately associated among the pixels. Pearson's correlation coefficient is defined using Eq. (9)

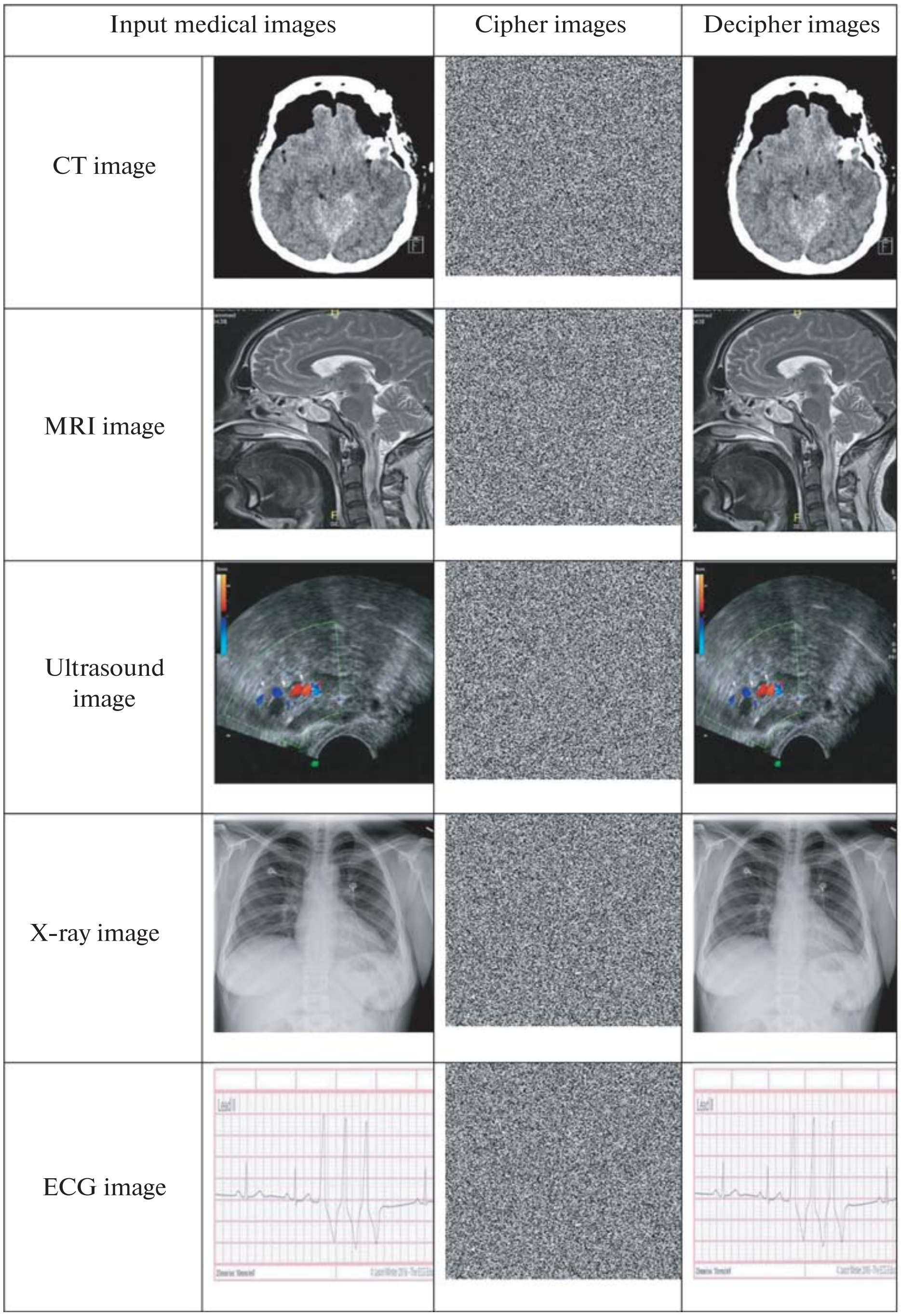


Fig. 2. The sample of medical images.

$$\text{Coeff} = \frac{N\Sigma OE - (\Sigma O)(\Sigma E)}{\sqrt{N\left(\Sigma O^2\right) + (\Sigma O)^2}\sqrt{N\left(\Sigma E^2\right) + (\Sigma E)^2}}, \quad (9)$$

where O and E are the original medical image and cipher image correspondingly, and N is a medical image size [$m \times n$]. The value of Coeff equals +1 means that pixels are correlated positively, and value equals −1 means negatively correlated. The value of Coeff equals zero means no correlation [12, 13].

The correlation coefficient among the original medical image and the decipher image is approximately equal to 0.996 (i.e., approximately equal to 1) is shown in Table 6. The correlation value equal to zero indicates no explicit relationship between medical images. The correlation of the original medical image and the cipher image is almost like –0.009 (i.e., approximately equal to 0) is shown in Table 6. These values prove that there is no association among pixels of cipher images. Hence, for attackers predicting the original medical image from cipher image is impossible.

Table 6. Correlation coefficient of the proposed system

Medical image	Direction	Cipher image	Decipher image
MRI image	Horizontal	0.008	0.994
	Vertical	–0.006	0.997
	Diagonal	–0.004	0.995
CT image	Horizontal	0.005	0.999
	Vertical	–0.010	0.998
	Diagonal	0.009	0.994
X-ray image	Horizontal	0.009	0.998
	Vertical	–0.010	0.997
	Diagonal	–0.011	0.999
Ultrasound image	Horizontal	0.008	0.998
	Vertical	–0.010	0.994
	Diagonal	–0.009	0.996
ECG image	Horizontal	0.008	0.993
	Vertical	–0.013	0.997
	Diagonal	–0.014	0.993

6.1.2. Histogram analysis. The histogram analysis is the illustration of dissemination of pixels, based on gray-scale levels. The histogram of the sample MRI image is shown in Figs. 3a and 3b histogram of cipher image, and in Fig. 3c histogram of decipher MRI image is shown. From Fig. 3, it is examined that the dissemination of pixels is consistent in cipher image, which proves that pixel values of cipher image are totally altered. Hence, the proposed high-level multiple chaotic maps-based encryption method has good confusion property.

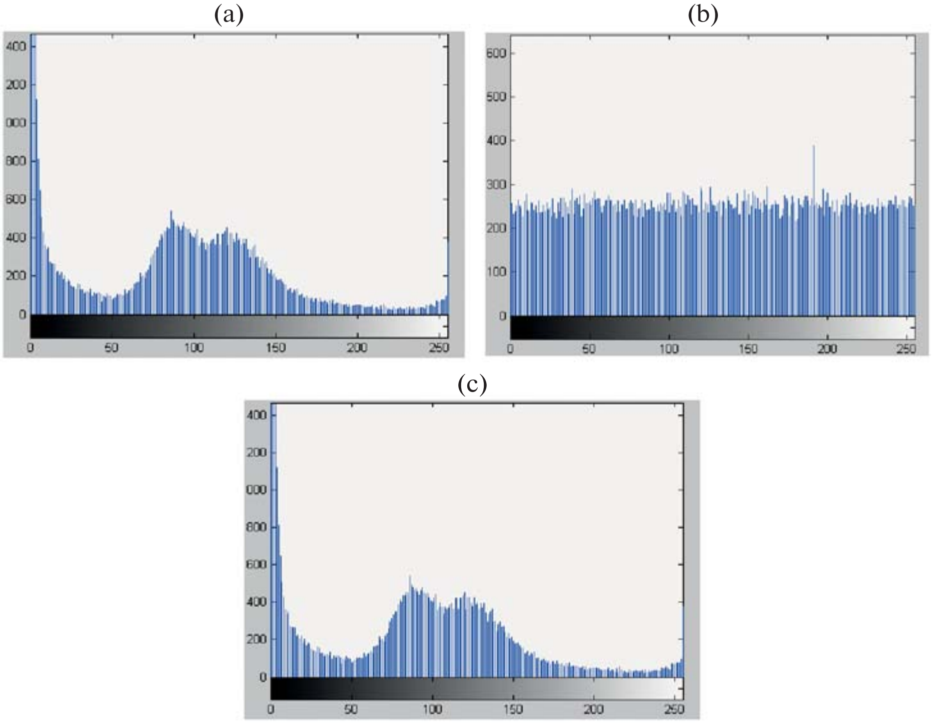
6.2. Differential Attack

The differential attack is used to evaluate resistance against the known ciphertext attack, chosen ciphertext and known plain text attack. The unified average changed intensity (UACI) and number of pixel changing rate (NPCR) methods are used for cryptanalysis.

6.2.1. NPCR and UACI. The intruders choose the cipher texts and secret key and try to get the decipher image. The NPCR is used to verify resistance against very small variance in plaintext. NPCR is defined using Eq. (10)

$$\mathrm{NPCR} = \frac{\sum_{m,n} G_1(m,n)}{W_1 \times H_1} \times 100\%, \tag{10}$$

where W_1 and H_1 are the breadth and length of the medical image, and $G_1(m, n)$ calculation using Eq. (11)


(a)

(b)

(c)

Fig. 3. Histogram of (a) sample MRI image, (b) cipher image, and (c) decipher MRI image.

Table 7. Performance analysis of the proposed system

Medical image	NPCR	UACI	Entropy	MSE	PSNR
MRI image	99.66	33.49	7.999	4.9020e+03	4.8277
CT image	99.66	33.45	7.998	5.5396e+03	5.1010
X-ray image	99.67	33.35	7.999	4.8975e+03	4.0010
Ultrasound image	99.66	33.41	7.999	5.0009e+03	4.1237
ECG image	99.67	33.46	7.999	5.1607e+03	4.6734

$$G_1(m,n) = \begin{cases} 0, & \text{if } E_{11}(m,n) = E(m,n) \\ 1, & \text{if } E_{11}(m,n) \neq E(m,n), \end{cases} \quad (11)$$

The UACI is defined in Eq. (12)

$$\text{UACI} = \frac{1}{W_1 \times H_1} \times \left[\sum_{r,c} \frac{|E_{11}(m,n) - E(m,n)|}{255} \right] \times 100\%, \quad (12)$$

where E is cipher image obtained from an original medical image. The selected 1000-pixel values of an original medical image are changed and encrypted as E_{11}.

6.3. Exhaustive Attack

A crypto analyst performs an exhaustive attack to check whether it can predict the secret keys by brute force search. The key space analysis is to verify an exhaustive attack.

6.3.1. Keyspace analysis. In the proposed system, the initial conditions of system and structure parameters of Chen's hyperchaotic map and Lorenz chaotic system are used as a secret key. A total of fourteen system parameters (X_0, Y_0, Z_0, W_0, α_0, β_0, γ_0, d_0, p_0, q_0, u_0, σ, ρ, and t) and two hash keys are secret keys of multiple levels. "According to the IEEE floating-point standard, the computational precision of the 64-bit double data is 10^{-15}." The key size of ten secret keys is $(10^{15})^{14}$, and the size of the hash key is 256 (2^8) bits. The key space is very large in size. Hence, proposed system key space is significant to survive against exhaustive attack.

6.4. Entropy

The entropy value specifies the significance of superiority of the proposed cryptosystem. The entropy is the probability of dissemination of gray-scale levels throughout the medical image. The superior value of entropy proves the good quality of proposed cryptosystem. The entropy is elucidated using Eq. (13)

$$E(I) = \sum_{i=1}^{n} P(O_i) \log(P(O_i)), \quad (13)$$

where $P(O_i)$ signifies the probability of scattering of the intensity level of the medical image and n signifies an overall intensity level.

6.5. MSE and PSNR

The MSE and PSNR metrics are utilized to validate the error rate of original medical image [24]. The MSE determines the error rate between the original medical image and the cipher. The higher value indicates good cryptosystem. The MSE computes nearly the average of squared errors between the original medical image O and cipher image E. where N is size $[m, n]$. The MSE is defined in Eq. (2)

$$\text{MSE} = \frac{\sum_{N} [O(m,n) - E(m,n)]^2}{N}. \quad (14)$$

The PSNR is to verify the alteration of cipher image due to noise affecting the original medical image. The PSNR is defined in Eq. (15)

$$\text{PSNR} = 10 \log_{10} \frac{(256-1)}{\text{MSE}}, \quad (15)$$

where N is the size ($m \times n$) of the digital medical image [8, 21].

The security analysis of the proposed system is depicted in Table 7. The average NPCR value 99.66 and the average UACI value is 33.43. These values prove that the proposed cryptosystem generates a different cipher image to very minor changes of original medical image. Hence, the proposed method resists against known and chosen plaintext and cipher attacks. The entropy value is 7.999 approximately close to ideal value 8.0 and proves that proposed system is appropriate to deliver high-level security for medical images. The MSE is nearly equal to 5.10014e+03, and PSNR is 4.5453 dB, proves that a medical image's quality is maintained. The security analysis exhibits that the proposed cryptosystem is adequate to convey multilevel security, confidentiality, and integrity for medical images.

