 MCB, vol.15, no.2, pp.63-83, 2018

An Effective Approach of Secured Medical Image Transmission Using Encryption Method

Ranu Gupta[1, 3, *], Rahul Pachauri[2, 3] and Ashutosh Kumar Singh[1, 4]

Abstract: Various chaos-based image encryption schemes have been proposed in last few years. The proposed image encryption method uses chaotic map. The encryption is done by using 256 bit long external secret key. The initial condition for the chaotic mapping is evaluated by the use of external secret key along with the mapping function. Besides that, the proposed method is made more robust by applying multiple operations to the pixels of the image depending on the outcome of the calculation of the logistic map. Moreover, block shuffling of the image and modifying the secret key after encryption of each row is also done to add chaos to the proposed method.

Keywords: Chaotic logistic map, encryption, ciphers, image, security.

1 Introduction

Information privacy plays an important role in medical science. In last one decade, the exploitation of personal computer networks has grown extremely and it continues to grow further. Roughly all these networks are being connected to the global internet and getting interconnection also. Ultimately, a lot of information is being transmitted over the internet. The information may be audio, image, text and other multimedia data. In this paper, the emphasis has been given on medical images. Medical images are widely used in medical telediagnosis by the doctors. The patient information is something very personal and should not be disclosed publicly. Doctors are transmitting the patient information through public network in the form of image in order to consult expert doctors. Thus security plays a vital role in transmitting the information through internet network. Thus the proposed method of image encryption would help in keeping the patient information confidential. On the other hand general images are used in our day to day life. Security is the major concern over the extensive use of these images in the public networks. For example, the secrets of the health of a patient, military documents, bank details, government documents etc must be secured. Number of cyber crimes is increasing day by day. Conventional encryption schemes like simple-Data Encryption Standard (DES), triple-DES, Rivest Shamir Adleman (RSA), International Data

[1] Department of Electronics and Communication.

[2] Department of Computer Science Engineering.

[3] Jaypee University of Engineering and Technology, Raghogarh, Guna (M. P.) 473226, India.

[4] Thapar Institute of Engineering and Technology University, Patiala, 147004, India.

* Corresponding author: Ranu Gupta. Email: ranu.gupta@juet.ac.in.

Encryption Algorithm (IDEA) and Advanced Encryption Standard (AES) are not appropriate to make cryptosystems for large digital data. For encrypting the digital images, plenty of encryption schemes have been proposed [Chen and Zhao (1987); Bourbakis and Alexopoulos (1992); Chung and Chang (1998); Yen and Guo (1999); Cheng and Li (2000); Fridrich (1998); Scharinger (1998); Baptista (1999); Liao, Li, Pen et al. (2004); Han, Yu and Han (2006); Lian, Sun and Wang (2005); He, Zhang, Luo et al. (2009); Chen, Mao and Chui (2004); Guan, Huang and Guan (2005); Gao and Chen (2008)]. Scanning procedure for the encryption and simultaneously applying compression to the image [Bourbakis and Alexopoulos (1992)] was proposed. The encryption was done using two-dimensional standard baker map and chaotic logistic map [Fridrich (1998)] in symmetric encryption technique. The image was encrypted using Kolmogorov-flow based chaotic system [Scharinger (1998)]. Pseudorandom generator based on chaotic maps was proposed [Yoon and Hyoungshick (2010)] for the image encryption. The random behavior of chaos is effectively introduced into the image to encrypt the image. A medical image encryption process using Genetic algorithm was proposed [Pareek and Patidar (2016)]. Each pixel value of the image is represented as a chromosome which is represented by a binary string. The plain image is divided into sub-blocks and pseudorandom numbers are generated with the help of random number generator. The chromosomes of the image are shuffled according to the random numbers generated and then crossover of chromosomes is done in order to produce new chromosome to generate new offspring. A method using simple chaotic system using hyperbolic sine function was used for the encryption of medical images [Liu, Ma, Li, Lian and Zhang (2017)]. The image was diffused row wise and column wise. The pseudo random numbers are generated using hyperbolic sine chaotic function and then de-correlation amongst the pixels is done using these random numbers. A quantum image encryption was proposed for medical images [El-Latif, El-Atty and Talha (2017)]. The image was scrambled using quantum gray code. Then the encryption was done using quantum xor operation which was controlled by the values generated by the logistic-sine map. A combination of encryption and water marking was proposed by Dagadu et al. [Dagadu and Li (2018)] for the medical images. In this firstly the image was embedded with multiple watermarks using integer wavelet transform least significant bit (IWT-LSB) and then the watermarked image was encrypted using chaos and random permutation.

Chaos based encryption techniques are considered to be the best for practical use as they provide a high security, speed and low power consumption. The neighboring pixels of digital images have strong correlation, redundancy of data, and less affected by the small changes in the attribute to the pixels and bulk capacity of data. For real time image encryption method which takes lesser amount of time and at the same time does not make any compromise with the security are preferred. The above mentioned methods have less security and resist low to various types of attacks. To prove the statement true, various methods are compared with the proposed method in Section-4. An encryption scheme which provides better security but runs very slowly is less practical in real time processes.

The paper is prearranged as follows:

Section-2 provides a short overview of chaotic logistic function. Subsequently in Section-3 a brief review of the proposed chaotic logistic function is included along with its

implication. The results obtained with the proposed chaotic logistic method and its comparison with the other encryption method is shown in Section-4. Finally the paper is ended in Section-5.

2 Chaotic logistic function

The characteristics of the chaotic logistic map have made the cryptographers to develop new algorithms for image encryption. The one dimensional chaotic function [Chen and Zhao (1987)] is expressed as:

$$X_{n+1} = rX_n(1 - X_n) \tag{1}$$

where X_n takes values in the range from [0-1]. It is one of the simplest models in chaos. Taking initial condition at random as X_0=0.3, for different value of the controlling parameter *r*, the logistic function can be examined by experiments. When *r* is in the interval [0-3], the function is almost constant after numerous iterations with no chaotic behavior as shown in Figs. 1(a) and 1(b). When *r* is in the interval [3.5-4], it shows a chaotic behavior as shown in Fig. 1(c).

So the following conclusions can be drawn:

(a) For $r \in$[0-3], the logistic function is almost constant and should not be used for image encryption.
(b) When $r \in$[3.5-4], the chaotic map exhibits chaotic behavior, and hence the property of sensitivity and dependence. So it can be used for image encryption.
(c) For r =3.9999, the chaotic map pertains maximum randomness and hence it is used for encryption in this paper.

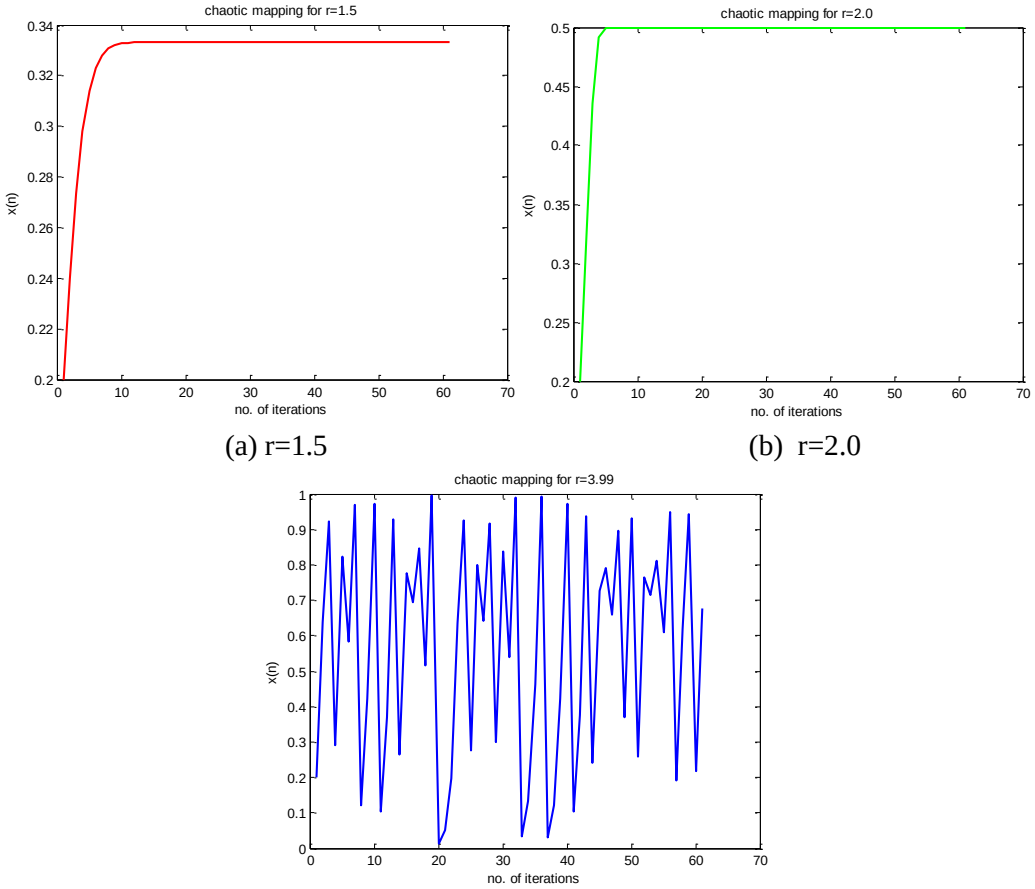
Chaos theory is a technical discipline that concentrates on nonlinear systems. The characteristics of chaotic systems are [Bourbakis and Alexopoulos (1992)]:

i Deterministic: Certain mathematical relationships is followed which make chaos deterministic.

ii Random in behavior but in actual fact it is not so.

iii Not predictable and non-linear: It is very sensitive to initial conditions and is not linear. Since it is random therefore cannot be predicted.

The encryption process is done by permutation of pixels followed by diffusion of the pixels. In this communication, the new proposed method effectively applies the chaotic properties [Chen and Zhao (1987)] such as randomness, sensitivity and mixing in the diffusion process in order to make secure image transfer.



(a) r=1.5 (b) r=2.0

(c) r=3.99 at x_0=0.2

Figure 1: Behavior of chaotic logistic function for different initial conditions

3 Proposed method

In the proposed image encryption method, the image is permutated by dividing it into blocks of 16x16 and shuffling the blocks horizontally and vertically. These blocks are then combined together to form one image. Here after, the external secret key of 32 ASCII characters (256-bit long) is used. A chaotic logistic function is used for image encryption. The initial condition is calculated by using the external secret key along with the mapping function to make it more chaotic. In addition to mapping function, ten various types of encryption operations are used. Number of iterations and the type of encryption is done depending on the last value of the secret key and the calculated value of the logistic map respectively. After encryption of each row the secret key is modified. The flow diagram of the proposed method is shown in Fig. 2. The proposed method is also explained through example in Tab. 1.

Table 1: Steps showing the Proposed Method

The example is demonstrated by taking only four ASCII keys, x = 500, y = 0.142, and image of 1x4 matrix

Let → | K_1 | K_2 | K_3 | K_4 | = | 25 | 128 | 142 | 56 |

Then M_i = | M_1 | M_2 | M_3 | M_4 | = | 0.3055 | 0.563 | 0.598 | 0.383 |

Then R = 186.0655

X_0 = R- $\lfloor R \rfloor$ = 0.0655

Further calculating Xi values with the chaotic function will be

= | X_1 | X_2 | X_3 | X_4 | | 0.244832 | 0.7395404 | 0.7704622 | 0.7073831 |

Let the shuffled image be Pi = | P_1 | P_2 | P_3 | P_4 | = | 42 | 246 | 108 | 192 |

Since X_1 = 0.24, therefore let 1st encryption operation be = NOT (P_i xor K_2). The image after 1st encryption will be=

| 85 | 137 | 19 | 191 |

Since X_2 = 0.74, let 2nd encryption operation be = NOT (P_i XOR K_4). The resulting image after 2nd operation will be =

| 146 | 78 | 212 | 120 |

Similarly X_3 = 0.77, let 3rd operation be = NOT (P_i XOR K_4). The resulting image after 3rd operation will be =

| 85 | 137 | 19 | 191 |

Since X_4 = 0.71, let the 4th operation be = (P_i XOR K_1 XOR K_3). The resulting image after 4th operation will be

C_i = | C_1 | C_2 | C_3 | C_4 | = | 194 | 30 | 132 | 40 |

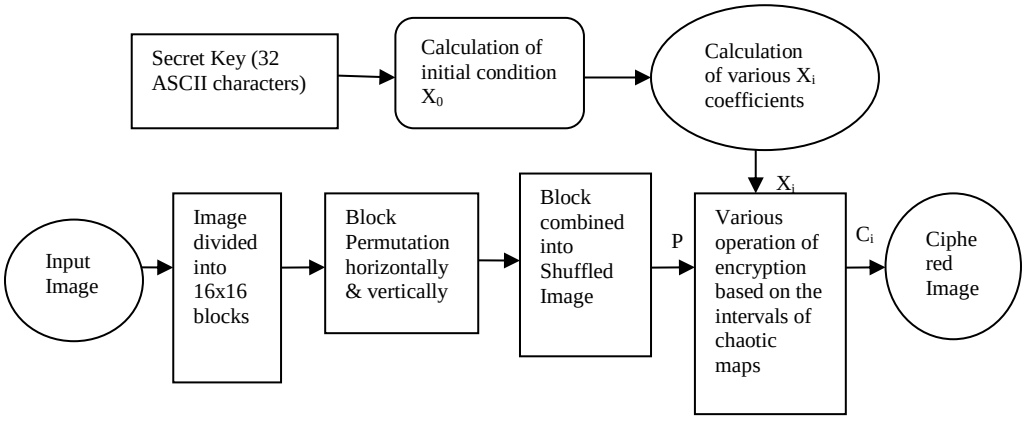


Figure 2: Block diagram of Proposed Method

Steps involved in the proposed method for the encryption of the image are as follows:

(a) The image is partitioned into sub blocks of 16×16 sizes. In case if the image size is odd then padding of zeros is done in order to divide the image into sub blocks of 16×16. The entire blocks are shuffled horizontally and vertically. The blocks are then combined into one to form one image.

(b) A secret key of 32 ASCII characters (256-bit long) is used in the proposed image encryption process. Each session key is divided into 8-bit of small blocks. The secret key can be represented as:

$$A_i = A_1, A_2, A_3, \ldots\ldots\ldots\ldots\ldots\ldots, A_{32} \text{ (in ASCII) (i=0-32)} \quad (2)$$

where, each A_i is the secret key or session key of 8-bit block.

(c) The initial condition (X_0) for the chaotic map is calculated as follows:

$$R = \left[\sum_{i=1}^{32} M_i(A_i)\right] \bmod 256 \quad (3)$$

$$X_0 = R - \lfloor R \rfloor \quad (4)$$

where,

$$M_i = \frac{A_i}{x} + y \quad (5)$$

and Ai, $\lfloor\ \rfloor$, and M_i are the decimal equivalent of the i^{th} session key, the floor function and mapping function of the i^{th} session key. Decimal value of ith session key is between 0-255. Whereas x is any natural number>255, and y is any rational number (<1) and up to three decimal digits.

(d) A chaotic logistic map as in Eq. (1) is used in the proposed method for image encryption.

(e) Then one by one the consecutive byte is read from the shuffled image. The range [0-1] has been divided into 30 different intervals in ten different groups as shown in Tab. 2. Different types of operations are assigned to each of the groups.

Tab. 2 shows the different intervals for the groups and their corresponding operations. Depending on the initial condition X_0 as calculated in Step (c), the next value of X is calculated using the logistic map. The output of the calculation of logistic map decides the operation that is to be performed on the corresponding pixel for encryption.

(f) Now the logistic map and the encryption of the pixel are iterated for $(A_{32})_{10}$ times. The encryption is done depending on the outcome of the logistic map. Step (e) is repeated for next pixel values of the image of the same row.

(g) When the encryption of a row is done, the session key A_1 to A_{32} is modified as follow:

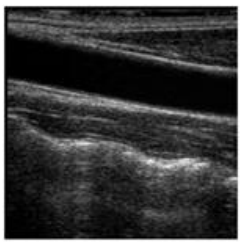
$$A_i = \left[(A_i)_{10} + (A_{32})_{10}\right] \bmod 256 \qquad (1 \le i \le 31) \quad (6)$$

(h) Then after, Steps (c)-(f) are repeated again until the whole of the image is completed.

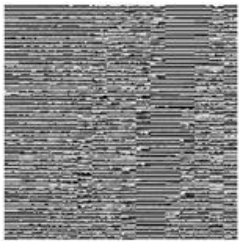
(i) In case of decryption process all the Steps from (b)-(e) are same except in Step (f) decryption is done in the reverse order.

Table 2: Non-overlapping 30 intervals and various operations for encryption/decryption

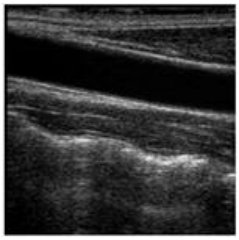
S. No.	Intervals	Operations for encryption/decryption
1.	0.00-0.03, 0.31-0.33, 0.61-0.63, 0.91	Encryption:-NOT (P) Decryption:-NOT (C)
2.	0.04-0.06, 0.34-0.36,0.64-0.66, 0.92	Encryption:-$((P)_{10}+(A_{14})_{10}+(A_{15})_{10})$ mod256 Decryption:-$(C)_{10}+512)-(A_{14})_{10}-(A_{15})_{10}$ mod256
3.	0.07-0.09,0.37-0.39,0.67-0.69, 0.93	Encryption:-$(P)_{10}$ XOR $(A_1)_{10}$ XOR $(A_2)_{10}$ Decryption:-$(C)_{10}$ XOR $(A_1)_{10}$ XOR $(A_2)_{10}$
4.	0.10-0.12, 0.40-0.42, 070-0.72, 0.94	Encryption:-(NOT (P XOR A_{10})) Decryption:-((NOT P) XOR A_{10})
5.	0.13-0.15, 0.43-0.45 ,0.73-0.75, 0.95	Encryption:-$(P)_{10}$ XOR (A_{25}) XOR (A_{26}) Decryption:-$(C)_{10}$ XOR (A_{25})
6.	0.16-0.18, 0.46-0.48,0.76-0.78, 0.96	Encryption:-$((P)_{10}+(A_{24})_{10}+(A_{25})_{10})$mod256 Decryption:-$((P)_{10}+512)-(A_{24})_{10}-(A_{25})_{10}$
7.	0.19-0.21, 0.49-0.51,0.79-0.81, 0.97	Encryption:-$(P)_{10}$ XOR $(A_{31})_{10}$ XOR $(A_{32})_{10}$ Decryption:-$(C)_{10}$ XOR $(A_{31})_{10}$ XOR $(A_{32})_{10}$
8.	0.22-0.24, 0.52-0.54,0.82-0.84, 0.98	Encryption:-(NOT(P XOR A_{23})) Decryption:-((NOT P) XOR A_{23})
9.	0.25-0.27,0.55-0.57,0.85-0.87, 0.99	Encryption:-$(P)_{10}$ XOR (A_5) Decryption:-$(C)_{10}$ XOR (A_5)
10.	0.28-0.30, 0.58-0.60, 0.88-0.90, 1.00	Encryption: -NOT (P). Decryption: -NOT (C).



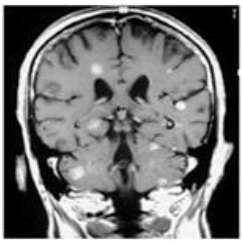
(a) Medical 1



(b) Medical 1 encrypted

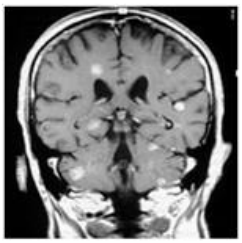


(c) Medical 1 decrypted



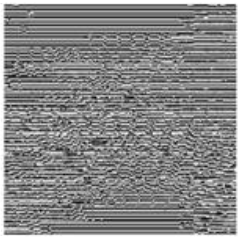
(d) Medical 2

(e) Medical 2 encrypted



(f) Medical 2 decrypted

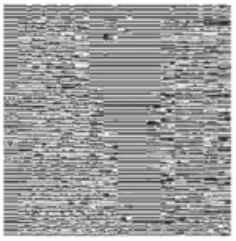
(g) Medical 3



(h) Medical 3 encrypt

(i) Medical 3 decrypted

(j) Medical 4



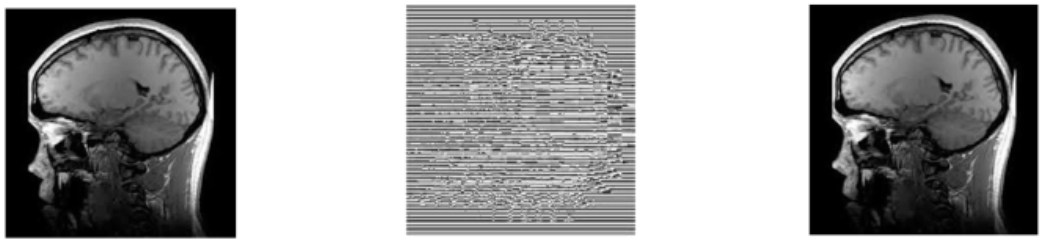
(k) Medical 4 encrypted

(l) Medical 4 decrypted

(m) Medical 5

(n) Medical 5 encrypted

(o) Medical 5 decrypted



(p) Medical 6 (q) Medical 6 encrypted (r) Medical 6 decrypted

Figure 3: Original and encrypted images with the proposed method

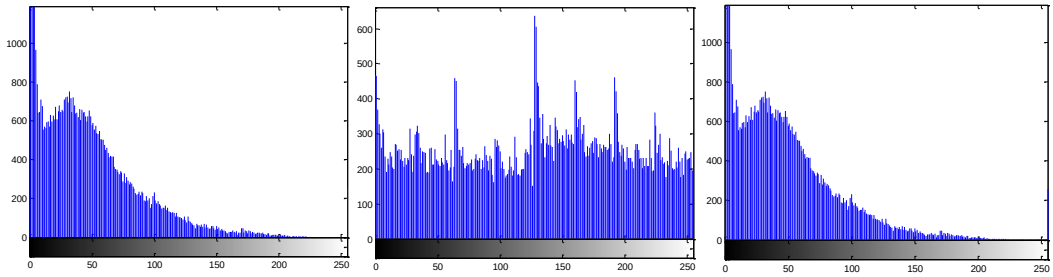
As shown in Fig. 3 six images (a), (d), (g), (j), (m) and (p) are encrypted by the proposed method using chaotic logistic function. It is evident in encrypted images as shown in Figs. 3(b), 3(e), 3(h), 3(k), 3(n) and 3(q) that it is very difficult to retrieve the original information, making the proposed method more efficient. Decrypted images as shown in Figs. 3(c), 3(f), 3(i), 3(l), 3(o) and 3(r) are similar to the original images there by showing that the proposed method is capable of recovering the original information.

4 Performance analysis

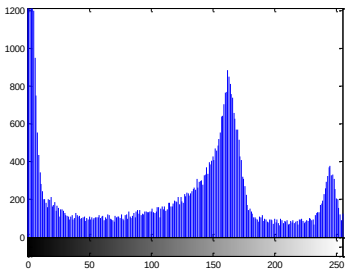
Ciphered images can be analyzed by doing statistical analysis. There are various statistical attacks that are designed on image encryption. Therefore, an ideal cipher should be robust against any statistical attack. Statistical, sensitivity and key space analysis are used to verify the efficiency of the image encryption method. These analyses are done in the proposed method in the following sections:

4.1 Histogram analysis

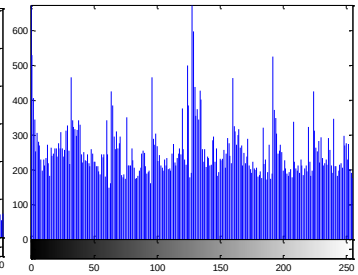
An image-histogram shows the distribution of color intensity level of image pixels. The histograms of various encrypted and original images have been shown in Figs. 4(b), 4(e), 4(h), 4(k), 4(n) and 4(q) and Figs. 4(a), 4(d), 4(g), 4(j), 4(m) and 4(p) respectively. Analysis of these histograms shows that both the histograms have widely different contents.



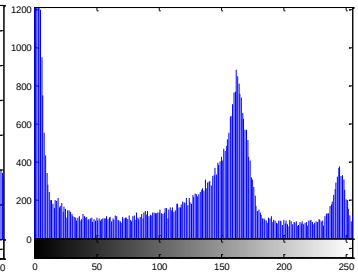
(a) Medical 1 Histogram (b) Medical 1 encrypted Histogram (c) Medical 1 decrypted Histogram



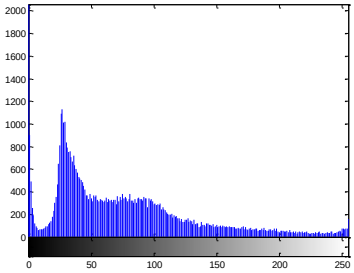
(d) Medical 2 Histogram



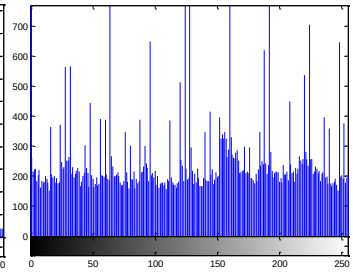
(e) Medical 2 encrypted Histogram



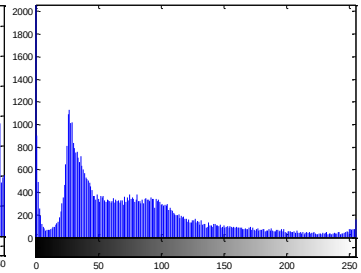
(f) Medical 2 decrypted Histogram



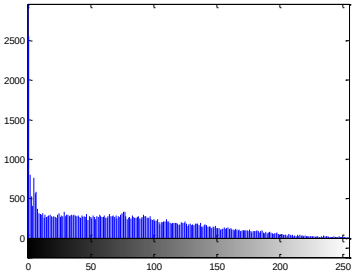
(g) Medical 3 Histogram



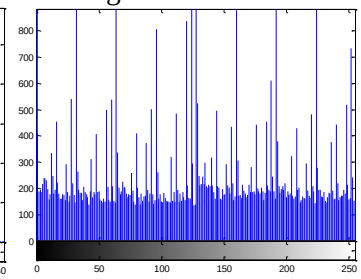
(h) Medical 3 encrypted Histogram



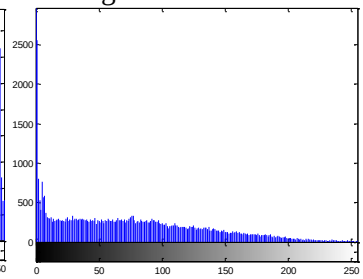
(i) Medical 3 decrypted Histogram



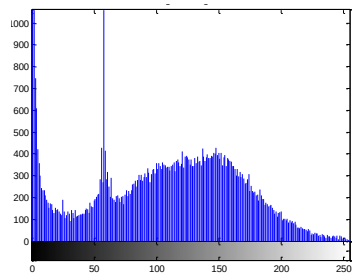
(j)Medical4 Histogram



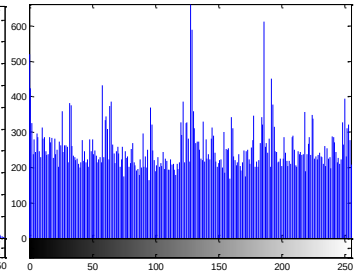
(k) Medical4 encrypted Histogram



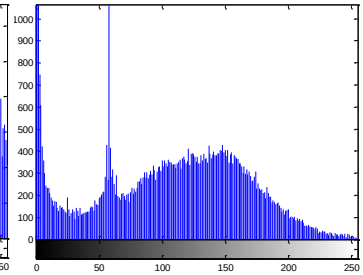
(l) Medical4 decrypted Histogram



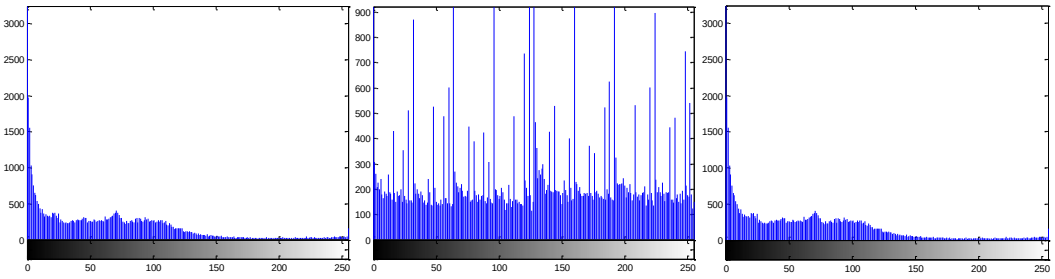
(m) Medical5 Histogram



(n) Medical5 encrypted Histogram

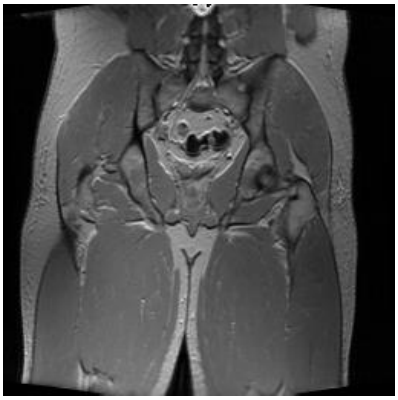


(o) Medical5 decrypted Histogram

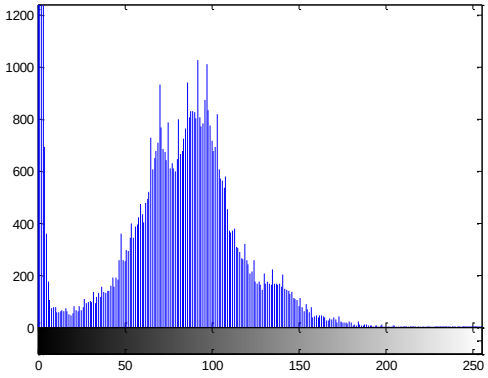


(p)Medical6 Histogram (q) Medical6 encrypted Histogram (r) Medical6 decrypted Histogram

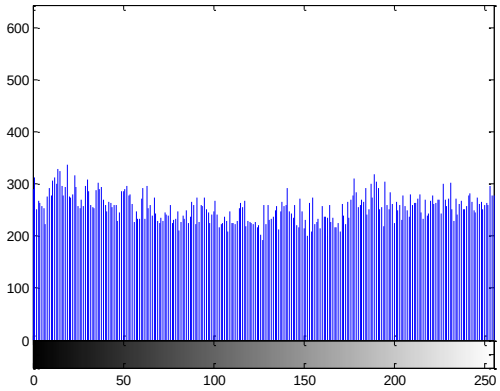
Figure 4: Histogram analyses of original & encrypted images



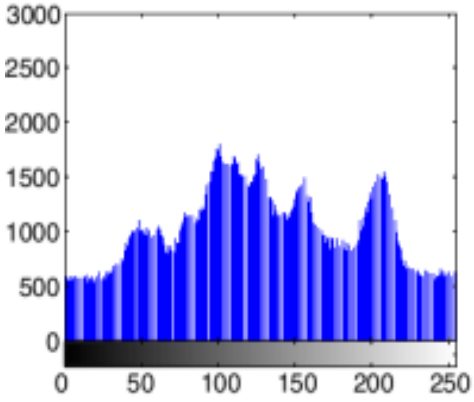
Original Medical



Medical Histogram



Encrypted Histogram [Abdmouleh et al (2013)



Encrypted Histogram [proposed method]

Figure 5: Comparison of histogram with the proposed method

As the histogram of the proposed method appears to be constant as compared to the other method, it can be said that the proposed method is better. Fig. 5 shows the comparison of histogram with the other method.

4.2 Correlation coefficient analysis

The value of correlation coefficient (C_r) shows the relation between the adjacent pixels. Its range is from -1<r<+1. The + sign means positive and -sign means negative correlations respectively.

Positive Correlation: -It means that pixels x and y of the image are positively correlated and both of them simultaneously increase or decrease.

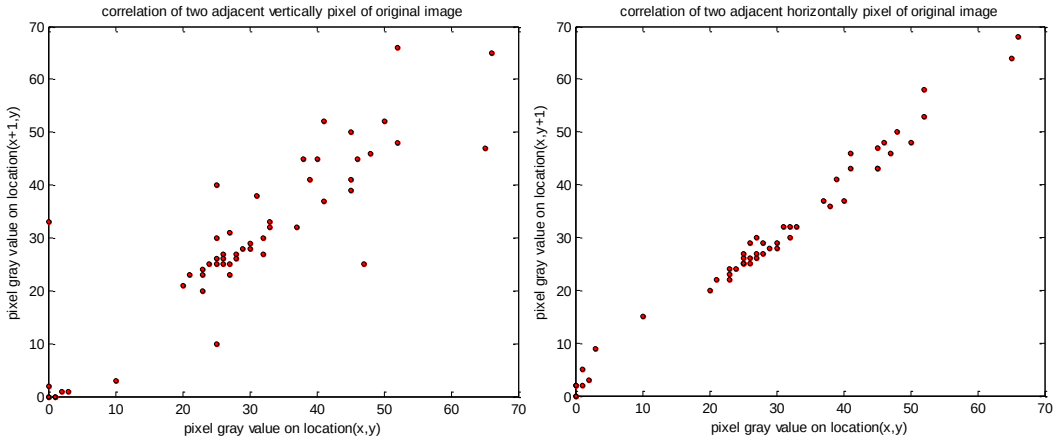
Negative Correlation: -It means that pixels of the image are negatively correlated and *x* and *y* are inversely related.

No Correlation: It means that *x* and *y* is weakly or not correlated. The correlation can differ on the "type" of data that is contained in the image.

The correlation between two horizontally, vertically and diagonally neighboring pixels in various original and encrypted images is calculated and analyzed. Following formula is used for calculation [Yen and Guo (1999)].

$$C_r = \frac{N\sum_{j=1}^{N}\left(x_j * y_j\right) - \sum_{j=1}^{N} x_j * \sum_{j=1}^{N} y_j}{\sqrt{\left(N\sum_{j=1}^{N} x_j^2 - \left(\sum_{j=1}^{N} x_j\right)^2\right) * \left(N\sum_{j=1}^{N} y_j^2 - N\left(\sum_{j=1}^{N} y_j\right)^2\right)}} \tag{7}$$

where *x* and *y* are the two neighboring pixels and *N* is number of pixels in the image. Tabs. 3 and 4 show the correlation coefficients of the original as well as encrypted images respectively. Its value for encrypted image is calculated in Tab. 4 by using the secret key **"1234567890qwertyuiopasdfghjklzxc"**. It is clear from the Tab. 4 that encrypted image has negligible correlation and thus the proposed method is secured and efficient. However, the neighboring pixels are highly correlated in the original image as shown in Tab. 3. Tab. 5 shows the comparison of correlation of coefficient for medical image.



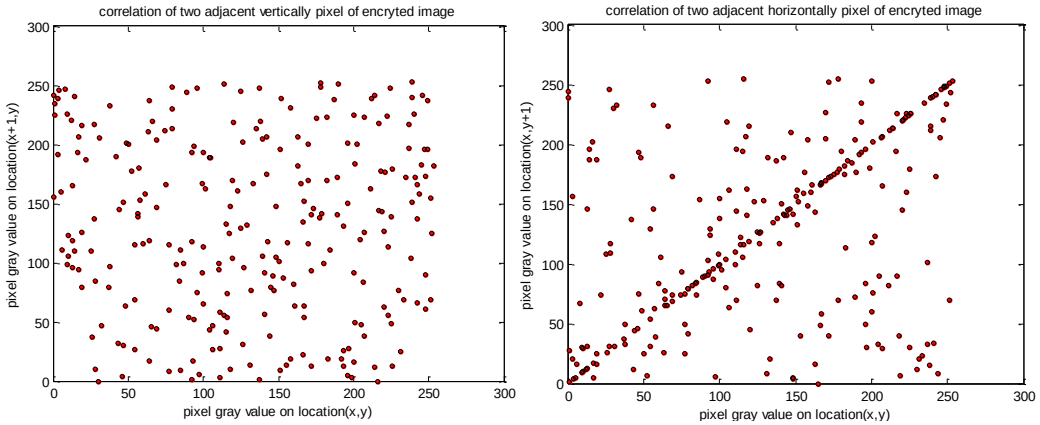


Figure 6: Horizontal and vertical Correlation coefficient of Medical original and encrypted image

Table 3: Correlation coefficients for the neighboring pixels in the original images

S. No.	Images	Size	Vertical	Horizontal	Diagonal
1.	Medical 1	389×367	0.8278	0.9194	0.8278
2.	Medical 2	203×200	0.9694	0.96714	0.9694
3.	Medical 3	225×225	0.971579	0.938491	0.971579
4.	Medical 4	400×307	0.9275	0.9718	0.9275
5.	Medical 5	225×225	0.9653	0.9794	0.9653
6.	Medical 6	225×225	0.9670	0.9578	0.9670

Table 4: Correlation coefficients for neighboring pixels in the encrypted images

Correlation Coefficient	[Pareek and Patidar (2016)]	[Liu, Ma, Li et al. (2017)]	[Dagadu and Li (2018)]	[El-Latif (2017)]	[Chen and Hu (2017)]	[Zhang, Zhu, Yang et al. (2015)]	Proposed method
Vertical	-0.0006	0.0062	0.0005	-0.0201	0.0171	-0.0084	-0.00111
Horizontal	-0.0043	0.0025	0.0063	-0.0152	-0.0028	-0.0131	0.001681
Diagonal	0.0019	0.0030	-0.0024	-0.0098	-0.0022	-0.0180	-0.0017
Average	0.0023	0.0039	0.0031	0.0150	0.01397	0.01317	0.00311

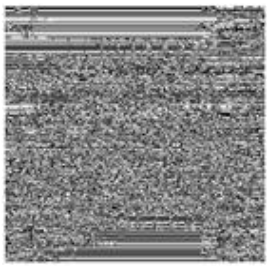
Table 5: Comparison of correlation coefficient of the proposed method (Medical image)

S. No.	Images	Size	vertical	horizontal	Diagonal
1.	Medical 1	389×367	-0.00199	0.11175	-0.00195
2.	Medical 2	203×200	0.001687	0.116906	0.000346
3.	Medical 3	225×225	-0.009576	0.122076	-0.000951
4.	Medical 4	400×307	-0.0194	0.1485	-0.0076
5.	Medical 5	225×225	-0.00175	0.001248	-0.00042
6.	Medical 6	225×225	-0.00111	0.001681	-0.0017

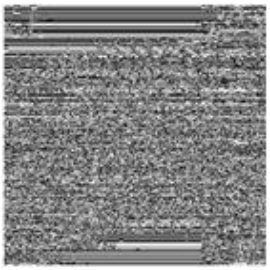
4.3 Sensitivity analysis

Sensitivity analysis can be done on the secret key as well as on the image. Any encryption method should be sensitive to the change in the session key. It means that a small change in the session key would result to totally different output. To test the sensitivity of the proposed method the original image is encrypted by three different session keys, first by changing the most significant bit and second by least significant bit. The three session keys are "1234567890qwertyuiopasdfghjklzxc", "m234567890qwertyuiopasdfghjklzxc", and "1234567890qwertyuiopasdfghjklzx2" respectively. The encrypted images and its correlation are shown in Fig. 7 and Tab. 6.

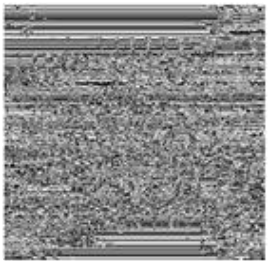
(i) Original medical image



(ii) Encrypted image



(iii) Encrypted image

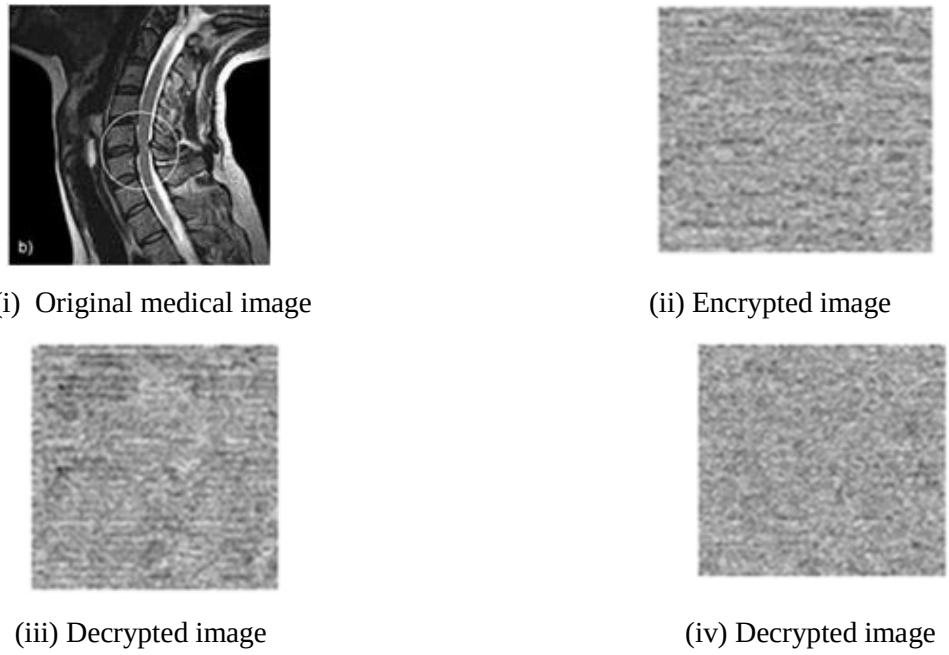


(iv) Encrypted image

Figure 7: Sensitivity test I: Frame (i) Original image, (ii), (iii), (iv) Encrypted images

Table 6: Correlation coefficients of the three encrypted images

S. No.	Images	Images	Correlation coefficient
1.	(ii)	(iii)	0.001128038
2.	(iii)	(iv)	0.001402722
3.	(iv)	(ii)	0.004229025



(i) Original medical image (ii) Encrypted image

(iii) Decrypted image (iv) Decrypted image

Figure 8: Key sensitivity test II: Frames (i) Original image, (ii) Encrypted image, (iii), (iv) Decrypted images

Tab. 6 shows the results of the correlation coefficients between the corresponding pixels of the three encrypted images (ii), (iii) and (iv). It shows that the proposed method is sensitive to the slight change in the secret key. Thereafter the encrypted image is attempted to decrypt with the changed secret key which fails to do so as shown in Fig. 8. Again the keys used were same as used in encryption process. Thus the proposed method is highly key sensitive.

4.4 Number of Pixels Change Rate (NPCR)

The number of pixels change rate (NPCR) measure the resistant against the change in the pixel in the original image. NPCR is calculated for the encrypted images by changing the pixel value of the original image. Higher NPCR approaching towards 100 (in percentage) shows that the encryption method is strong for the differential attack. Two encrypted images are *E1* and *E2* with one pixel change in the original image. The NPCR [Han, Yu and Han (2006)] is defined by the following equation:

$$NPCR = \sum_{i=1,j=1}^{x,y} \frac{D(i,j)}{x * y} * 100\% \tag{8}$$

If

$$E_1(i,j) = E_2(i,j) \quad \text{then} \quad D(i,j) = 0 \quad \text{else} \quad D(i,j) = 1$$

where *x* and *y* are the width and height of encrypted image. The *NPCR* for various images is calculated by the proposed encryption method and found to be above ***99%***. Tab. 7 shows the comparison of the NPCR with the proposed method for medical image. It comes to the conclusion that the proposed method is sensitive to changes in the image.

4.5 Unified Average Change Intensity (UACI)

The UACI shows the degree of resisting the differential attack. The UACI calculates the average change in the intensities of the pixel when there is change in the pixel value. UACI can be defined as

$$UACI = \sum_{i=j=1}^{w,h} \frac{\left|E_1(i,j) - E_2(i,j)\right|}{255 * w * h} * 100 \tag{9}$$

where *w* and *h* are the width and height of the image. The comparison of UACI with other methods is shown in Tab. 7.

Table 7: Comparison of NPCR and UACI criteria of proposed method and the other methods for Medical image

Methods	**NPCR%**	**UACI %**
[El-Latif (2017)]	99.5727	33.4553
[Liu, Ma, Li et al. (2017)]	99.5804	33.3227
[Dagadu and Li (2018)]	92.09	18.50
[Pareek and Patidar (2016)]	97	--
[Chen and Hu (2017)]	99.59	33.42
[Sokouti, Zakerolhosseini and Sokouti (2016)]	99.49	35.6
Proposed Method	**99.9984**	**32.7396**

4.6 Mean Square Error (MSE)

Mean square error is calculated between original image and encrypted image. It should be large for good encryption scheme. Mean square error indicates the amount of error present in the encrypted image as compared to original image. It signifies the amount of randomness that has been created to the pixel position as well as pixel values. Mean square error is calculated by the formulae:

$$MSE = \frac{1}{M * N} \sum_{i=1}^{M} \sum_{j=1}^{N} \left(E_{i,j} - I_{i,j}\right)^2 \tag{10}$$

where *E* and *I* are encrypted and original images respectively. The MSE for Medical image was calculated and found to be **13249.7820.**

4.7 Peak Signal to Noise Ratio (PSNR)

Peak signal to noise ratio is calculated between original image and encrypted image. It should be low for good encryption scheme which indicates that the encryption method is robust and has created randomness in the pixel position and its values. It is calculated by the formulae:

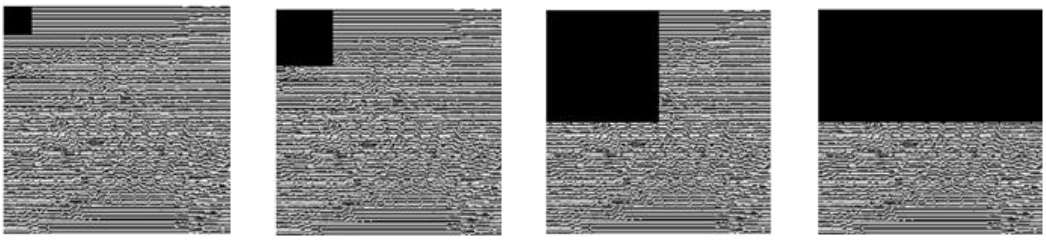
$$PSNR = 10\log_{10}\frac{I_{max}^2}{MSE} \tag{11}$$

where I_{max} is the maximum pixel value of the image. The PSNR for Medical image was calculated and found to be **6.90872.**

4.8 Occlusion attack

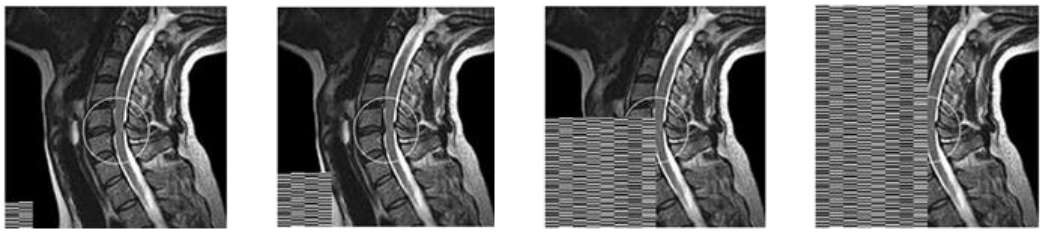
The original information may be corrupted during transmission. The occlusion attack analysis shows the power of defending the noise that is being introduced in the image during transmission and destroying the original information. The analysis was done by adding 6.25%, 12.5%, 25% and 50% occlusion to the baboon image as shown in Fig. 9.

Fig. 10(a) shows the graph between MSE and occlusion while Fig. 10(b) shows graph between PSNR and occlusion. The graph indicates the increase in MSE with respect to increase in occlusion in Fig. 10(a) whereas Fig. 10(b) shows the decrease in PSNR with increase in occlusion.



(i) (ii) (iii) (iv)

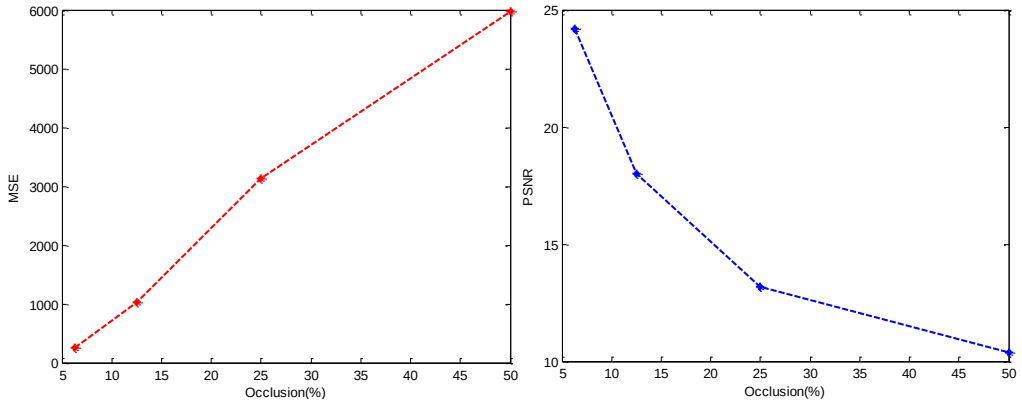
(a) Encrypted images



(i) (ii) (iii) (iv)

(b) Decrypted images

Figure 9: Resistance against occlusion attack (Information lost with 6.25%, 12.5%, 25% and 50% respectively of Medical image)



(a) (b)

Figure 10: Graph showing MSE and PSNR for 6.25%, 12.5%, 25% and 50% occlusion (for medical image)

4.9 Key space analysis

The secret key space should be such that the method should have the capability to resist brute force attack. The secret key of 256 bit long has $2^{256}(=1.157920892\times10^{77})$ different combinations. Thus the cipher method with such large number of combinations for the key is secured enough and reliable for practical use. However, the secret key length can be modified and can be easily used for practical application but too longer key is not suitable for real time transmission. Tab. 8 shows the comparison of key length.

Table 8: Comparison of key lengths

Methods	[Chen and Hu (2017)]	[Zhang, Zhu, Yang et al. (2015)]	[Pareek and Patidar (2016)]	[Liu, Ma, Li et al. (2017)]	Proposed
Length (Binary)	2^{128}	2^{202}	2^{128}	$>2^{100}$	2^{256}
Length (Decimal)	--	10^{45}	--	10^{60}	10^{76}

4.10 Time analysis

Besides security analysis which is done above, the running speed is also a prime parameter for better encryption method. The time is calculated for the encryption and decryption of Lena image by the proposed method. The time analysis is done on Intel(R) Core (™) 2 Duo CPU T5870 @2.00 GHz with 3 GB RAM computer. The coding is done on MATLAB 7.9.0(R2009b). Tab. 9 shows the encryption/ decryption time taken by the proposed method.

Table 9: Time taken in Encryption and Decryption by the proposed method

Image	Size	Encryption Time (s)	Decryption Time (s)
Lena	256×256	0.0232775	0.0224049

5 Conclusions

The proposed image encryption and decryption method is efficiently implemented to various images. The performance of various parameters concludes that the proposed method provide sufficient amount of security while transmitting the medical images through the network. It can also be concluded that the method can be efficiently used in real time applications. The proposed method utilizes the 256 bit long key which is well enough to resists brute force attack. Its future scope is that the proposed method can be modified by changing the key length and varying the method of calculating the initial condition for the logistic map. It can also be modified by varying the intervals and the encryption operations. As the medical images are vast which require large memory space and wider bandwidth to transmit. Therefore if image compression technique is applied in combination of encryption it will not only secure the information but will also reduce the bandwidth while transmitting. In this paper the various analyses is carried out. Finally, it can be concluded with the comment that the proposed encryption method would certainly be helpful for transmission and encryption of real time image like medical images.

Disclosure: This research did not receive any specific grant from funding agencies in the public, commercial, or government bodies. There is no conflict of interest.

Acknowledgments: The general images were taken from goggle sites. http://sipi.usc.edu/database/whereas; Medical images were taken from Government medical college, Gwalior, Madhya Pradesh, India.

References

Abdmouleh, M. K.; Khalfallah, A.; Bouhlel, M. S. (2013): Dynamic chaotic look-up table for MRI medical image encryption. *Proceedings of the International conference system, control, signal processing and informatics*, pp. 241-246.

Baptista, M. S. (1999): Cryptography with chaos. *Physics Letter A*, vol. 240, no. 1-2, pp. 50-54.

Bourbakis, N.; Alexopoulos, C. (1992): Picture data encryption using SCAN patterns. *Pattern Recognition*, vol. 25, no. 6, pp. 567-581.

Chen, G.; Mao, Y.; Chui, C. (2004): A symmetric image encryption schemes based on 3D chaotic cat maps. *Chaos Solitons and Fractals*, vol. 21, no. 3, pp. 749-761.

Chen, G.; Zhao, X. (1987): A self-adaptive algorithm on image encryption. *International Journal Software*, vol. 16, pp. 1975-1982.

Cheng, H.; Li, X. (2000): Partial encryption of compressed images and videos. *IEEE Transaction in Signal Processing*, vol. 48, no. 8, pp. 2439-2451.

Chen, X.; Hu, C. (2017): Adaptive medical image encryption algorithm based on multiple chaotic mapping. *Saudi Journal of Biological Sciences*, vol. 24, pp. 1821-1827.

Chung, K.; Chang, L. (1998): Large encrypting binary images with higher security. *Pattern Recognition Letters*, vol. 19, no. 5-6, pp. 461-468.

Dagadu, J. C.; Li, J. (2018): Context-based watermarking cum chaotic encryption for medical images in telemedicine applications. *Multimedia Tools and Applications*, https://doi.org/10.1007/s11042-018-5725-y.

El-Latif, A. A. A.; Abd-El-Atty, B.; Talha, M. (2017): Robust encryption of quantum medical images. *Special Section on Mobile Multimedia for Healthcare, IEEE Access*.

Fridrich, J. (1998): Symmetric ciphers based on two-dimensional chaotic maps. *International Journal of Bifurcation and Chaos*, vol. 8, no. 6, pp. 1259-1284.

Gao, T.; Chen, Z. (2008): Image encryption based on a new total shuffling algorithm. *Chaos Solitons Fractals*, vol. 38, no. 1, pp. 213-220.

Guan, