Multimed Tools Appl (2018) 77:8393–8418
DOI 10.1007/s11042-017-4741-7

Transreceiving of encrypted medical image – a cognitive approach

Padmapriya Praveenkumar[1] · N. Kerthana Devi[1] ·
Dhivya Ravichandran[1] · J. Avila[1] · K. Thenmozhi[1] ·
John Bosco Balaguru Rayappan[1] ·
Rengarajan Amirtharajan[1]

Received: 3 September 2016 / Revised: 15 April 2017 / Accepted: 20 April 2017 /
Published online: 29 April 2017

Abstract Recently, there is an increasing demand for efficient and secure transreception of medical images in telemedicine applications. Though a fixed spectrum is allocated to each user, most of the time it remains unused by the concerned user. Cognitive Radio (CR) is a technology that utilizes the unused spectrum efficiently by adopting spectrum sensing concept. This paper proposes an efficient and secure transmission of medical images by adopting CR technology and image encryption technique. Firstly, the novel medical image encryption algorithm is proposed to encrypt the DICOM (Digital Imaging and Communications in Medicine) image effectively. Then, the spectrum sensing technique is carried out via Universal Software Radio Peripheral (USRP) to sense the unused frequency band to transmit the encrypted bio signal. The proposed encryption algorithm combines DNA (Deoxyribo Nucleic Acid) sequence operation and chaotic maps to successfully encrypt the DICOM image pixels. Experimental results are done and various analysis such as Unified Average Changing Intensity (UACI), Number of Pixel Changing Rate (NPCR), entropy estimation and chi-square tests are carried out to validate the sternness of the encryption algorithm.

Keywords Image encryption · DNA · Chaotic maps · Cognitive radio · USRP

1 Introduction

With the advancement in the field of telecommunication and medicine, the need for sharing the medical data files has increased drastically. Security is concerned to be the significant problem while transferring the medical files in real time medical applications such as telemedicine.

✉ Rengarajan Amirtharajan
amir@ece.sastra.edu

[1] School of Electrical & Electronics Engineering, SASTRA University, Thanjavur 613 401, India

Therefore, there is an emerging need for ensuring the security of patient data files. Cryptography is a discipline of mathematics and computer science that provides numerous security services. Advanced Encryption Standard (AES), Data Encryption Standard (DES) are the traditional encryption algorithms to encrypt the text files. These encryption schemes are less suited or less efficient to encrypt the bulk DICOM images since they require large computational overhead [24, 33].

A variety of conventional encryption schemes has been employed to encrypt the medical images [8, 10, 24, 29, 30]. Recently, chaos-based cryptography has attracted many researches to develop efficient algorithms to conceal the secret information [17, 33, 38]. A chaotic system is a nonlinear system known for its strong properties like very high dependency on the control parameters and initial condition, topological transitivity and the density of the periodic points [5, 17, 28]. Chaos is a branch of study that is highly focused on dynamic systems. This concept has been employed in information security for a variety of reasons. Highly sensitive to initial conditions, ergodicity, random progression of sequences, etc. are some of the features of such chaotic based systems. Chaotic attractors [31] and maps [3] have found a significant role in encryption of images.

Chaotic maps are governed through a single or set of mathematical equations. These maps have been constructed using single or more variables. There are many maps found in literature on one dimensional and two-dimensional platforms [3]. 1D maps yield good model of chaotic systems, where the phase plane is stretched in a one-dimensional pattern on a single axis [6]. Some of the commonly used 1D maps are a logistic map, tent map, sawtooth map, etc. These maps have a random pattern generation model based on the control parameters and initial conditions. However, a combination of 1D chaotic maps can be employed in image encryption applications to improve the keyspace.

In order to exploit the complex random behaviour of chaotic signals, multidimensional chaotic maps have been suggested [3, 6, 7, 9]. The one step ahead of the 1D chaotic map is a 2D chaotic map wherein more than one variable control the chaotic system. Some of the 2-D chaotic maps are Bakers map, Henon map, Arnolds map, etc. These chaotic maps are well suited for confusion as well as diffusion operations during the encryption of secret images [7, 9].

Similarly, DNA computing is another emerging field to store and transmit the information. DNA has the advantage of high storage and massive parallelism, and thus it matches the demand of image encryption [12, 19, 37]. Few works have been reported in the literature which combines DNA sequence and chaotic sequences to encrypt the digital and medical images [36].

Jain and Rajpal have proposed an image encryption scheme based on DNA sequence, 1D and 2D chaotic maps [13]. Two matrices are generated from 1D logistic map to perform DNA addition and complementary operation. Finally, block shuffling is performed with 2D logistic sequences. Zhen et al. have combined DNA sequence, 1D logistic and spatiotemporal system to effectively encrypt the digital image [39]. DNA coding and addition operations are based on the sequences generated from the logistic system; spatiotemporal system permutes the image before decoding. Liu et al. have developed an image encryption algorithm based on the logistic system, chen system and DNA sequence [27]. Li et al. have proposed the color image encryption scheme employing real and complex chaotic system [21]. Hamming distance generated from the plain image and key 1 are used to generate key 2 which is then utilized for scrambling the color plane pixels [26]. Guesmi et al. have projected the improved scheme to enhance the information entropy based on DNA sequence operation, Lorentz attractor and SHA 2 algorithm [11]. In [18], a noise resistive image encryption scheme based on piecewise linear chaotic map (PWLCM), logistic map and DNA sequence are proposed. 128-bit hash is calculated from the plain image to select the DNA rule and control parameters of chaotic maps [25].

The electromagnetic spectrum is a natural resource. Due to the increase in population, this natural resource has become limited and crowded. Usually, the spectrum is allocated to each user statically. Due to the static allocation, the spectrum might be unutilized by the certain users for a prolonged time. In order to efficiently utilize the unused resources, Cognitive Radio (CR) technology has come into existence [1, 2]. It has reduced the scarcity of spectrum to a greater extent by employing dynamic allocation scheme. In cognitive radio concept, by using spectrum sensing technique, sensing is done to detect the presence of secondary user [4, 35]. On the other hand, spectrum management calculates how long the user can work in the spectrum of the primary user and finally spectrum sharing is the sharing of the spectrum with the secondary user. Spectrum mobility is used to maintain the requirements of communication during transition.

Inspired from the above discussion, the cognitive radio concept can be well utilized to reuse the unused radio spectrum to transreceive the medical images efficiently in real-time telemedicine applications. However, as mentioned earlier, security will be the primary concern for achieving the efficient trans-reception of medical files [32]. Hence, this paper proposes a novel approach to combine the CR concept and image encryption algorithm to transmit the bio-inspired biomedical images efficiently and securely. The proposed approach comprises two phases namely, security phase and transreception phase. In the security phase, a Quadra layer security scheme is designed based on DNA and chaotic sequences [14–16, 20, 22, 23, 34, 40]. In the second phase, spectrum sensing concept is used to effectively transmit the encrypted medical image.

2 Methodology

The proposed approach has two phases namely, security phase and transreception phase. In the security phase, a four level security scheme based on DNA encoding, DNA addition and subtraction, 1D logistic map and PWLCM map is proposed [34]. In the transreception phase, the spectrum sensing concept using cognitive radio is utilized to efficiently transreceive the encrypted medical image.

2.1 Security phase

The overall working model of the encryption algorithm is shown in Fig. 1.

2.1.1 DNA coding

DNA sequence composes four bases namely Adenine (A), Guanine (G), Thymine (T) and Cytosine (C). Among these bases, A and T are complementary, G and C are complementary to each other. Watson and Crick [37], framed a structure in which one member of a pair of bases must always be a purine, and the other should be pyrimidine to bridge the two chains in DNA structure. Hence, the following conditions prevail:

- Adenine can only pair with thymine, and guanine only with cytosine.
- A and T are complementary. Similarly, G and C are complementary.

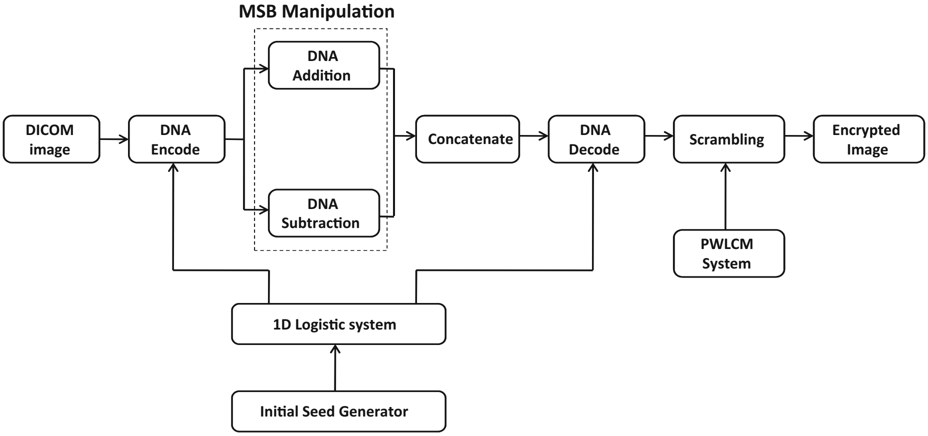


Fig. 1 Block diagram of proposed image encryption algorithm

In a binary system 0 and 1 are complementary; similarly, 00 and 11, 10 and 01 are complementary to each other. By mapping the 2-bit binary system to the DNA bases, one can obtain 24 set of rules. Since the alignments of these sequences which coincide with binary complementary rule were proposed by Watson, the suggested rule was called Watsons Cricks Complementary rule. A can bond only with T and C can bond only with C.

However, among those 24 rules only 8 rules satisfy the Watson crick's complementary rule.

Hence, the DNA-based computing ends with 8 set of encoding and decoding rules [34] as depicted in Tables 1, 2, 3, 4, 5. Using these rules the image pixel value can be encoded into equivalent DNA bases. Using Watson's complementary rule, A can bond with T and C with G only.

Considering C = 00, A = 01, T = 10, G = 11, the encoding and decoding rules are given in Table 5.

With the advancement of DNA computing, some algebraic operations are created based on DNA bases. In order to enhance the diffusion effect, the DNA addition and subtraction rules are derived as shown in Tables 6 and 7 respectively.

Table 1 DNA bonding rules

1	C A ― T G	5	A G ― C T
2	C T ― A G	6	A C ― G T
3	G A ― T C	7	T G ― C A
4	G T ― A C	8	T C ― G A

Table 2 Watson crick's complementary rule

1	C(00)	G(11)	A(01)	T(10)	5	A(00)	T(11)	C(01)	G(10)
2	C(00)	G(11)	A(10)	T(01)	6	A(00)	T(11)	C(10)	G(01)
3	G(11)	C(00)	A(01)	T(10)	7	A(11)	T(00)	C(01)	G(10)
5	G(11)	C(00)	A(10)	T(01)	8	A(11)	T(00)	C(10)	G(01)

2.1.2 Proposed image encryption algorithm

Step 1: Read the DICOM image of size 256 × 256.

Step 2: Logistic map is defined by,

$$X_{n+1} = r \times X_n(1 - X_n),$$

where r is the control parameter, and X_0 is the initial condition. To be chaotic the value of r should lie in the interval (3.57, 4) and X in the range of (0, 1).

Let 'n' be the user defined positive integer key value. Set the initial conditions and control parameters to the 1D logistic map and iterate the map upto n iterations. After n iterations, allow the chaotic system to iterate for extra 2 times.

$X = \{S_{n+1}, S_{n+2}\}$, S_{n+m} is m^{th} element in the chaotic sequence X.

Step 3: Quantize the sequence using the following equation,

$$Xq = \left\{ \left(X^{*} 10^{14} \right) \, mod \, 8 \right\}$$

Step 4: Out of 8 encoding rules, select the particular rule set from Tables 1, 2, 3, 4, and 5 using the first element from the quantized chaotic sequence Xq. Encode the plain DICOM pixels into corresponding DNA bases using the selected rule as in [34].

Step 5: The DNA-encoded matrix of size 256 × 256 × 8 is divided into two blocks B1 and B2. DNA addition and subtraction operations are performed in B1 and B2 respectively.

Step 6: Few methods have employed the DNA addition/ subtraction operation to diffuse the image pixels [7, 9]. In these methods, all the bits of image pixels are employed in diffusion process which may increase the computational overload. In order to reduce the computational overhead, the proposed method diffuses only the Most Significant Bit (MSB) and Least Significant Bit (LSB). The new MSB of cipher pixel is obtained by using DNA addition/subtraction operation on MSB and LSB of DNA encoded matrix.

Step 7: Out of 8 decoding rules, select the particular rule set from Tables 1, 2, 3, 4 and 5 using the second element from the quantized chaotic sequence Xq. Using the selected rule, decode the DNA base into corresponding decimal value to get the diffused cipher image [34]. The process from step 1 to step 7 are explained in Fig. 2.

Table 3 Binary addition in DNA

00 + 00 = 00	00 + 10 = 10	00 + 01 = 01	00 + 11 = 00
10 + 00 = 10	10 + 10 = 00	10 + 01 = 11	10 + 11 = 00
01 + 00 = 00	01 + 10 = 11	01 + 01 = 10	01 + 11 = 00
11 + 00 = 00	11 + 10 = 01	11 + 01 = 00	11 + 11 = 10

Table 4 Binary subtraction in DNA

00–00 = 00	00–10 = 10	00–01 = 11	00–11 = 01
10–00 = 10	10–10 = 00	10–01 = 01	10–11 = 11
01–00 = 01	01–10 = 11	01–01 = 00	01–11 = 10
11–00 = 11	11–10 = 01	11–01 = 10	11–11 = 00

Step 8: The mathematical expression of PWLCM is

$$x_{i+1} = \left\{ \begin{array}{cc} x_i/P_0 & 0 \le x_i < p_0 \\ (x_i/P_0)/(0.5-P_0) & p_0 \le x_i < 0.5 \\ (1-x_i) & x_i \ge 0.5 \end{array} \right\}$$

where x_0 € (0,1), when the control parameter P_0 lies in the interval (0,0.5) the system behaves chaotic.

Iterate the above equation upto 256 × 256 times, sort the obtained sequences in ascending order to get the sorted sequence. Map the pixels based on the sorted sequence to get the final encrypted image. Figure 3a and b show the 1D logistic map bifurcation diagram for 50 and 1000 iterations respectively. Similarly, Fig. 3c and d shows the 2D Henon map bifurcation diagram for 50 and 1000 iterations respectively. From the figures, it is clear that 2D map takes advantage of complexity and randomness as the number of iterations becomes more.

Figure 4a and b represents the bifurcation diagram of logistic map for 100 and 1000 iterations respectively for Xn Vs X(n + 1). Figure 4c and d represents the bifurcation diagram of logistic map for 100 and 1000 iterations respectively for X(n + 1) Vs r. From the figures, it is clear that randomness of the logistic map has become more complex as increasing the number of iterations.

For example, to generate permutation matrix of size 128 × 128, the logistic map is iterated 1000, 1500 and 2000 times. Let r = 3.989 and Xn = 0.449, then the output of the logistic map equals.

$$\begin{aligned} \mathrm{X(n+1)} = \{ & 0.987, 0.052, 0.195, 0.627, 0.933, 0.251, 0.749, 0.749, \\ & 0.749, 0.749, 0.75, 0.749, 0.75, 0.747, 0.754, 0.74, 0.767, \\ & 0.712, 0.817, 0.595, 0.961, 0.15, 0.508, 0.997, 0.012, 0.047, \\ & 0.179, 0.587, 0.967, 0.128, 0.445, 0.985, 0.059, 0.221, 0.687, \\ & 0.857, 0.489, 0.997, 0.013, 0.051, 0.193, 0.621, 0.938, 0.231, \\ & 0.708, 0.825, 0.576, 0.974, 0.1, 0.36, 0.919, 0.297, 0.834, \\ & 0.553, 0.986, 0.055, 0.209, 0.659, 0.896, 0.371, 0.931, \\ & 0.257, 0.762, 0.724, \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{aligned}$$

Table 5 DNA encoding and decoding rules

1	2	3	4	5	6	7	8
10-C	10-A	10-A	10-C	10-G	10-T	10-T	10-G
00-A	00-C	00-G	00-T	00-T	00-G	00-C	00-A
11-T	11-G	11-C	11-A	11-A	11-C	11-G	11-T
01-G	01-T	01-T	01-G	01-C	O1-A	01-A	01-C

Table 6 DNA addition

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

After sorting the values in ascending order, the new indices of these values will be used to fill the permutation matrix.

$$\begin{aligned} Y = \Big\{ & 62, 5, 13, 30, 55, 17, 41, 40, 42, 39, 43, 38, 44, 37, 45, 36, 47, 34, 48, 28, \\ & 57, 10, 24, 64, 1, 3, 11, 27, 13\ 58, 9, 22, 60, 7, 15, 32, 51, 23, 63, 2, 4, 12, \\ & 29, 56, 16, 33, 49, 26, 59, 8, 20, 53, 19, 50, 25, 61, 6, 14, 31, 52, 21, 54, \\ & 18, 46, 35, \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{aligned}$$

Figure 5(a–c) represents the permutation sequence matrix formed from the logistic chaotic sequences after iterating 1000, 1500 and 2000 times respectively. From the figure, it is clear that the randomness of the permutation matrix increases along with the iterations of the logistic map.

2.2 Spectrum sensing using cognitive radio

In the proposed scheme, initial spectrum sensing is done using USRP, and then the unused spectrum is identified to transmit the encrypted biomedical images. The following steps explain the spectrum sensing concept.

Step 1: Initially, a USRP transmitter is acting as a primary user and the receiver USRP will be performing sensing of the primary data.
Step 2: From the available spectrum, the unused spectrum is sensed using energy detector technique as follows:

- The received signal is represented as $y(n) = s(n) + w(n)$ where s (n) is the signal to be detected and w (n) is the Additive White Gaussian Noise and n is the index.
- The metrics used in the energy detector is $M = \sum_{n=0}^{N} |y(n)|^2$ where ‘N’is the size of the vector and the decision metric M is compared with the threshold value λ_E
- The probability of detection P_D and the probability of false alarm P_F can be used to analyze the performance of the detection algorithm.

Table 7 DNA subtraction

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

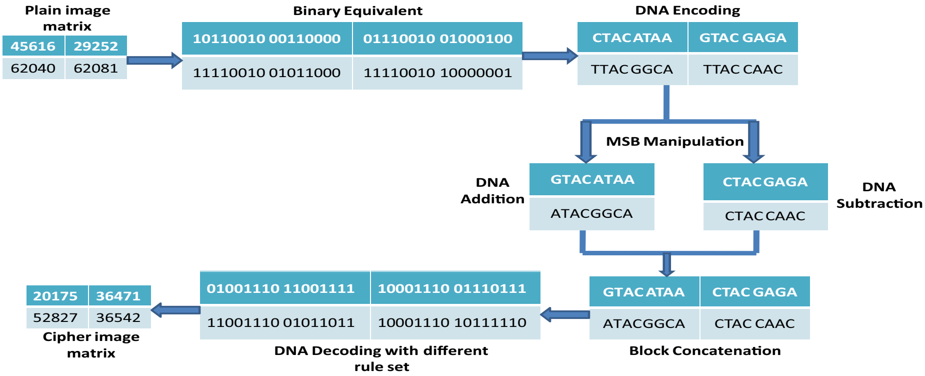
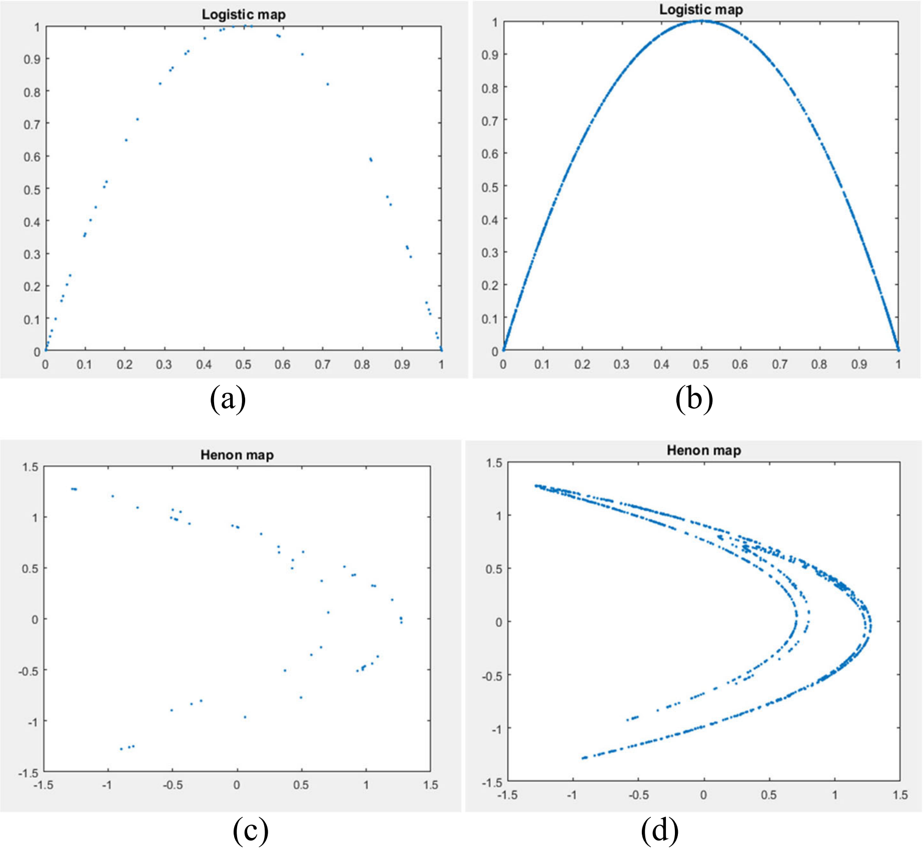


Fig. 2 Illustration of proposed diffusion process

- The probabilities are given by $P_D = 1 - \tau\left(L_f L_t, \frac{\lambda_E}{\sigma_\omega^2}\right)$ and $P_F = 1 - \tau\left(L_f L_t, \frac{\lambda_E}{\sigma_\omega^2 + \sigma_s^2}\right)$ where λ_E is the threshold and τ (a, b) is the incomplete gamma function.



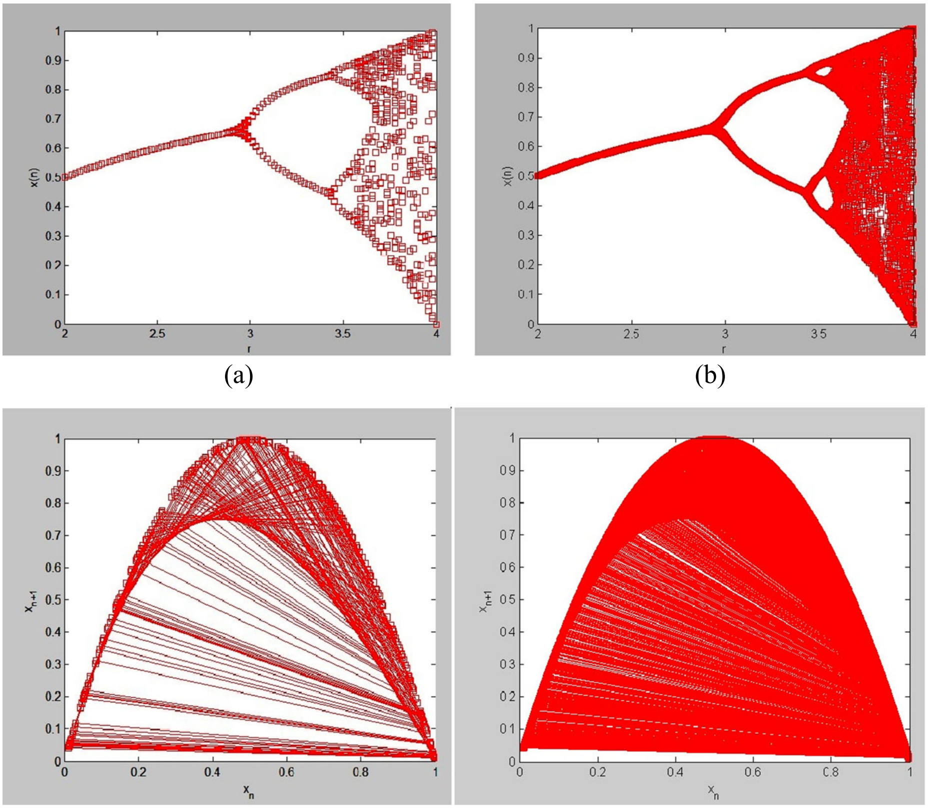
(a)

(b)

(c)

(d)

Fig. 3 **a** 1D logistic map iterated for 50 times, **b** 1D logistic map iterated for 1000 times. **c** 2D Henon map iterated for 50 times, **d** 2D Henon map iterated for 1000 times

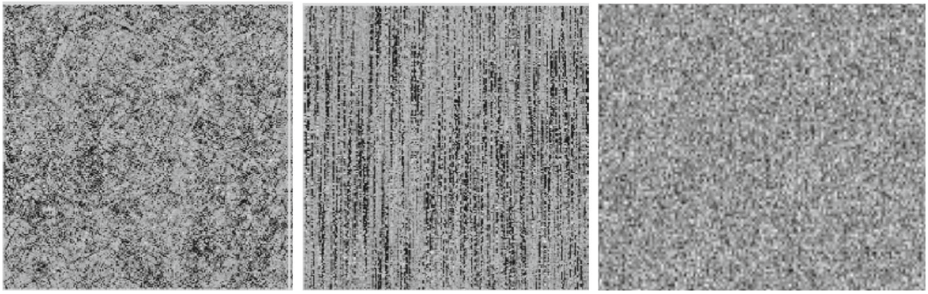


(a) (b)

(c) (d)

Fig. 4 **a** and **b** bifurcation diagram of logistic map for Xn Vs X(n + 1) for 100 and 1000 iterations respectively. c and d bifurcation diagram of logistic map for X(n + 1) Vs r for 100 and 1000 iterations respectively

Step 3: The value of P_D should be greater and the value of P_F should be smaller. When the above condition is satisfied the spectrum is free to transmit the encrypted bio-inspired signal, else the sensing is done until the condition is satisfied. The whole process is explained in Fig. 6.



(a) (b) (c)

Fig. 5 **a**–**c** Permutation matrix formed from chaotic sequences after 1000, 1500 and 2000 iterations

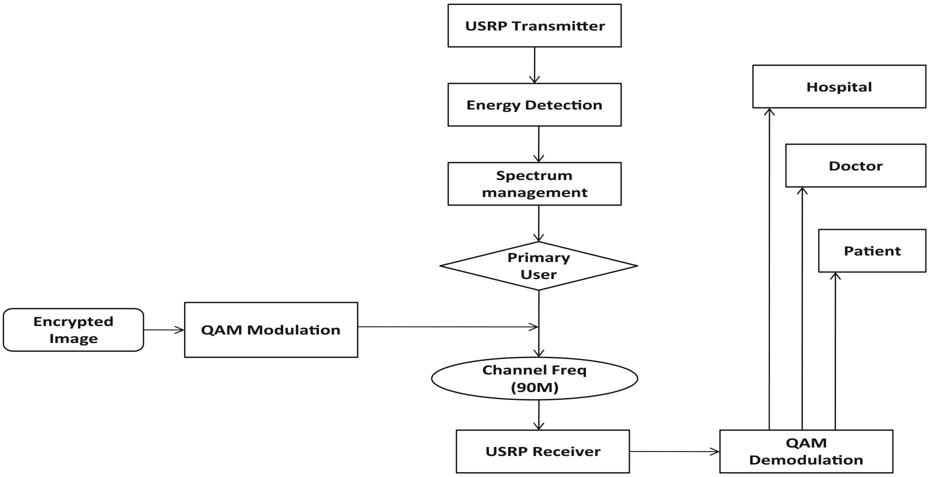


Fig. 6 Block diagram of the proposed scheme

The RX1 antenna is used in USRP transmitter with 15 dB as gain and the frequency bandwidth of 88MHZ – 100 MHZ. The spectrum is analyzed as portrayed in Fig. 7(a and b). It shows that the primary user is present at 94 MHZ and other frequencies are considered as spectrum holes. A 98 MHZ is selected as the suitable frequency spectrum in order to avoid interference from the primary user.