Table 8. Comparison of the proposed system with the methods discussed in the literature

Scheme	Size	Entropy	NPCR	UACI
[7]	256 × 256	7.9832	99.66	33.62
[11]		7.9993	99.59	33.41
[23]		7.9993	99.63	33.59
[16]		7.9990	99.62	33.42
Proposed system		**7.9992**	**99.66**	**33.43**
[7]	512 × 512	7.9975	99.51	33.58
[23]		7.9980	99.62	33.45
[16]		7.9990	99.58	28.63
Proposed system		**7.9991**	**99.66**	**33.42**

The two 256-bit hash keys are generated to verify the integrity of the medical image during transmission in the proposed cryptosystem.

7. COMPARISON OF THE PROPOSED METHOD

The proposed system is compared with methods specified in the literature survey [7, 11, 16, 23] for Lena images of different sizes 256 × 256 and 512 × 512. The proposed system's entropy, NPCR, and UACI are almost equal and greater than the other methods, as shown in Table 8. Hence it proves that the performance and efficiency of the proposed cryptosystem are high enough and superior for medical images. The time efficiency of the proposed cryptosystem is O (8 mn).

8. CONCLUSIONS

In this paper, the high-level encryption method for medical image using a SHA-256, multiple chaotic map chaotic maps, and DNA diffusion operation is proposed. Primarily, the original medical image is divided into two subimages. The hash keys are generated for both subimages using SHA-256. The subimages are converted into binary images. The binary images are transformed into a DNA synthesis at the first level. Both DNA synthesis pixels are jumbled using Chen's hyperchaotic sequence, and Lorenz chaotic sequences in the second and third levels. The logical XOR operation is used between the chaotic sequences and hash keys in fourth level. The DNA XOR operation is employed to diffuse the pixels of both DNA synthesis in fifth level. The DNA decoding rules are used to get the cipher images in the last level. The simulation results demonstrate that the proposed high-level cryptosystem enhances the security, validates integrity and proves confidentiality. The originality of the proposed system is to afford high-level security, confidentiality, and integrity using SHA-256, DNA coding rules, and multiple high dimensional chaotic maps. The cryptanalysis shows that the proposed method is resistant against known ciphertext, known plaintext, statistical, exhaustive, and differential attacks. The proposed cryptosystem is applicable for e-health systems and telemedicine applications.

FUNDING

This work was supported by ongoing institutional funding. No additional grants to carry out or direct this particular research were obtained.

CONFLICT OF INTEREST

The authors of this work declare that they have no conflicts of interest.

REFERENCES

1. J. Ahmad and S. O. Hwang, "A secure image encryption scheme based on chaotic maps and affine transformation," Multimedia Tools Appl. **75**, 13951–13976 (2016). https://doi.org/10.1007/s11042-015-2973-y
2. P. T. Akkasaligar and S. Biradar, "Automatic segmentation and analysis of renal calculi in medical ultrasound images," Patern Recognit. Image Anal. **30**, 748–756 (2020). https://doi.org/10.1134/S1054661820040021
3. A. Al-Haj, N. Hussein, and G. Abandah, "Combining cryptography and digital watermarking for secured transmission of medical images," in *2016 2nd International Conference on Information Management (ICIM), London, 2016* (IEEE, 2016), pp. 40–46. https://doi.org/10.1109/INFOMAN.2016.7477531
4. K. Anusudha, N. Venkateswaran, and J. Valarmathi, "Secured medical image watermarking with DNA codec," Multimedia Tools Appl. **76**, 2911–2932 (2017). https://doi.org/10.1007/s11042-015-3213-1
5. A. Sebastian and T. R. Delson, "Secure magnetic resonance image transmission and tumor detection techniques," in *IEEE International Conference on Circuit, Power and Computing Technologies (ICCPCT), Nagercoil, India, 2016* (IEEE, 2016), pp. 1–5.
6. M. Brindha, "Confidentiality, integrity and authentication of DICOM medical images," in *2018 2nd International Conference on Inventive Systems and Control (ICISC), Coimbatore, India, 2018* (IEEE, 2018), pp. 71–75. https://doi.org/10.1109/icisc.2018.8398924
7. X. Chai, Zh. Gan, K. Yang, Yi. Chen, and X. Liu, "An image encryption algorithm based on the memristive hyperchaotic system, cellular automata and DNA sequence operations," Signal Process.: Image Commun. **52**, 6–19 (2017). https://doi.org/10.1016/j.image.2016.12.007

8. C. S. Chan, C. C. Chang, and Y. C. Hu, “Image hiding scheme using modulus function and optimal substitution table,” Patern Recognit. Image Anal. **16**, 208–217 (2006). https://doi.org/10.1134/s1054661806020076

9. J. Chen, Yu. Zhang, L. Qi, Ch. Fu, and L. Xu, “Exploiting chaos-based compressed sensing and cryptographic algorithm for image encryption and compression,” Opt. Laser Technol. **99**, 238–248 (2018). https://doi.org/10.1016/j.optlastec.2017.09.008

10. X. Chen and C.-J. Hu, “Medical image encryption based on multiple chaotic mapping and wavelet transform,” Biomed. Res. **28**, 9901–9004 (2017).

11. R. Enayatifar, A. H. Abdullah, I. F. Isnin, A. Altameem, and M. Lee, “Image encryption using a synchronous permutation-diffusion technique,” Opt. Lasers Eng. **90**, 146–154 (2017). https://doi.org/10.1016/j.optlaseng.2016.10.006

12. P. S. Hiremath, P. T. Akkasaligar, and Sh. Badiger, “An optimal wavelet filter for despeckling echocardiographic images,” in *International Conference on Computational Intelligence and Multimedia Applications (ICCIMA 2007), Sivakasi, Tamilnadu, India, 2007* (IEEE, 2007), pp. 245–249. https://doi.org/10.1109/iccima.2007.227

13. P. S. Hiremath, P. T. Akkasaligar, and Sh. Badiger, “Speckle reducing contourlet transform for medical ultrasound images,” International Journal of Computer and Information Engineering **5** (8), 932–939 (2011).

14. Zh. Hua, Sh. Yi, and Yi. Zhou, “Medical image encryption using high-speed scrambling and pixel adaptive diffusion,” Signal Process. **144**, 134–144 (2018). https://doi.org/10.1016/j.sigpro.2017.10.004

15. S. Janakiraman, K. Thenmozhi, J. B. B. Rayappan, and R. Amirtharajan, “Lightweight chaotic image encryption algorithm for real-time embedded system: Implementation and analysis on 32-bit microcontroller,” Microprocessors Microsyst. **56**, 1–12 (2018). https://doi.org/10.1016/j.micpro.2017.10.013

16. B. Li, X. Liao, and Ya. Jiang, “A novel image encryption scheme based on logistic map and dynatomic modular curve,” Multimedia Tools Appl. **77**, 8911–8938 (2018). https://doi.org/10.1007/s11042-017-4786-7

17. National Library of Medicines Open Access Biomedical Images Search Engine. https://openi.nlm.nih.gov

18. S. F. Nimmy, M. G. Sarowar, N. Dey, A. S. Ashour, and K. C. Santosh, “Investigation of DNA discontinuity for detecting tuberculosis,” Journal of Ambient Intelligence and Humanized Computing **15**, 1149–1163 (2024). https://doi.org/10.1007/s12652-018-0878-0

19. B. Norouzi, S. M. Seyedzadeh, S. Mirzakuchaki, and M. R. Mosavi, “A novel image encryption based on hash function with only two-round diffusion process,” Multimedia Syst. **20**, 45–64 (2014). https://doi.org/10.1007/s00530-013-0314-4

20. Q.-A. Kester, L. Nana, A. Ch. Pascu, S. Gire, J. M. Eghan, and N. N. Quaynor, “A cryptographic technique for security of medical images in health information systems,” Procedia Computer Science **58**, 538–543 (2015). https://doi.org/10.1016/j.procs.2015.08.070

21. A. Rasmi, B. Arunkumar, and V. M. Anees, “A comprehensive review of digital data hiding techniques,” Patern Recognit. Image Anal. **29**, 639–646 (2019). https://doi.org/10.1134/s105466181904014x

22. S. M. Ismail, L. A. Said, A. G. Radwan, A. H. Madian, and M. F. Abu-Elyazeed, “Generalized double-humped logistic map-based medical image encryption,” J. Adv. Res. **10**, 85–98 (2018). https://doi.org/10.1016/j.jare.2018.01.009

23. S. J. Sheela, K. V. Suresh, and D. Tandur, “Image encryption based on modified Henon map using hybrid chaotic shift transform,” Multimedia Tools Appl. **77**, 25223–25251 (2018). https://doi.org/10.1007/s11042-018-5782-2

24. S. P. Vaidya, P. V. S. S. R. Ch. Mouli, and K. C. Santosh, “Imperceptible watermark for a game-theoretic watermarking system,” Int. J. Mach. Learn. Cybern. **10**, 1323–1339 (2019). https://doi.org/10.1007/s13042-018-0813-x

25. G. Vallathan, G. G. Devi, and A. V. Kannan, “Enhanced data concealing technique to secure medical image in telemedicine applications,” in *2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, India, 2016* (IEEE, 2016), pp. 186–190. https://doi.org/10.1109/wispnet.2016.7566117

26. Q. Wang, Q. Zhang, and Ch. Zhou, “A multilevel image encryption algorithm based on chaos and DNA coding,” in *2009 Fourth International on Conference on Bio-Inspired Computing, Beijing, 2009* (IEEE, 2009), pp. 1–5. https://doi.org/10.1109/BICTA.2009.5338154

Publisher's Note. Pleiades Publishing remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.
AI tools may have been used in the translation or editing of this article.

Dr. Sumangala Biradar is working as Head and Associate Professor in Department of CSE (Artificial Intelligence and Machine Learning), BLDEA's V.P. Dr. P.G. Halakatti College of Engineering and Technology, Vijayapur, Karnataka, India. She has completed her Bachelor of Engineering from Visvesvaraya Technological University Belagavi, Karnataka, India in the year 2002. M.Tech. (CSE) from Visvesvaraya Technological University, Belagavi, Karnataka, India in 2011 and completed PhD in 2023 from Visvesvaraya Technological University, Belagavi, Karnataka, India. Her areas of interest are Machine learning, Information Security, and Cryptography. She has published papers in reputed and peer reviewed International Journals and conference proceedings. She has also received research fund from Vision Group of Science and Technology (VGST), Karnataka.

Dr. Prema T. Akkasaligar is working as Professor in Department of Computer Science and Engineering, KLE Technological University's Dr. M.S. Sheshgiri College of Engineering and Technology, Belagavi Campus, Belgaum, Karnataka, India. She has completed her Ph.D. from Gulbarga University, Gulbarga in 2013, ME(CSE) from Gulbarga University, Gulbarga in 1999. She has published 9 book chapters, 24 international journals, 20 international conference papers and 3 national conference papers. Selected for National Level AICTE–UKIERI Technical Leadership Development Programme for the year 2019–2020 and received CMI Level 5 certificate from Government of United Kingdom. She has received the Karnataka state level Award for Research Publications (ARP) by Vision Group of Science and Technology (VGST), Department of Information Technology, Biotechnology and Science and Technology, Government of Karnataka, for the year 2019–2020. She is an Executive council member of IEEE North Karnataka subsection, member of Board of Examiners (BOE) of Visveswaraya Technological University, Belagavi for the year 2018–2019, member of Department Advisory Board (DAB) for various prestigious Engineering colleges of North Karnataka. She has received Highest Research Publications of the year 2018 awarded by BLDEA's VP Dr. PGH Engineering College, Vijaypur. Appreciation certificate by LEAD programme of Deshpande foundation on account of International Womens Day 2019. BEST Publisher of the Department for the year 2017–2018 awarded by BLDEA's VP Dr. PGH Engineering College, Vijaypur. BRONZE certificate by Income Tax Department for the year 2016–2017, 2017–2018, and 2018–2019. She is guiding several research scholars under VTU, Belagavi. She is life member of Computer Society of India (CSI), Indian Society for Technical Education (ISTE), The Institution of Engineers, India (IEI), and International Association of Computer Science and Information Technology (IACSIT), Singapore. She has been a resource person in several workshops and FDPs. She has completed several research project sanctioned by KBITS Incubation centre Karnataka, VTU-FOSS Belagavi. Her areas of interest are Medical image processing and Computer vision.

Dr. Sunanda Biradar is working as Associate Professor in Department of CSE (Artificial Intelligence and Machine Learning), BLDEA's V.P. Dr. P.G. Halakatti College of Engineering and Technology, Vijayapur, Karnataka, India. She has completed her Bachelor of Engineering from Visvesvaraya Technological University Belagavi, Karnataka, India in the year 2002. M.Tech. (CSE) from Visvesvaraya Technological University, Belagavi, Karnataka, India in 2009 and PhD from Visvesvaraya Technological University, Belagavi, Karnataka, India in 2021. Her areas of interest are medical image processing and pattern recognition. She has more than 15 research publications in reputed and peer reviewed international journals, conference proceedings, and book chapters. She has also received research fund from Vision Group of Science and Technology (VGST), KBITS, Govt. of Karnataka and KSCST, Karnataka.