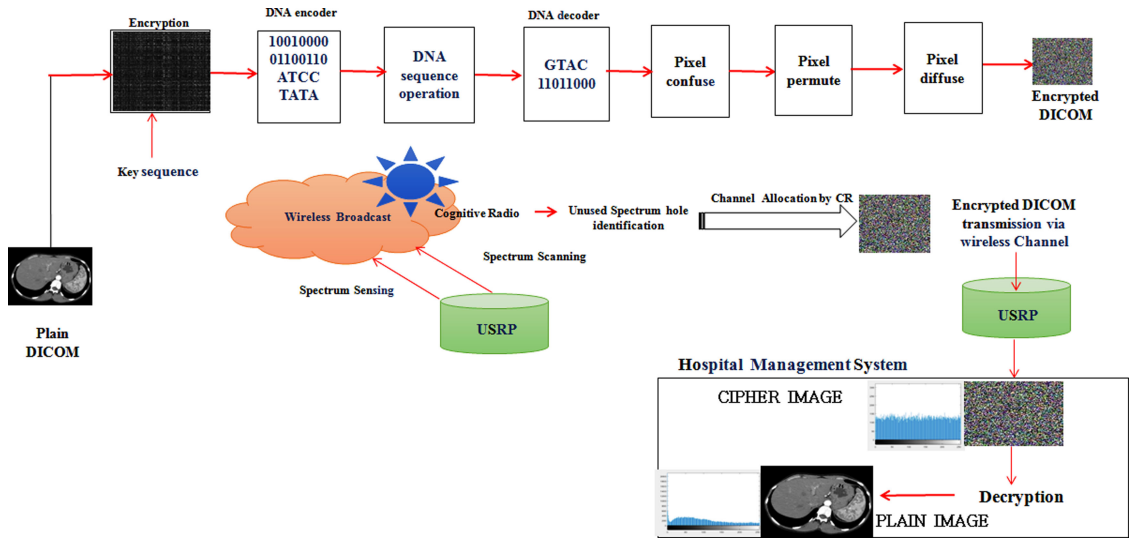
IEEE Photonics Journal
An IEEE Photonics Society Publication

Open Access

CR Assisted IE Guarded Authenticated Biomedical Image Transactions

Volume 10, Number 05, September 2018

K. Revathy
K. Thenmozhi
Rengarajan Amirtharajan
Padmapriya Praveenkumar



DOI: 10.1109/JPHOT.2018.2872160
1943-0655 © 2017 IEEE

IEEE photonics SOCIETY

IEEE

CR Assisted IE Guarded Authenticated Biomedical Image Transactions

K. Revathy,[1] K. Thenmozhi,[2] Rengarajan Amirtharajan,[2] and Padmapriya Praveenkumar[2]

[1]Department of Electronics and Communication Engineering, Srinivasa Ramanujan Centre, Kumbakonam 612001, India
[2]School of Electrical and Electronics Engineering, SASTRA Deemed to be University, Thanjavur 613401, India

DOI:10.1109/JPHOT.2018.2872160

Manuscript received May 10, 2018; revised August 25, 2018; accepted September 19, 2018. Date of current version October 12, 2018. Corresponding author: Padmapriya Praveenkumar (e-mail: padmapriya@ece.sastra.edu).

Abstract: In this android era, the word spectrum is connected with trillion faces. The underutilization problem of the spectrum in most of the applications results in the paucity of this scarce resource. Cognitive radio (CR) is an astute technology implemented for the opportunistic usage of idle spectrum resource dynamically. This paper focuses on sensing of the vacant channels, and it is pre-owned for the transmission of encrypted DICOM information. The proposed algorithm involves encryption schemes like RC5, latin square image cipher, deoxyribo nucleic acid, and discrete Gould transform (DGT) to render confusion, diffusion, and permutation operations. Further, the uncorrelated cipher image is transmitted via the identified unused licensed spectrum. The proposed scheme guarantees the authorised transactions among the stack holders like patients, doctors, and hospital management systems. It also ascertains and enhances the validation of the cipher biomedical interactions among peers by assuring tamper proofing using DGT. Simulations have been conceded over universal software radio peripheral to validate the biomedical data transactions after sensing the unused spectrum. Metrics like global–local entropies, correlation coefficients, key sensitivity, chi-square tests, cropping attacks and differential attack analysis were estimated to authenticate the robustness of the projected encryption scheme.

Index Terms: Cognitive security, dicom, image encryption, USRP.

1. Introduction

In recent times accessing the web as an excellent medium; one can transfer information from any source to destinations within a fraction of a second. Telemedicine is one of the applications of clinical medicine where restorative data are exchanged through telecom systems and in some cases for remote medicinal techniques or examinations. Remote telemedicine is characterised as the conveyance of medical services, administrations and sharing of therapeutic information over the remote station [1]. An essential issue confronting the future in remote frameworks is the place to discover suitable spectrums to satisfy the interest of future administrations. While the more significant part of the radio range is apportioned to various administrations and applications. Clients, perception demonstrate that utilization of the spectrum is quite low. To conquer this issue and to enhance the range usage, Cognitive radio idea has been developed [2]. Cognitive Radio (CR), a system initially presented by Mitolais considered as a promising strategy to take care of the range proficiency issue, in which unlicensed users are allowed to utilize the authorized recurrence groups

TABLE 1
RC5 Parameters

Parameters used in encryption	Description	Range
W	Word size	32,64,128 bytes
R	Rounds	0-255
B	Secret key in bytes	0-255

without creating a destructive obstruction to the authorized Primary Users (PUs) [3]. To conserve the concealment of the information new proficiency was developed to make high authentication in communication, one such developed is encryption. Encryption techniques are very optimistic for digital images and should be used to disappoint opponent attacks from unintended users [4], [5].

Nowadays, the encryption field is further dominated by Deoxyribo Nucleic Acid (DNA) cryptography [6]. DNA computing is a newly emerging field, which is providing a very high level of security for data storage and cryptographic data transportation [7]. Using DNA computing, information and images can be transmitted with a high level of protection. Thus it remains immune to differential and robust attacks [8]–[10].

Chaos is now gaining more attention because of it is of severe sensitivity to initial conditions, control parameters and its ergodic behaviour [11]. The main advantages of the chaotic encryption in any encryption is that size based available system design, a considerable number of variants and complex keys [12]–[18].

In the diagnosis of diseases, medical images play a vital role as to secure digital images widely over the internet. Today healthcare organizations can dislocate financial barriers by eliminating traditional-IT fuss associated with sharing, exchanging and storing diagnostic imaging [19]–[21]. Cybercriminals tag information regarding the patient, such as names, birth dates and health insurance contract indulged in the act of stealing about 20 dollars on the black market, according to researchers at Aberdeen Group. To seamlessly transfer medical images like CT, MRI and other law within hospitals or around the globe some standards are maintained [22]–[26].

This paper proposes a secure encrypted biomedical data transmission and exchanging among peers by utilizing the unused frequency spectrum. CR network is used to identify the spectrum free holes, and encrypted data transmission was carried out. Encryption schemes were entangled with RC5, and chaos to provide better encrypted biomedical images. The proposed method guarantees tamper proofing, authentication, randomness and better encrypted cipher output.

2. Background of the Proposed Scheme

The proposed scheme involves operations like RC5, Logistic mapping, DNA, DGT, LSIC and CR based sensing schemes. The descriptions of the methods are as follows [4]–[6], [8], [10], [12]:

2.1 RC5 Encryption

It is an encryption algorithm and can adapt to different word lengths and variable length secret cryptographic key. The key is iterative due to inconsistent rounds involved in it. The algorithm employs rounds, length of the key and the size of the word used. The parameters used in RC5 encryption algorithm is given in Table 1.

Key expansion in RC5 can be generated using key scheduling operation which in-turn depends on the number of rounds. The operations involved in RC5:

- Two's complement addition ('+')
- Bitwise EXOR ($\oplus$)
- Left notation (x$<<<$ y) and right notation (x $>>>$ y)

TABLE 2
DNA Operations

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

2.2 Chaotic System

It is a nonlinear polynomial of second degrees and can be expressed using the following equation:

$$\beta_{m+1} = \mu\beta_m (1 - \beta_m) \tag{1}$$

where μ is the control parameter which ranges from 0 to 4 is, β_m is the initial seed; $\beta_m \in (0, 1)$ and m denotes the number of rounds involved in key generation. The key for RC5 encryption algorithm is generated using the logistic map [6]–[12].

2.3 DNA Coding

In DNA, the elements are arranged in a unique structure. It consists of four bases(A (adenine), C (cytosine), G (guanine), T (thymine), and the bonding structure is formed by these bases as two complement pairs. DNA addition and subtraction rules can be formed from the combination of these bases as in Table 2 [4], [6], [8]–[10].

2.4 DGT

Discrete Gould Transform (DGT) was generally employed in hiding secret data bits providing high withstanding capacity. In the proposed methodology, it helps in identifying the unauthorized access or any manipulation done by the third party users [5]. This feature helps in authentication of the proposed algorithm. The value of a and b decides the values of the Gould coefficients in the Gould transform X and is given by

$$\begin{matrix} a \\ b \end{matrix} X = \left(\begin{matrix} 1 \\ b \end{matrix} X \right)^a \tag{2}$$

2.5 LSIC

Latin Square Image Cipher (LSIC) is a Square matrix which has an n $\times$ n matrix, in which each element in the matrix is distinct. No element in a row/column will be repeated in the entire matrix. It contains three Latin square based encryption processes, namely Latin Square Whitening, Latin Square Substitution and Latin Square Permutation [13].

2.6 Cognitive Radio Technology

Cognitive Radio is a smart, intelligent network which is mainly used to sense the unused spectrum. In this scheme, initially a threshold value is fixed, then the availability of the primary user is monitored continuously if the channel is unused, then the encrypted biomedical data bits are modulated utilising the vacant spectrum via USRP module.

2.7 Algorithms of the Proposed Model

The proposed model involves the sensing of the spectrum using CR network, then encrypted biomedical images will be transmitted using the sensed frequency spectrum.

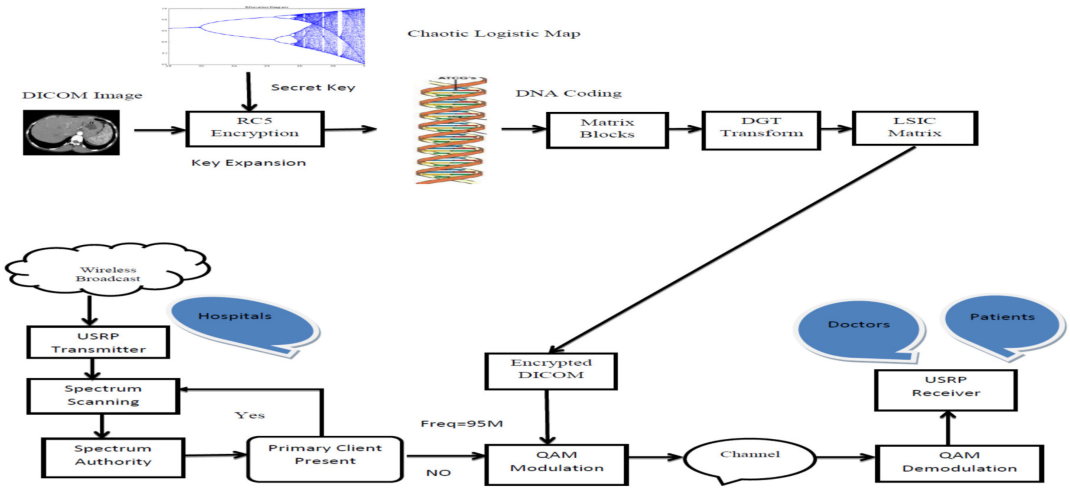


Fig. 1. Proposed block diagram.