3 Results and discussions

This section presents and analyzes the experimental results of both medical image encryption and effective transreception. The proposed algorithm is analyzed by using five test images. The test CT and MRI DICOM images of size 256 × 256 and 512 × 512 are shown in Fig. 8(a–e). In order to validate the robustness of the proposed medical image encryption algorithm, various tests such as statistical, differential, key sensitivity, cropping, noise attack analyses have been performed.

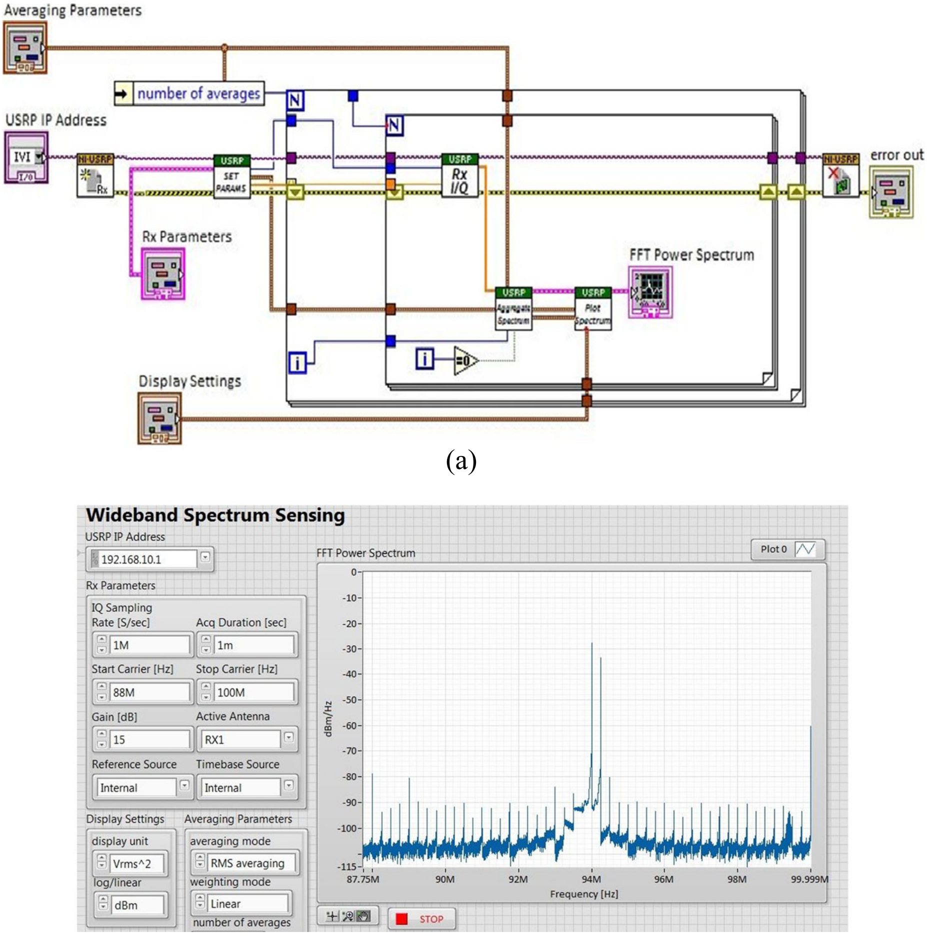
MR-1 image of size 256 × 256 and the various stage outputs are shown in Fig. 9(a–d).

3.1 Statistical analysis

This analysis can be proven by estimating histogram, chi-square test, and histogram deviation, deviation from ideality, entropy and correlation coefficients of the cipher image.

3.1.1 Histogram analysis

Histogram analysis is the graphical representation of the number of pixels and the gray scale level. The original image, its histogram and the histogram of the encrypted image are shown in Fig. 10 (a–c) respectively. The perfectly encrypted image should have the flat histogram. From



(a)

Wideband Spectrum Sensing

USRP IP Address: 192.168.10.1

Rx Parameters

IQ Sampling Rate [S/sec]: 1M
Acq Duration [sec]: 1m
Start Carrier [Hz]: 88M
Stop Carrier [Hz]: 100M
Gain [dB]: 15
Active Antenna: RX1
Reference Source: Internal
Timebase Source: Internal

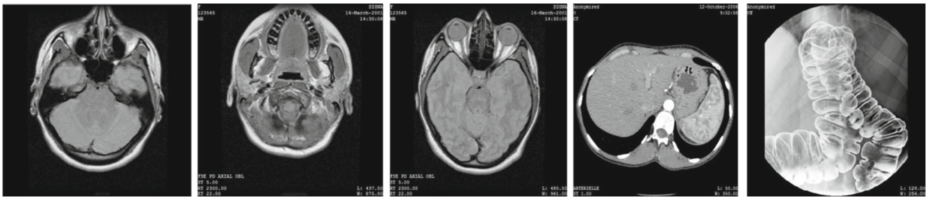
Display Settings
display unit: Vrms^2
log/linear: dBm

Averaging Parameters
averaging mode: RMS averaging
weighting mode: Linear
number of averages

(b)

Fig. 7 **a** Block diagram of spectrum analyzer; **b** Front panel of spectrum analyzer

the Fig. 10, it is clear that the histogram of the encrypted image is flat which means the pixels are uniformly distributed at all the gray levels. From this, it is evident that it is very hard to estimate the statistical relationship between the pixels.



(a) (b) (c) (d) (e)

Fig. 8 Test images: **a** MR-1of size 256 × 256; **b** CT-2 of size 256 × 256; **c** CT-3 of size 256 × 256; **d** MR-2 of size 512 × 512; **e** MR-3 of size 512 × 512

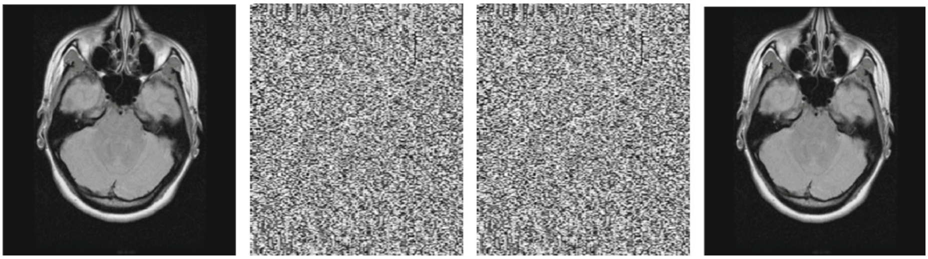

(a) (b) (c) (d)

Fig. 9 **a** Input DICOM image; **b** Combined image; **c** Encrypted image; **d** Decrypted image

3.1.2 Chi-square test

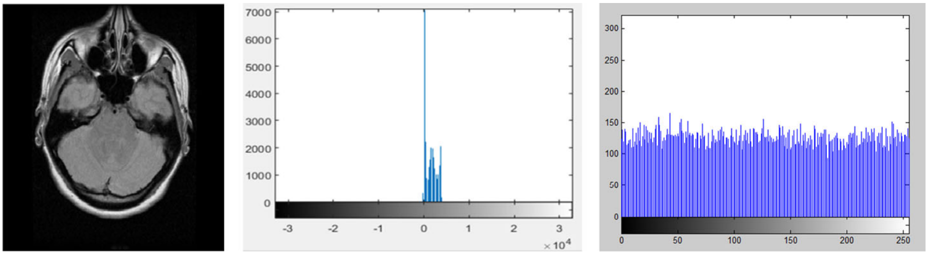
Chi-square test is a very important and significant non-parametric test. It is based on calculating the difference between the observed and the expected value to estimate the statistical value of the uniform distribution of pixels in the encrypted image. This can be calculated using the formula given below,

$$\chi 2=\sum_{i=1}^{256}\frac{(O(i)-E(i))^2}{E(i)}$$

Where, O is the histogram value of the observed cipher image, and E is the histogram value of the ideally encrypted image. The chi-square distribution value of the test images of size 256 × 256 and 512 × 512 are given in Table 8. The test values with degrees of freedom equal to 255 and probability of 0.95, the theoretical, critical value is 293.2478. From Table 8, the chi-square distributions of all the test image values are below the theoretical value which confirms that the proposed encryption scheme achieves uniform distribution of cipher pixels.

3.1.3 Histogram deviation analysis

This section presents the quantitative analysis of the deviation in histogram between the original and the encrypted image. As the name implies, the deviation value should be large



(a) (b) (c)

Fig. 10 Histogram Analysis: **a** Input image; **b** Histogram of (**a**); **c** Histogram of the encrypted image

Table 8 Chi-square test analysis

Test images	$\chi 2 = \sum_{i=1}^{256} \frac{(O(i)-E(i))^2}{E(i)}$	Decision
MR_1 (256 × 256)	270.1406	Accept
CT_2 (256 × 256)	263.9567	Accept
CT_3 (256 × 256)	264.6298	Accept
MR_2 (512 × 512)	241.5664	Accept
MR_3 (512 × 512)	233.8320	Accept

to achieve the better encryption standard. This analysis can be carried out by adapting the following equation,

$$\text{Deviation} = \left(\frac{\frac{D0 + DL}{2} + \sum_{i=1}^{L-1} D_i}{M \times N} \right)$$

where, D is the absolute difference of the observed cipher histogram from the original histogram of the image of size M × N.

3.1.4 Deviation from ideality analysis

Deviation from ideality measures the deviation of the encrypted image from the ideally encrypted histogram. This value should be as low as possible to achieve better encryption. The histogram deviation and the deviation from ideality values are tabulated in Table 9. From the Table 9, it is clear that the histogram deviation values are higher and the deviations from ideality values are smaller for all the test images which prove the robustness of the proposed encryption scheme.

3.1.5 Correlation analysis

The correlation between the adjacent pixels in the plain image should be equal to 1and for the encrypted image it should be equal to 0. The proposed algorithm achieves the above criterion which is shown in Table 10. Also, the correlation between the adjacent pixels is calculated in all horizontal, vertical and diagonal directions. The Fig. 11(a–c) illustrates the pixel distribution of the original plain image in all

Table 9 Deviation analysis measure

Test images	Histogram deviation	Deviation from ideality
MR_1 (256 × 256)	23,230	0.5020
CT_2 (256 × 256)	23,502	0.4826
CT_3 (256 × 256)	23,127	0.5193
MR_2 (512 × 512)	102,325	0.9844
MR_3 (512 × 512)	102,586	0.9724

Table 10 Correlation values of the test images

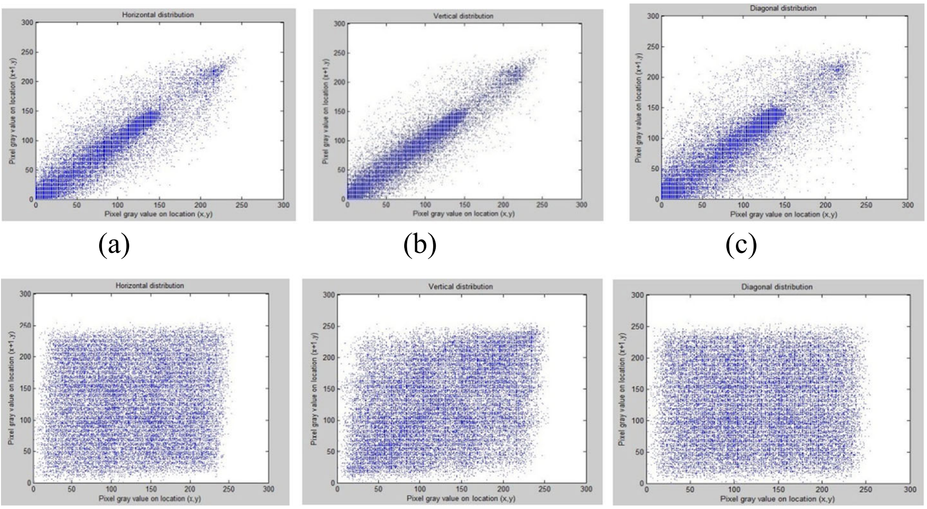
METRICS	VC	DC	HC
MR_1 (256 × 256)	−0.0193	0.0091	0.0682
CT_2 (256 × 256)	0.0091	0.0964	0.0756
CT_3 (256 × 256)	−0.8452	0.0078	0.2567
MR_2 (512 × 512)	−0.2355	0.0054	0.0056
MR_3 (512 × 512)	0.4687	0.0942	0.7342

directions. Figure 11(d–f) illustrates the pixel distribution of the encrypted image. The correlation coefficient is calculated by the following formula,

$$Cor(x_1, x_2) = \frac{E[x_1 - E(x_1))(x_2 - E(x_2))]}{\sigma_{x_1}\sigma_{x2}}$$

where E(x) is the expected value of x and σ_x is the standard deviation of x.

From the Fig. 11, the pixels value are concentrated in horizontal, vertical and diagonal directions for the original test image MR_1 and is uniformly distributed over the entire region for the encrypted image. The estimated table values are closer to zero which reveal that there exists no correlation between the adjacent pixels of the encrypted images in all the three directions. Hence, the statistical relationship between the neighboring pixels are totally broken which means the algorithm has high immunity to defend statistical attacks.



(a) (b) (c)

(d) (e) (f)

Fig. 11 Pixel distribution analysis: **a** Horizontal pixel distribution of original image; **b** Vertical pixel distribution of original image; **c** Diagonal pixel distribution of original image; **d** Horizontal pixel distribution of encrypted image; **e** Vertical c pixel distribution of encrypted image; **f** Diagonal pixel distribution of encrypted image

3.1.6 Information entropy

Global Shannon entropy is used to test the randomness and robustness of the encrypted image. It can be measured by the following equation

$$H(x) = -\sum_{i=1}^{L} p(x_i)_2^{\log} p(x_i)$$

where p(x_i) is the probability of the symbol x_i. The maximum entropy is "n" for a random image with 2^n symbols. The global Shannon entropy is not the perfect measure to find the randomness of the encrypted image [33]. To overcome this local Shannon entropy is calculated. It is estimated by choosing K random blocks in the encrypted image and calculating the entropy of each individual blocks and taking an average of the obtained entropies. Table 11 estimates the global, as well as local entropy considering 40 random blocks, in both the cases; the values, are closer to 8 which reveal the randomness the proposed encryption scheme.

3.2 Differential analysis

Number of Changing Pixel Rate (NPCR) and Unified Averaged Changed Intensity (UACI) are the universal measure used to validate the differential attack resistance of the encryption scheme. NPCR calculates the difference in change in number of pixels between two cipher images. It is calculated by the formula,

$$\mathrm{NPCR} = \left(\frac{1}{N} \sum_{i=0}^{N-1} d(i) \right) \times 100\%$$

where, di = 0 if Xi = Yi; di = 1 if Xi ≠ Yi for any i ϵ {0,1, N-1}. X_i is the pixel of the encrypted image obtained from the original image, Y_i is the pixel of the encrypted image obtained from the original image with single pixel changed. UACI calculates the difference of the gray value between two encrypted images.

$$\mathrm{UACI} = \sum_{i=0}^{N-1} \frac{|X_i - Y_i|}{f.T} \times 100\%$$

where f is the largest supported pixel and T is the size of the image. The NPCR and UACI values for the test image 1 are found to be 99.88% and 33.49% respectively.

Table 11 Global and local entropy calculation

Test images	Original image entropy	Global Shannon entropy	Local Shannon entropy K = 40 blocks
MR_1 (256 × 256)	2.1582	7.9953	7.8776
CT_2 (256 × 256)	1.4090	7.9974	7.9236
CT_3 (256 × 256)	1.7045	7.9948	7.9376
MR_2 (512 × 512)	1.4092	7.9985	7.8976
MR_3 (512 × 512)	1.5268	7.9988	7.9026

3.3 Key sensitivity analysis

Keys are the basic and the most important element in any crypto system. This analysis is to check the sensitivity of the algorithm for input key stream. Even a small change in the input key should bring a drastic change in the expected output. The key space used in the proposed scheme is 2^{104} thus it is highly resistant to brute force attack. The input key used is k = {a f w k y t m q l e p v z, $\mu = 3.99$, $p_0 = 0.490123$}. The encrypted image is decrypted with three different keys such as k1 = {b f w k y t m q l e p v z, $\mu = 3.99$, $p_0 = 0.490123$}, k2 = {a f c k y t m q l e p v z, $\mu = 3.99$, $p_0 = 0.490123$}, k3 = {a f w k d t m q l e p v z, $\mu = 3.99$, $p_0 = 0.490123$}. Figure 12(a–e) provides the encrypted image and the decrypted image using three different key values. From the Fig. 9, it can be understood that the algorithm is highly sensitive towards the change in key.

3.4 Cropping attack analysis

Nowadays hackers try to steal the information as much as possible from the encrypted image when it is transmitted through the common channel. The algorithm should be strong enough to resist these attacks. In this analysis, the encrypted images are intentionally cropped to study its effect on the decrypted image. Figure 13(a–h) portrays the cropped and the corresponding decrypted images. From the figure, it can be noticed that despite intentional cropping, the proposed algorithm is still able to retrieve the meaningful image.

3.5 Noise attack analysis

It is highly essential to take care of the noise effect in the channel when the encrypted images are needed to be transmitted over the public channel. This section tends to analyse the noise effect on the cipher image. In order to study the performance of proposed algorithm against noise effects, three types of noises namely the Gaussian, salt and pepper and speckle noise are added intentionally to the cipher image. Figure 14(a–c) shows the encrypted images after adding the Gaussian, salt and pepper and speckle noises respectively. Figure 14(d–f) shows the corresponding decrypted images. From the decrypted images, it is clear that even after the addition of noise, most of the information about the original image could be retrieved.

3.6 Complexity analysis

The proposed method involves DNA encoding, addition, subtraction, decoding and permutation. DNA mapping is carried out using one of the eight available rules. Hence the complexity is 2^8. The

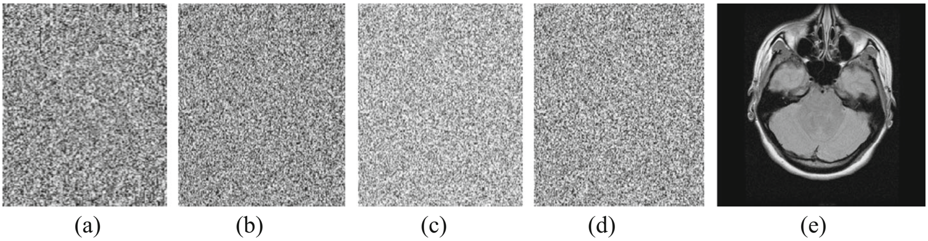


Fig. 12 Key sensitivity analysis: **a** Encrypted image; **b** Decrypted image with wrong key k1; **c** Decrypted image with wrong key k2; **d** Decrypted image with wrong key k3; **e** Decrypted image with original correct key k

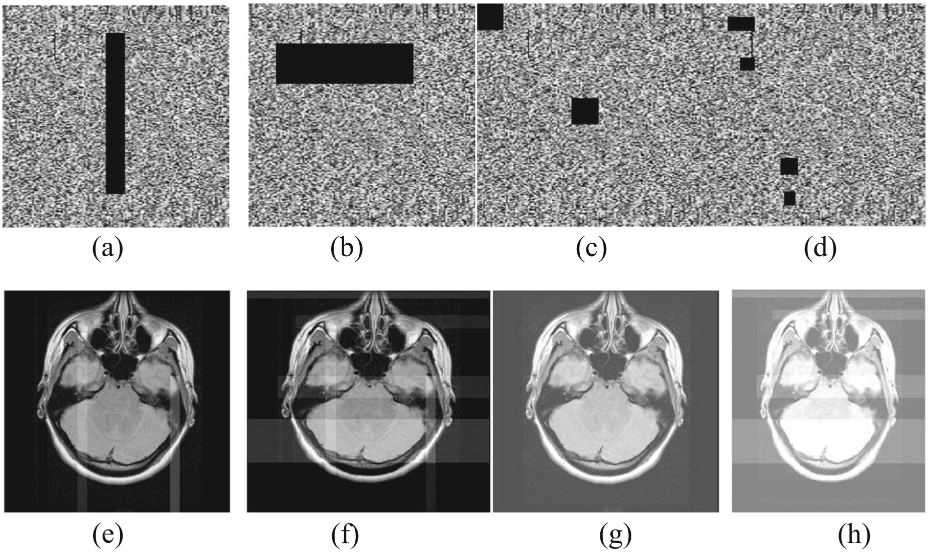


Fig. 13 Cropping attack analysis: **a** Encrypted image with 190 × 5 cropped; **b** Encrypted image with 80 × 50 cropped; **c** Encrypted image with 25 × 10 and 25 × 10 cropped; **d** Encrypted image with multiple cropping; **e** Decrypted image of (**a**); **f** Decrypted image of (**b**); **g** Decrypted image of (**c**); **h** Decrypted image of (**d**)

rules for diffusion operation are selected based on logistic chaotic sequence which depends on the control parameter and 104 bit input key. The permutation is done by PWLCM which is based on control parameter. Hence the total complexity of the proposed system is 2^8 × 2^8 × 10^104.

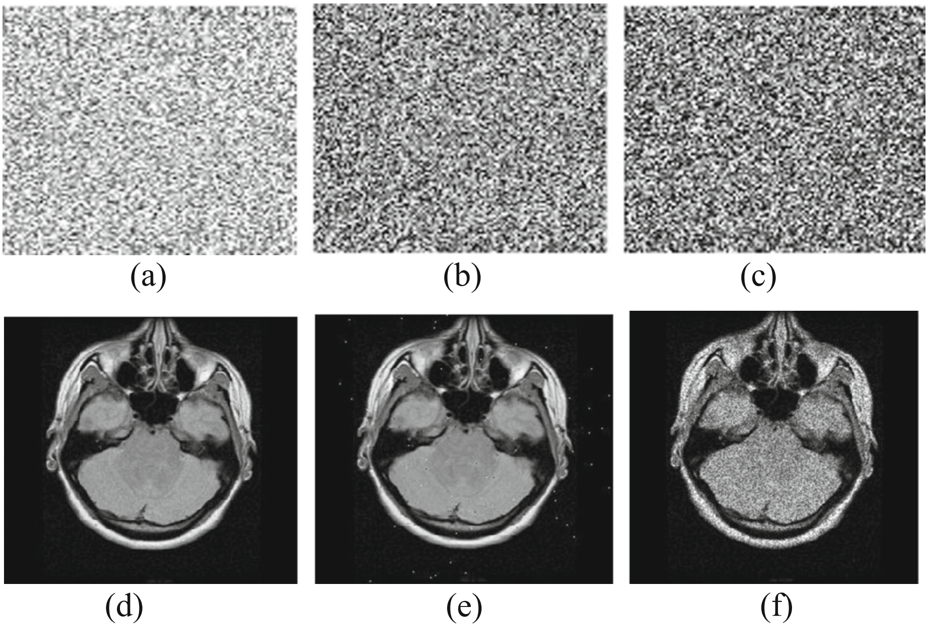


Fig. 14 Noise attack analysis: **a** Cipher image with Gaussian noise; **b** Cipher image with Salt and pepper noise; **c** Cipher image with Speckle noise; **d** Decrypted image of (**a**); **e** Decrypted image of (**b**); **f** Decrypted image of (**c**)

3.7 Performance comparison with existing work

Table 12 shows the comparison of proposed algorithm with few algorithms available in the literature. The comparison has been made based on correlation, NPCR and UACI values.

To estimate the effective decryption of the proposed algorithm, Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), Mean Absolute Error (MAE) and correlation in horizontal, vertical and diagonal directions have been estimated. The expressions pertaining to the computation of MSE, PSNR and MAE are given below:

$$MSE = \frac{1}{M \times N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} \left[I_{i,j} - K_{i,j}\right]^2$$

$$\text{PSNR} = 1 - \log_{10}[M \times N] \frac{1}{MSE}$$

M × N represents the total number of pixels.
$K_{i,j}$ and $I_{i,j}$ represent the original and the decrypted image pixels respectively.

$$MAE = \frac{1}{N} \sum_{i=1}^{n} \sum_{j=0}^{N-1} [f_i - y_i]$$

Here, N represents the total number of pixels. f_i and y_i represent the predicted and true pixel values of the images respectively.

Table 13 presents the analyses between the original and the decrypted images. It can be inferred that the results of zero obtained for the computation of MSE and MAE reiterate the worthiness of the proposed approach in the error-free recovery of original images. Further, the infinity value of PSNR proves a point on the hassle free reconstruction of the secret image back during the decryption process. The three correlation estimations in horizontal, vertical and diagonal directions yield a close to 1 coefficient which is an important metric to substantiate the secured and proper reception of medical record in the form of images.

Table 12 Comparison of the proposed work with the literature

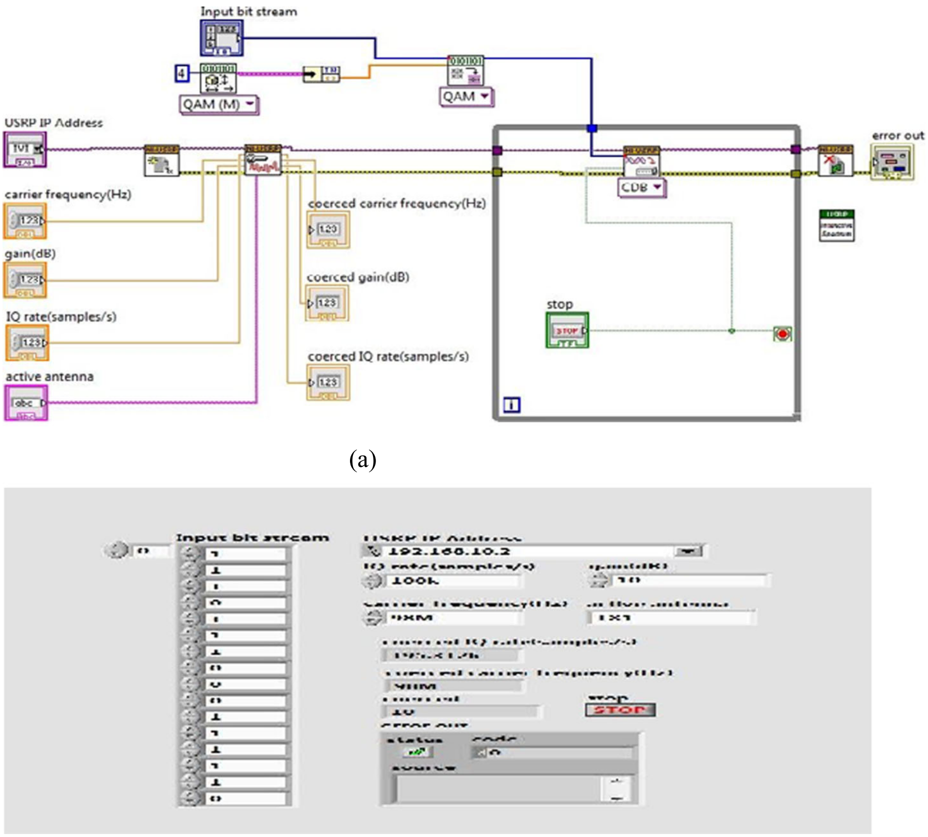
Metrics	Proposed work	Ravichandran et al. [33]	Praveenkumar et al. [32]	Zhen et al. [39]	Liu et al. [27]
Vertical correlation	−0.0840	−0.0385	−0.0033	0.0465	0.0025
Horizontal correlation	0.0682	−0.0519	0.0037	0.0214	0.0003
Diagonal correlation	0.0092	0.00046	0.0117	−0.0090	0.0004
NPCR	99.88	99.996	99.62	99.58	99.64
UACI	33.49	33.37	33.45	33.44	33.57
Entropy	7.9953	7.999	7.9975	7.9993	7.9972

Table 13 Secure image recovery analyses

Images	MSE	PSNR	MAE	Horizontal correlation	Vertical correlation	Diagonal correlation
MR_1 (256 × 256)	0	Inf	0	1.000	0.959	1.000
CT_2 (256 × 256)	0	Inf	0	0.999	0.992	1.000
CT_3 (256 × 256)	0	Inf	0	0.995	1.000	0.999
MR_2 (512 × 512)	0	Inf	0	0.991	1.000	0.909

3.8 Transmission and reception of cipher pixels using CR concept

Initially, the pixel elements of the cipher image are transformed into 16-bit binary information to achieve the efficient transmission. The block diagram and front panel of the designed bit transformation unit is shown in Fig. 15. This data is further modulated by 4-QAM modulation before transmission. The transmission is done with the help of TX1 antenna of NI USRP with the carrier frequency of 98 MHZ.



(a)

Input bit stream: 0; 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0

USRP IP Address: 192.168.10.2

IQ rate(samples/s): 100k

gain(dB): 10

carrier frequency(Hz): 98M

active antenna: TX1

coerced IQ rate(samples/s): [illegible]

coerced carrier frequency(Hz): 98M

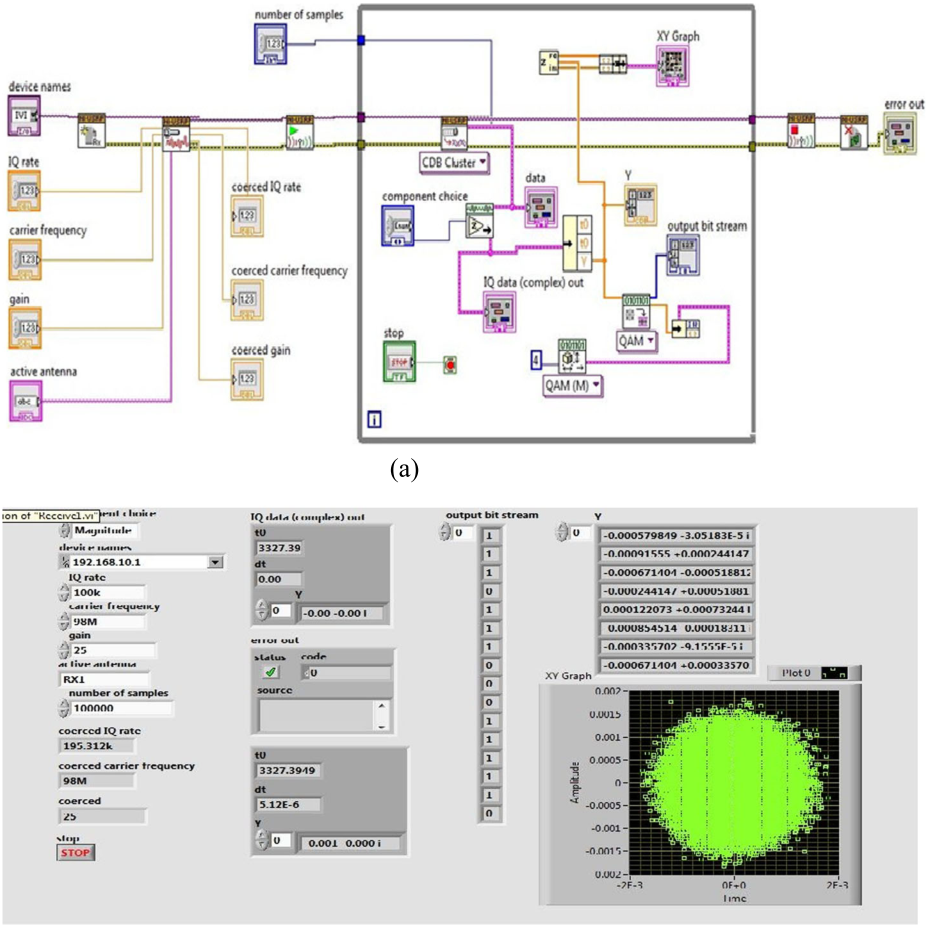
coerced gain: 10

stop: STOP

error out: status ✓ code 0 source

(b)

Fig. 15 Transmission of binary bits (**a**) Block diagram of a transmitted information bits (**b**) Front panel of transmitted information bits



(a)

ion of "Receive1.vi" ent choice
Magnitude
device names
192.168.10.1
IQ rate
100k
carrier frequency
98M
gain
25
active antenna
RX1
number of samples
100000
coerced IQ rate
195.312k
coerced carrier frequency
98M
coerced
25
stop
STOP

IQ data (complex) out
t0
3327.39
dt
0.00
Y
0 -0.00 -0.00 i

error out
status ✓ code 0
source

t0
3327.3949
dt
5.12E-6
Y
0 0.001 0.000 i

output bit stream
0
1
1
1
0
1
1
1
0
0
0
1
1
1
1
1
0

Y
0
-0.000579849 -3.05183E-5 i
-0.00091555 +0.000244147
-0.000671404 -0.00051881
-0.000244147 +0.00051881
0.000122073 +0.00073244 i
0.000854514 0.00018311
-0.000335702 -9.1555E-5 i
-0.000671404 +0.00033570

(b)

Fig. 16 Reception of binary bits (**a**) Block diagram of a received information bits (**b**) Front panel of received information bits

The receiver antenna RX1 of NI USRP is tuned to the frequency of 98MHZ at which the information needs to be transmitted. The received signal is demodulated by 4-QAM and thus the 16-bit binary information is retrieved from the signal. This is shown in Fig. 16.

4 Conclusion

An efficient and secure transmission of medical images by adopting CR technology and image encryption technique has been proposed. DNA and chaos-based encryption system are used to encrypt the medical images and CR technique was utilized to sense the unused spectrum to transreceive the encrypted bio images effectively. The combination of DNA and the chaotic map has increased the algorithm's resistance towards statistical, differential analysis, noise and cropping attacks. Hence this technique can be widely implemented in rural areas connecting ambulance, doctor and patient monitoring system in a secured manner.

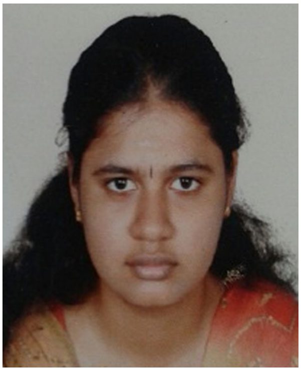
Acknowledgements Authors would like to express their sincere thanks to SASTRA University, for the financial support under R&M fund (R&M/0027/SEEE – 010/2012–13) to carry out this research work. Also, we are grateful to Dr. S. Vanoli, Medical Superintendent, Government Hospital, Ariyalur, for his valuable suggestions in carrying out this work.

References

1. Akyildiz I, Lee WY, Vuran MC, Mohanty S (2008) A survey on spectrum management in cognitive radio networks. IEEE Commun Mag 46:40–48. doi:10.1109/MCOM.2008.4481339
2. Al-Ayyoub M, Jararweh Y (2016) Virtualization-based cognitive radio networks. J Syst 117:15–29. doi:10.1016/j.jss.2016.02.014
3. Alsaedi, M. (2016) Colored image encryption and decryption using multi-chaos 2D quadratic strange attractors and matrix transformations. Multimed Tools Appl (2016). doi:10.1007/s11042-016-4206-4
4. Althunibat S, Wang Q, Granelli F (2016) Flexible channel selection mechanism for cognitive radio based last mile smart grid communications. Ad Hoc Netw 41:47–56. doi:10.1016/j.adhoc.2015.10.008
5. Alvarez G, Li S (2006) Some basic cryptographic requirements for chaos-based cryptosystems. Int J Bifurc Chaos 16:2129–2151. doi:10.1142/S0218127406015970
6. Belazi A, Abd El-Latif AA, Diaconu A-V, Rhouma R, Belghith S (2017) Chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transforms. Opt Lasers Eng 88:37–50. doi:10.1016/j.optlaseng.2016.07.010
7. Boriga, R., Dăscălescu, A.C., Diaconu, A.-V. (2014) A new one-dimensional chaotic map and its use in a novel real-time image encryption scheme (2014) advances in multimedia, 2014, art. no. 409586. doi:10.1155/2014/409586
8. Cedillo-Hernandez M, Garcia-Ugalde F, Nakano-Miyatake M, Perez-Meana H (2013) Robust watermarking method in DFT domain for effective management of medical imaging. Signal, Image Video Process 9: 1163–1178. doi:10.1007/s11760-013-0555-x
9. Diaconu AV (2016) Circular inter-intra pixels bit-level permutation and chaos-based image encryption. Inf Sci 355–356:314–327. doi:10.1016/j.ins.2015.10.027
10. Dridi M, Bouallegue B, Mtibaa A (2014) Crypto-compression of medical image based on DCT and chaotic system. *Global Summit on Computer & Information Technology (GSCIT)*, Sousse, pp. 1-6. doi:10.1109/GSCIT.2014.6970113
11. Guesmi R, Farah M, Kachouri A, Samet M (2016) A novel chaos-based image encryption using DNA sequence operation and secure hash algorithm SHA-2. Nonlinear Dyn 83:1123–1136. doi:10.1007/s11071-015-2392-7
12. Heider D, Barnekow A (2007) DNA-based watermarks using the DNA-crypt algorithm. BMC Bioinf 8:176. doi:10.1186/1471-2105-8-176
13. Jain A, Rajpal N (2015) A robust image encryption algorithm resistant to attacks using DNA and chaotic logistic maps. Multimed Tools Appl 75:5455–5472. doi:10.1007/s11042-015-2515-7
14. Khan MK, Zhang J (2007) An intelligent fingerprint-biometric image scrambling scheme. Advanced Intelligent Computing Theories and Applications. With Aspects of Artificial Intelligence Volume 4682 of the series Lecture Notes in Computer Science pp 1141–1151. doi:10.1007/978-3-540-74205-0_118
15. Khan MK, Zhang J, Tian L (2005) Protecting biometric data for personal identification. Advances in Biometric Person Authentication Volume 3338 of the series Lecture Notes in Computer Science pp 629–638 doi:10.1007/978-3-540-30548-4_72
16. Khan MK, Zhang J, Alghathbar K (2011) Challenge-response-based biometric image scrambling for secure personal identification. Futur Gener Comput Syst 27(4):411–418. doi:10.1016/j.future.2010.05.019
17. Kocarev L (2001) Chaos-based cryptography: a brief overview. IEEE Circuits Syst Mag 1:6–21. doi:10.1109/7384.963463
18. Kulsoom A, Xiao D, Abbas S (2016) An efficient and noise resistive selective image encryption scheme for gray images based on chaotic maps and DNA complementary rules. Multimed Tools Appl 75:1–23. doi:10.1007/s11042-014-2221-x

19. Leier A, Richter C, Banzhaf W, Rauhe H (2000) Cryptography with DNA binary strands. Biosystems 57: 13–22. doi:10.1016/S0303-2647(00)00083-6
20. Li J, Li X, Yang B, Sun X (2015) Segmentation-based image copy-move forgery detection scheme. IEEE Trans Inf Forensics Secur 10(3):507–518. doi:10.1109/TIFS.2014.2381872
21. Li X, Wang L, Yan Y, Liu P (2016) An improvement color image encryption algorithm based on DNA operations and real and complex chaotic systems. Opt - Int J Light Electron Opt 127:2558–2565. doi:10.1016/j.ijleo.2015.11.221
22. Liao X, Shu C (2015) Reversible data hiding in encrypted images based on absolute mean difference of multiple neighboring pixels. J Vis Commun Image Represent 28(4):21–27. doi:10.1016/j.jvcir.2014.12.007
23. Liao X, Li K, Yin J (2016) Separable data hiding in encrypted image based on compressive sensing and discrete Fourier transform. Multimed Tools Appl (2016). doi:10.1007/s11042-016-3971-4
24. Lima JB, Madeiro F, Sales FJR (2015) Encryption of medical images based on the cosine number transform. Signal Process Image Commun 35:1–8. doi:10.1016/j.image.2015.03.005
25. Liu H, Wang X, kadir A (2012) Image encryption using DNA complementary rule and chaotic maps. Appl Soft Comput 12:1457–1466. doi:10.1016/j.asoc.2012.01.016
26. Liu L, Zhang Q, Wei X (2012) A RGB image encryption algorithm based on DNA encoding and chaos map. Comput Electr Eng 38:1240–1248. doi:10.1016/j.compeleceng.2012.02.007
27. Liu Y, Wang J, Fan J, Gong L (2016) Image encryption algorithm based on chaotic system and dynamic S-boxes composed of DNA sequences. Multimed Tools Appl 75:4363–4382. doi:10.1007/s11042-015-2479-7
28. Masuda N, Aihara K (2002) Cryptosystems with discretized chaotic maps. IEEE Trans Circuits Syst I Fundam Theory Appl 49:28–40. doi:10.1109/81.974872
29. Moumen A, Bouye M, Sissaoui H (2015) New secure partial encryption method for medical images using graph coloring problem. Nonlinear Dyn 82:1475–1482. doi:10.1007/s11071-015-2253-4
30. Nazeer M, Nargis B, Malik YM, Kim D-G (2013) A fresnelet-based encryption of medical images using arnold transform. Int J Adv Comput Sci Appl 4:131–140. doi:10.14569/IJACSA.2013.040322
31. Parvees MYM, Samath JA, Bose BP (2016) Secured medical images - a chaotic pixel scrambling approach. J Med Syst 40:232. doi:10.1007/s10916-016-0611-5
32. Praveenkumar P, Amirtharajan R, Thenmozhi K, Balaguru Rayappan JB (2015) Medical data sheet in safe havens - a tri-layer cryptic solution. Comput Biol Med 62:264–276. doi:10.1016/j.compbiomed.2015.04.031
33. Ravichandran D, Praveenkumar P, Balaguru Rayappan JB, Amirtharajan R (2016) Chaos based crossover and mutation for securing DICOM image. Comput Biol Med 72:170–184. doi:10.1016/j.compbiomed.2016.03.020
34. Rehman AU, Liao XF, Kulsoom A, Abbas SA (2015) Selective encryption for gray images based on chaos and DNA complementary rules. Multimed Tools Appl 74:4655–4677. doi:10.1007/s11042-013-1828-7
35. Tragos EZ, Zeadally S, Fragkiadakis AG, Siris VA (2013) Spectrum assignment in cognitive radio networks: a comprehensive survey. IEEE Commun Surveys Tuts 15:1108–1135. doi:10.1109/SURV.2012.121112.00047
36. Troncoso-Pastoriza JR, Katzenbeisser S, Celik M (2007) Privacy preserving error resilient DNA searching through oblivious automata. In *Proceedings of the 14th ACM conference on Computer and communications security* (CCS '07). ACM, New York, NY, USA, 519–528. doi:10.1145/1315245.1315309
37. Watson JD, Crick FHC (1953) A structure for deoxyribose nucleic acid. Nature 171:737–738 http://www.nature.com/nature/dna50/watsoncrick2.pdf
38. Zhang L, Liao X, Wang X (2005) An image encryption approach based on chaotic maps. Chaos, Solitons Fractals 24:759–765. doi:10.1016/j.chaos.2004.09.035
39. Zhen P, Zhao G, Min L, Jin X (2016) Chaos-based image encryption scheme combining DNA coding and entropy. Multimed Tools Appl 75:6303–6319. doi:10.1007/s11042-015-2573-x
40. Zheng Y, Jeon B, Xu D, Wu QMJ, Zhang H (2015) Image segmentation by generalized hierarchical fuzzy C-means algorithm. J Intell Fuzzy Syst 28(2):961–973. doi:10.3233/IFS-141378

Padmapriya Praveenkumar received her B.E (ECE) from Angala Amman college of Engineering and Technology and M.E (Communication system) from Jayaram college of Engineering and Technology. Currently she is working as an Assistant Professor III in the Department of ECE in SASTRA University, Thanjavur. She has a teaching experience of 13 years and she has published 35 Research articles in National & International journals. She is currently working towards her Ph.D. Degree in SASTRA University. Her research area includes Wireless communication and Steganography.



N. Kerthana Devi received her B.E. (Electronics and communication engineering) in 2014 from Park College of engineering, Coimbatore and M.Tech in communication systems in 2016 from SASTRA university, Thanjavur. Her research area includes information security and medical security.

Dhivya Ravichandran received her B.E. (Electronics and communication engineering) in 2012, from St. Joseph's college of engineering, Chennai and M.Tech in Advanced communication systems from SASTRA University, Thanjavur in 2014. She is currently working as research scholar in school of electrical and electronics engineering, SASTRA University, India. Her research areas include information security, embedded systems and medical image security. So far she has published 7+ Research articles in National & International journals.

J. Avila received her B.E (ECE) from the V.M.K.V college of Engineering and M.E (Communication Engineering) from Vellore Institute Of Technology. Currently she is working as Assistant Professor III in the Department of ECE in SASTRA University, Thanjavur. She has a teaching experience of 10 years and she has published 21 Research articles in National & International journals. She is currently working towards her Ph.D. Degree in SASTRA University. Her research area includes Wireless communication and Cognitive radio

K. Thenmozhi received her B.E (ECE) and M.E (Communication system) degrees from Regional Engineering college (NIT) Tiruchirappalli and Ph.D. from SASTRA University, Thanjavur. Currently she is working as an Associate Dean in the Department of ECE in SASTRA University, Thanjavur. She has a teaching experience of 20 years. Her current research area includes Wireless communication, Steganography and Information Theory and Coding. She has supervised more than 100 UG projects, 10 Master Students and Supervising 4 Ph.D. Scholars. So far she has published 80+ Research articles in National & International journals@conferences. She received EDI award from broadcast Engineering Society for the year 2007.

John Bosco Balaguru Rayappan was born in Trichy, Tamil Nadu province, India in 1974. He received the B.Sc., M.Sc. and M.Phil. Degree in Physics from St. Joseph College, Bharathidasan University, Trichy and Ph.D. in Physics from Bharathidasan University, Trichy, Tamil Nadu India in 1994, 1996, 1998 and 2003, respectively. He joined the faculty of SASTRA University, Thanjavur, India in Dec 2003 and is now working as Professor & Associate Dean Research School of Electrical and Electronics Engineering at SASTRA University, Thanjavur, Tamil Nadu, India. His research interests include Lattice Dynamics, Nanosensors, Embedded System and Steganography. So far he has published 170+ Research articles in National and International journals and 14 conference papers. He has Supervised 25 Master Students and Supervising 5 Ph.D. Scholars. Currently he is working on four funded projects in the fields of Nanosensors and Steganography supported by DST and DRDO, Government of India, New Delhi. Indo-Swedish collaboration work.

Rengarajan Amirtharajan was born in Thanjavur, Tamil Nadu province India, in 1975. He received B.E. degree in Electronics and Communication Engineering from P.S.G. College of Technology, Bharathiyar University, Coimbatore, India in 1997. M.Tech. and Ph. D. from SASTRA University Thanjavur, India in 2007 and 2012 respectively. He joined SASTRA University, Thanjavur, Tamil Nadu, India (Previously Shanmugha College of Engineering) as a Lecturer in the Department of Electronics and Communication Engineering since 1997 and is now Associate Professor, His research interests include Image Processing, Information Hiding, Computer Communication and Network Security. So far, he filed one international patent; he has published more than 125+ research articles in national and international journals and 22 I.E. conference papers with 4 Best Paper Awards. He also holds the Certificate of Appreciation from IBM in 2009 for Great Mind Challenge, Mentor IBM Academic Initiative Program. Recently, he received the Founder Chancellor Award for the best Ph.D. thesis for 2013 from SASTRA University and he received the SASTRA Anukul Puraskar for Higher Involvement in Research and Education Award for 2011–2012 and 2013–2014. He serves as a Life Member in CRSI, SSI, IAENG, and IACSIT. He also served as the TPC Member and Review Member for more than 30+ IEEE and Springer supported international conferences apart from more than 10 peer reviewed journals. He had been working on funded project in the field of steganography supported by DRDO, Government of India, New Delhi, India