2.8 Block Diagram

Here initially spectrum sensing was carried out to diagnose the presence of primary user availability. If the spectrum is found to be free, then encrypted biomedical data transmission will be carried out in an authenticated manner as in Fig. 1.

2.9 Spectrum Sensing Using CR Network

- Cognitive Radio is a trustworthy communication for efficient utilisation of radio spectrums.
- Initially, the threshold value is fixed for efficient transmission.
- Then the filter on receiving the signal a(t), it is transformed into binary and threshold value is estimated.
- To identify the primary user presence, FFT is applied on the bins, integrated and compared with the threshold value.

$$a(t) = \begin{cases} N(t) & L \\ S(t) + N(t) & M \end{cases}$$

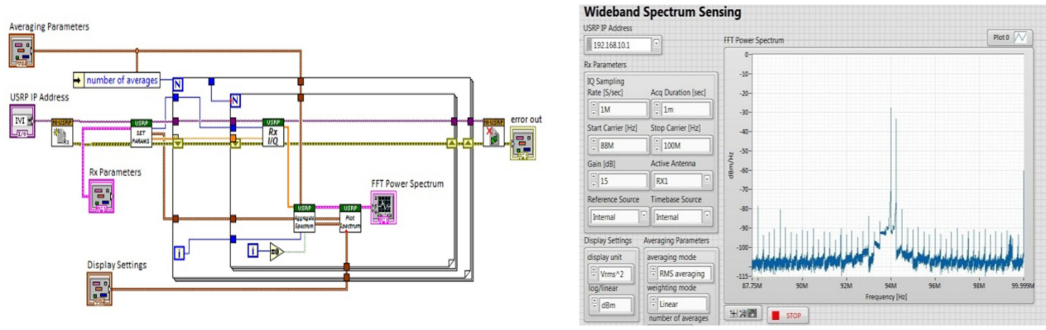
where L and M indicates the primary user presence and absence. S(t) represents the signal waveform, and N(t) represents the Gaussian Noise. False alarm detection probability is given by $\begin{cases} P_d(TD) = P_r[Y > TD|L] \\ P_f(TD) = P_r[Y > TD|M] \end{cases}$

TD represents threshold. Pf represnts the probability of false alarm and the value should be minimum, and Pd denotes the probability of detection and it should be maximum to evade transmission underutilization.

- The Spectrum hole is sensed, in the absence of a primary user and it is utilized to exchange encrypted biomedical information among peers.
- On examining the signal spectrum with the help of receiving antenna, the restriction of bandwidth in the range of 88 MHz to 100 MHz with again of 15 dB(NI USRP) is selected as shown in Figs. 2(a) and (b).

2.10 Biomedical Encryption Algorithm

- Read the DICOM image.
- The input image is initially encrypted using RC5 encryption algorithm.



(a) (b)

Fig. 2. (a) and (b) Spectrum estimation and its output screen using LabVIEW.

- The key for each round of RC5 is obtained using chaotic logistic sequence

$$\beta_{m+1} = \mu\beta_m (1 - \beta_m)$$

- Iterating β obtains K1and the key is iterated as

$$K'_i = (K1 \times 2^{18} \text{mod} 255) \tag{3}$$

- After generating the chaotic sequence, the key expansion for RC5 encryption is performed as below:
- The array L is initialized into S(t) where $t = 2r + 2$. r indicates the round of operation. The registers are initialized as
- $R_1 = R_1 + s[0]$; $R_2 = R_2 + s[1]$, count $= 1$; (as in section 2.1)
- Perform XOR Rotation between the registers,

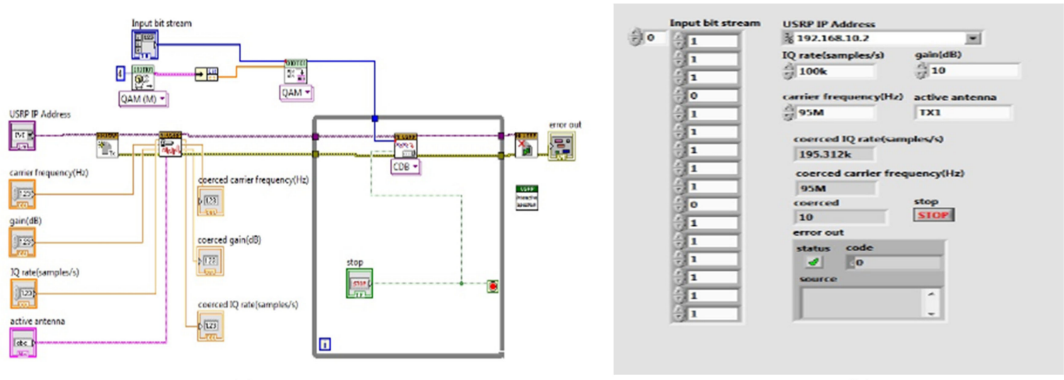
$$R_1 = (R_1 \oplus R_2 \ll R_2) + s[2 \times i]$$
$$R_2 = (R_2 \oplus R_1 \ll R_1) + s[2 \times i + 1] \tag{4}$$

- Increment the counter and if the counter and number of rounds are equal terminate the loop, else continue the iteration. Then the encrypted image is divided into four quadrants.
- DNA operations are performed as in Table 2.
- Combine the quadrants to get the DNA encrypted image.
- Then to the resultant image, DGT is applied for better authentication.
- Gould transform matrices are formed using a b values. ${}^{a}_{b}X = ({}^{1}_{b}X)^{a}$
- Latin Square Image Cipher technique again shuffles the resultant image.
- To perform LSIC two keys are required. The resultant image is first XORed by key1 and then by key2 to attain the final encrypted image.

2.11 Encrypted Biomedical Image Transmission Using USRP

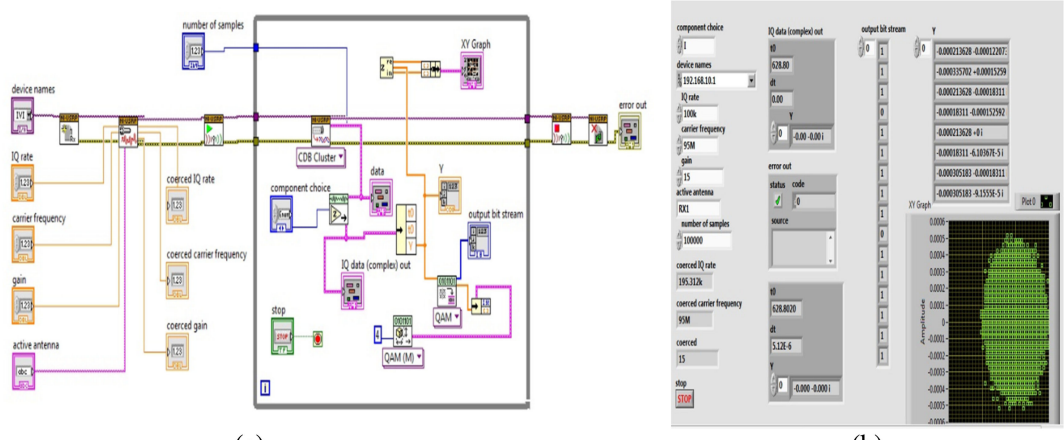
- The USRP is set up to work in the spectrum bandwidth of 88 MHz to 100 MHz with a gain of 20 dB.
- Using the energy detector algorithm, initially the free spectrum is identified.
- Then the modulated encrypted biomedical signals are transmitted on the USRP channel, and USRP receiver also obtains the reception of the signal by setting the receiver to the same channel frequency.
- Figs. 3(a) and (b) represents the binary information. After modulation, the information will be transmitted via transmitting antenna of USRP.

The transmission and reception can be carried out by doctors, patients and the hospital management systems to make the biomedical image transactions in an authenticated and



(a) (b)

Fig. 3. (a) and (b) Block diagram of information bits transmission and its output.



(a) (b)

Fig. 4. (a) and (b) Block representation of information reception and its output.

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

Fig. 5. Original test images. (a) Test_image1. (b) Test_image2. (c) Test_image3. (d) Test_image4. (e) Test_image5.

tamper-proof manner. Fig. 4(a) and 4(b) depict the LabVIEW block and its front panels of the received information bits.

3. Results and Discussion

In the proposed scheme, DICOM test images of various sizes are considered as shown in Figs. 5(a–e). The proposed algorithm has been implemented using the keyset K = $\{\beta m + 1 = 0.29453657866777, \mu = 3.88889999888899\}$.

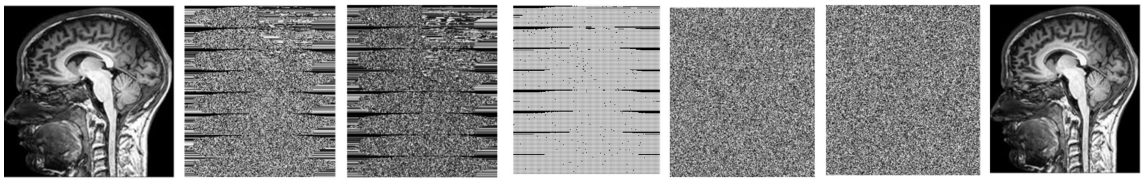


Fig. 6. (a) Test_image. (b) RC5 output. (c) DNA Coded output. (d) DGT output. (e) LSIC with key 1. (f) LSIC with key 2. (g) Decrypted output.

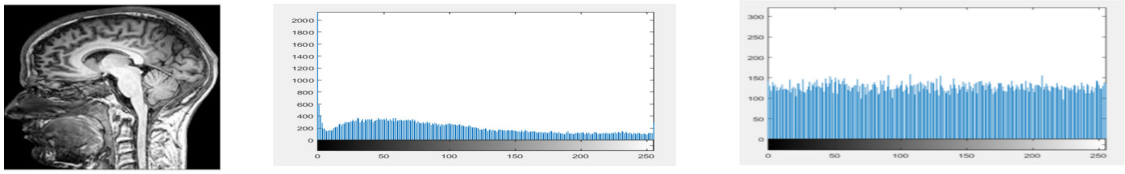


Fig. 7. (a) Test_image1. (b) Histogram of (a). (c) Encrypted Histogram of (a).

Figure 6(a–g) shows the input image followed by various stages of encryption and finally the decrypted output.

3.1 Statistical Analysis

To confirm the robustness of the proposed encryption algorithm against various statistical and differential attacks, histogram analysis, chi-square tests, deviation from ideality, histogram deviation, irregular deviation and CC of the encrypted images were estimated and analyzed.

3.1.1 Pixel Distribution Analysis: Fig. 7(a–c) represents the test_image, histogram and the encrypted images respectively. From the figures, the pixels in the histogram of the encrypted image are equally spread over the entire region which is entirely different from the original image histogram. This proves the unpredictability and the randomness of the proposed encryption algorithm.

3.1.2 CHI-Square Tests: The pixel distribution uniformity is validated using chi-square($\chi 2$) test, to enhance the security performance. Table 1 summarises the result of the $\chi 2$ test for various cipher image. It is the statistical test to analyze any fluctuations of the encrypted image from the expected result. The chi-square parameter $\chi 2$ is defined as

$$\chi^2 = \sum_{1}^{256} \frac{(P_i - C_i)^2}{C_i} \tag{5}$$

where i represent the number of grey values in the image, Pi and Ci are observed and expected occurrence of each grey values.

The chi-square values for the various tests images are computed and given in Table 3. The theoretical chi-square value is equal to 293.24 of the degree of freedom 255. The measured chi-square values from the histogram are lesser than the theoretical value, which indicates that the encrypted image pixels are distributed uniformly. From Table 3, all the tests images are lesser than the theoretical Chi-square tests value which proves the uniformity of the encrypted pixels of all the tests images.

TABLE 3
Chi Square Analysis

Test Images	χ^2
MR_1	232.901
MR-2	247.31
CT_1	276.76
CT_2	266.48
CT_3	252.56

TABLE 4
Cipher Assessment Metrics

Test Images	Histogram Deviation	Irregular Deviation	Deviation from Ideality
MR_1	5.8945e+03	0.6220	0.3416
MR_2	5.634e+03	1.7290	0.1213
CT_1	5.8134e+04	1.0923	0.2103
CT_2	2.3948e+04	2.1001	3.0028
CT _3	2.3681 e+04	2.5672	3.4527

3.1.3 Histogram Deviation: It is defined as the quantity that deviates between the encrypted and the original image pixels, and it is given by

$$D_H = \frac{\left(\frac{d_0+d_{255}}{2} + \sum_{j=1}^{255} d_j\right)}{M \times N}$$

where di denotes the absolute amplitudes difference at j, $d_0 d_{255}$ represents the initial and final amplitudes of the image pixels and the size of the cipher output is given by M × N.

3.1.4 Irregular Deviation: It is used to access the pixel deviated in the encrypted image from the original image, and it is given by

$$D_1 = \frac{\sum_{i=0}^{255} H_D(i)}{M \times N} \tag{6}$$

where absolute histogram deviation is given by HD(i) = | H(i) – MH |, H(i) represnts the histogram for i = 0 to 255 and MH is the mean of the histogram.

3.1.5 Deviation from Ideality: It is a measure of reducing the difference of cipher image from the input image, and it is given by

$$D = \frac{\sum_{C_I=0}^{255} |H_{C_I} - H_C|}{M \times N} \tag{7}$$

where H(C) and H_{C_I} are the encrypted and the original image histograms considering the image size MXN. The above evaluation metrics are reported in Table 4. From the table, smaller the values of irregular deviation and the deviation from ideality and a more significant value in histogram deviation indicate that the proposed algorithm has provided the complete encryption.

3.1.6 Correlation Coefficient: Correlation between adjacent pixels in the original image is very high since the correlation with the neighbourhood pixels of plain text is high in any direction. However, the correlation in the cipher image is very low to withstand the robustness of the algorithm and is given by the equation

$$\text{Correlation } (m, n) = \frac{E[(m - E(n))(b - E(b))]}{\alpha_m \alpha_n} \tag{8}$$

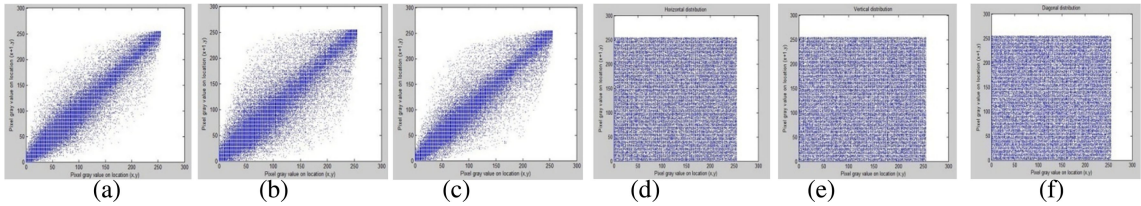


Fig. 8. (a–c) Correlation in horizontal, vertical, and in diagonal directions of Test image 1. (d–f) Correlation in horizontal, vertical, and in diagonal directions of encrypted test image1.

TABLE 5
Correlation Analysis of Various Sample Images

Test Samples	Correlation in vertical direction	Correlationin diagonal direction	Correlation in horizontal direction
MR_1	-0.0188	0.0015	0.031
MR_2	-0.0068	0.0152	-0.0036
CT_1	-0.0539	0.0848	0.0639
CT_2	-0.0021	0.0107	-0.0015
CT_3	-0.0583	0.0929	0.0846

where E(m) and E(n) are the accepted value of m and n; $\alpha_m \alpha_n$ represnts are the standard deviations of m and n.

Figure 8(a–c) represents the original image pixel distribution in horizontal, vertical and diagonal directions respectively. Fig. 8(d–f) represents the encrypted image pixel distribution in all three directions. The correlation coefficient for all test images is tabulated in Table 5.

The pixel distribution in the encrypted images is entirely different from the original image pixel distribution which proves there exists no relationship between the image pixels in the original and the encrypted images. Unifrom pixel distribution in the cipher image leaks no clue to the intruders about the encryption scheme.

3.2 Information Entropy

The randomness of the information is evaluated with the help of Global Shannon entropy. It is given by,

$$K(L) = -\sum_{j=1}^{p} p(n_i) \log_2 p(n_i) \tag{9}$$

where p(ni) represents the symbol appearance probability.

Global entropy will not provide the randomness of the cipher image blocks at many times. To overcome the weakness of global entropy, modified Shannon entropy is computed by the randomly selecting the non-overlapping blocks in the encrypted image [25]. The Local entropy analysis is given in Table 6 for non overlapping blocks. From the table, the entropy value of all the encrypted images are almost adhere to the theoretical value.

3.3 Differential Analysis

Number of Pixel Change Rate (NPCR) and Unified Average Change in Intensity (UACI) are the measures to validate against differential attacks [26]. The observations are done by computing the relationship between the two encrypted images of size M $\times$ N. The minimum number of pixels altered is done by NPCR, and UACI does the average difference between those images. Let the

TABLE 6
Entropy Analysis

Sample images	Entropy of original image	Global Shannon entropy	Local Shannon entropy	
			30blocks	40blocks
MR_1	2.1582	7.9969	7.7797	7.697
MR_2	2.001	7.989	7.789	7.701
CT_1	1.4090	7.9243	7.871	7.861
CT_2	1.7045	7.9152	7.864	7.869

TABLE 7
NPCR Randomness Test

Tested Image 256×256		UACI Critical Value $U^{*-}_{0.05}=33.2824\%$ $U^{*-}_{0.01}=33.2255\%$ $U^{*-}_{0.001}=33.1594\%$ $U^{*+}_{0.05}=33.6447\%$ $U^{*-}_{0.01}=33.7016\%$ $U^{*-}_{0.001}=33.7677\%$		
Image Encryption Methods Value(s)	Reported	NPCR Test Results 0.05-level	0.01-level	0.001-level
Test 1	33.43%	Pass	Pass	Pass
Test 2	33.23%	Pass	Pass	Pass

TABLE 8
UACI Critical Value Tests

Tested Image Size M-by-N 256-by-256		Theoretically NPCR Critical Value $N^{*}_{0.05}=99.5693\%$ $N^{*}_{0.01}=99.5527\%$ $N^{*}_{0.001}=99.5341\%$		
Image Encryption Methods Value(s)	Reported	NPCR Critical level values 0.05	0.01	0.001
Test1	99.66%	Pass	Pass	Pass
Test 2	99.56%	Pass	Pass	Pass

two encrypted images be C1, C2.The NPCR and UACI values are estimated using the equations given

$$NPCR = \left(\frac{\sum_{l=1}^{M} \sum_{m=1}^{N} A(l, m)}{M \times N} \right) \times 100\% \tag{10}$$

$$UACI = \frac{1}{M \times N} \sum_{k,l} \left(\frac{C_1(k, l) - C_2(k, l)}{255} \right) \times 100\% \tag{11}$$

where A(l, m) is a bipolar array with the same size as images C_1 and C_2. A(l, m) is defined as,

$$A(l, m) = \begin{pmatrix} 0 \text{ if } C_1(l, m) = C_2(l, m) \\ 1 \text{ if } C_1(l, m) \neq C_2(l, m) \end{pmatrix}$$

Critical values of tests are consequently derived and calculated both symbolically and numerically. The critical values for NPCR and UACI are tabulated as below in Table 7 and Table 8.

From the Table 7 and 8, NPCR and UACI values passed the critical value tests, which validate the strengths and the effectiveness of the proposed scheme.

3.4 Keyspace Analysis

Keys play an essential constraint in any cryptosystem. For a successful scrambled algorithm, even a bit change in the keys ought to bring about totally undesired yield. Fig. 7(a) represents the encrypted

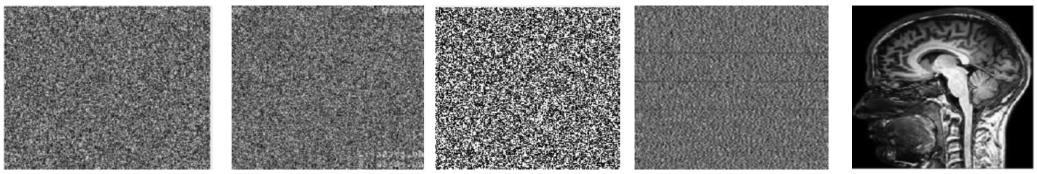


Fig. 9. (a) Encrypted cipher image with correct key K. (b) Decrypted image with wrong key1: Kw^1. (c) Decrypted image with wrong key2: Kw^2. (d) Decrypted image with wrong key3: Kw^3. (e) Decrypted image with correct key K.

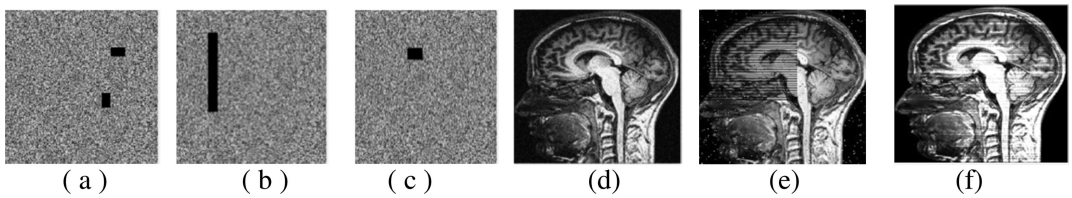


Fig. 10. Cropping attack analysis. (a) Cropping of 35 × 35 and 10 × 80. (b) Cropping of 190 × 10. (c) Cropping of 50 × 45. (d–f) Decrypted image of (a–c), respectively.

image using the key

$$K = \{\beta_{m+1} = 0.29453657866777,\ \mu = 3.88889999888899.$$

The three different key sets used for analysis is given by

$$\text{Keyset 1} = (\beta m + 1 = 0.29453557866777, \mu = 3.88889999888899)$$

$$\text{Keyset 2} = (\beta m + 1 = 0.29453657866777, \mu = 3.78889999888899)$$

$$\text{Keyset 3} = (\beta m + 1 = 0.29453657266777, \mu = 3.88889999888899)$$

Figure 9(b–d) represents the decrypted images of 9(a) using key sets K1, K2 and K3 respectively. Fig. 9(e) represents the decrypted image using original keys. From the figures, it is evident that the proposed encryption key is more susceptible and withstands the sensitivity of the proposed scheme.

3.5 Cropping Attack

When the images are transmitted through the channels, some portion of the cipher image may get affected. To validate this, intentional cropping is done in the encrypted images and decryption is done to prove the robustness of the encryption algorithm. Fig. 10(a)–(c) represents the intentional cropping on the cipher images and 10(d–f) represents the decrypted original images of (a–c) respectively. From the Figures, it is clear that the proposed scheme can withstand cropping attack and recovers some significant images.

3.5.1 Noise Attack Analysis: Noises like Gaussian, Speckle, Salt and Pepper, Poisson were tested on the encrypted image to check the sustainability and the security against the noise attacks. Fig. 11(a–d) depicts the encrypted image by adding the Gaussian noise with density as 0.02, poison noise, salt and pepper noise with density as 0.05, speckle noise with density as 0.04 respectively. Fig. 11(e–h) represents the decrypted outputs of (a–d) respectively. From the results, it is evident that even after including various noises to the encrypted images, the proposed decryption scheme withstands to produce the decrypted image output at an acceptable level.

This method involves RC5, DGT and LSIC encryption schemes. The chaotic logistic map generates the key for RC5 encryption. The logistic map involves key size of 256 bits and has 16 iterations.

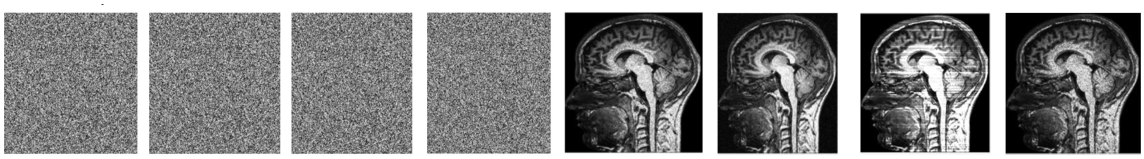


Fig. 11. Attack analysis using noise. (a) Gaussian noise added to the encrypted image. (b) Salt and pepper noise added to the encrypted image. (c) Poisson noise added to the encrypted image. (d) Speckle noise added to the encrypted image. (e–h) Decrypted images of (a–d).

TABLE 9
Comparison of the Proposed Algorithm [12]–[17]

METRICS	Algorithm Proposed	[12]	[13]	[14]	[15]	[16]	[17]
Vertical Correlation	**-0.0188**	-0.03850	-0.00330	0.00180	-0.00030	0.00560	0.00510
Horizontal Correlation	**0.0312**	-0.05190	0.00370	0.00370	0.00120	0.01320	-0.01250
Diagonal Correlation	**0.0015**	0.000460	0.01170	-0.00170	-0.00870	-0.00060	0.005830
NPCR	**99.660**	99.9960	99.620	99.610	99.6020	99.60770	99.5400
UACI	**33.430**	33.370	33.450	32.450	33.46820	33.45010	33.4670

It is followed by diffusion operation which in turn depends on DNA addition and subtraction rules. For performing DGT operation, a 2×2 matrix is chosen with 128 iterations. Finally, LSIC involves two keys of 256-bit size and the round involved is 8. Thus the complexity of the proposed encryption algorithm is $2^{256} \times 16 \times 28 \times 4 \times 104 \times 128 \times 2^{256} \times 2^{256} \times 8$.

3.6 Performance Comparison With the Existing Literature

This section provides the comparison of the proposed algorithm with the available encryption algorithms in the literature. The vertical, diagonal and horizontal correlation values, NPCR and UACI values are tabulated in Table 9. From Table 9, the correlation values are comparably better than the existing methods [14], [16], [17] and comparable with [13], [15]. NPCR and UACI show better results than [13]–[17] and comparable with [12].

4. Conclusion

In this paper, spectrum sensing using energy detection method was utilized to identify the unused free spectrum. Further, encryption scheme was utilized to provide robustness, validation and integrity of the encrypted biomedical data. For telemedicine applications in rural areas, these unused spectrum were used to transmit and exchange the encrypted biomedical data between doctors, patients and hospitals. Metrics like correlation, NPCR, UACI, chi-square tests and key space analysis were carried out to prove the strength and the robustness of the proposed encryption scheme.

Acknowledgment

The authors would like to thank SASTRA Deemed to be University, Thanjavur, India, for extending infrastructural support to carry out this work.

References

[1] R. Ebad and D. Ph, "Telemedicine: Current and future perspectives," *Int. J. Comput. Sci. Issues*, vol. 10, pp. 242–249, 2013.
[2] E. Tragos, "Spectrum assignment in cognitive radio networks: A comprehensive survey," *Surv. Tut.*, vol. 15, pp. 1108–1135, 2013, doi: 10.1109/SURV.2012.121112.00047.

[3] Y. He, H. Yin, and N. Zhao, "Multiuser-diversity-based interference alignment in cognitive radio networks," *AEU- Int. J. Electron. Commun.* vol. 70, pp. 617–628, 2016, doi: 10.1016/j.aeue.2016.01.018.

[4] P. Praveenkumar *et al.*, "Transreceiving of encrypted medical image–A cognitive approach," *Multimedia Tools Appl.*, vol. 77, pp. 8393–8418, 2018, doi: 10.1007/s11042-017-4741-7.

[5] P. Praveenkumar *et al.*, "Tamper proofing identification and authenticated DICOM image transmission using wireless channels and CR network," *Wireless Pers. Commun.*, vol. 97, pp. 5573–5595, 2017 doi: 10.1007/s11277-017-4795-x.

[6] D. Ravichandran, P. Praveenkumar, J. B. B. Rayappan, and R. Amirtharajan, "DNA chaos blend to secure medical privacy," *IEEE Trans. Nanobiosci.*, vol. 16, no. 8, pp. 850–858, Dec. 2017, doi: 10.1109/TNB.2017.2780881.

[7] Y.-Q. Zhang, X.-Y. Wang, J. Liu, and Z.-L. Chi, "An image encryption scheme based on the MLNCML system using DNA sequences," *Opt. Lasers Eng.* vol. 82, pp. 95–103, 2016, doi: 10.1016/j.optlaseng.2016.02.002.

[8] M. Kumar, A. Iqbal, and P. Kumar, "A new RGB image encryption algorithm based on DNA encoding and elliptic curve Diffie–Hellman cryptography," *Signal Process.*, vol. 125, pp. 187–202, 2016, doi: 10.1016/j.sigpro.2016.01.017.

[9] Q. Zhang and X. Wei, "A novel couple images encryption algorithm based on DNA subsequence operation and chaotic system," *Opt. - Int. J. Light Electron Opt.* vol. 124 pp. 6276–6281, 2013, doi: 10.1016/j.ijleo.2013.05.009.

[10] Q. Zhang, L. Guo, and X. Wei, "Image encryption using DNA addition combining with chaotic maps, *Math. Comput. Model.* vol. 52, pp. 2028–2035, 2010, doi: 10.1016/j.mcm.2010.06.005.

[11] G. Alvarez, S. Li, and L. Hernandez, "Analysis of security problems in a medical image encryption system," *Comput. Biol. Med.*, vol. 37, pp. 424–7, 2007, doi: 10.1016/j.compbiomed.2006.04.002.

[12] D. Ravichandran, P. Praveenkumar, J. B. Balaguru Rayappan, and R. Amirtharajan, "Chaos based crossover and mutation for securing DICOM image," *Comput. Biol. Med.*, vol. 72, pp. 170–184, 2016, doi: 10.1016/j.compbiomed.2016.03.020.

[13] P. Praveenkumar, R. Amirtharajan, K. Thenmozhi, and J. B. Balaguru Rayappan, "Medical data sheet in safe havens–A tri-layer cryptic solution," *Comput. Biol. Med.*, vol. 62, pp. 264–76, 2015, doi: 10.1016/j.compbiomed.2015.04.031.

[14] J. Xin Chen, Z. liang Zhu, C. Fu, L. Bo Zhang, and Y. Zhang, An image encryption scheme using nonlinear inter-pixel computing and swapping based permutation approach," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 23, pp. 294–310, 2015, doi: 10.1016/j.cnsns.2014.11.021.

[15] J. B. Lima, F. Madeiro, and F. J. R. Sales, "Encryption of medical images based on the cosine number transform," *Signal Process. Image Commun.*, vol. 35, pp. 1–8, 2015, doi: 10.1016/j.image.2015.03.005.

[16] G. Liu, A. Kadir, and H. Liu, "Color pathological image encryption scheme with S-boxes generated by complex chaotic system and environmental noise," *Neural Comput. Appl.*, vol. 27, pp. 687–697, 2016, doi: 10.1007/s00521-015-1888-x.

[17] A. Kanso and M. Ghebleh, "An efficient and robust image encryption scheme for medical applications," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 24, pp. 98–116, 2015, doi: 10.1016/j.cnsns.2014.12.005.

[18] A. V. Diaconu, "Circular inter-intra pixels bit-level permutation and chaos-based image encryption," *Inf. Sci.*, vol. 355–356, pp. 314–327, 2016, doi: 10.1016/j.ins.2015.10.027.

[19] R. Norcen, M. Podesser, A. Pommer, H. P. Schmidt, and A. Uhl, "Confidential storage and transmission of medical image data," *Comput. Biol. Med.*, vol. 33, pp. 277–292, 2003, doi: 10.1016/S0010-4825(02)00094-X.

[20] C. Lakshmi, K. Thenmozhi, J. B. B. Rayappan, and R. Amirtharajan, "Encryption and watermark-treated medical image against hacking disease—An immune convention in spatial and frequency domains," *Comput. Methods Programs Biomed.*, vol. 159, pp. 11–21, 2018, doi: 10.1016/j.cmpb.2018.02.021.

[21] D. Ravichandran, S. Rajagopalan, H. N. Upadhyay, J. B. B. Rayappan, and R. Amirtharajan, "Encrypted biography of biomedical image–A pentalayer cryptosystem on FPGA," *J. Signal Process. Syst.*, pp. 1–27, 2018. [Online]. Available: https://doi.org/10.1007/s11265-018-1337-z

[22] R. Acharya, U. C. Niranjan, S. S. Iyengar, N. Kannathal, and L. C. Min, "Simultaneous storage of patient information with medical images in the frequency domain," *Comput. Methods Programs Biomed.*, vol. 76, pp. 13–19, 2004, doi: 10.1016/j.cmpb.2004.02.009.

[23] H. Gao, Y. Zhang, S. Liang, and D. Li, "A new chaotic algorithm for image encryption, Chaos," *Solitons Fractals*. vol. 29, pp. 393–399, 2006, doi: 10.1016/j.chaos.2005.08.110.

[24] H. T. Panduranga and S. K. NaveenKumar, "Selective image encryption for medical and satellite images," *Int. J. Eng. Technol.*, vol. 5, pp. 115–121, 2013.

[25] Y. Wu, Y. Zhou, G. Saveriades, S. Agaian, J. P. Noonan, and P. Natarajan, "Local Shannon entropy measure with statistical tests for image randomness," *Inf. Sci.*, vol. 222, pp. 323–342, 2013.

[26] Y. Wu, J. P. Noonan, and S. Agaian, "NPCR and UACI randomness tests for image encryption," *Cyber J., Multidisciplinary J. Sci. Technol. J. Sel. Areas Telecommun.*, pp. 31–38, 2011.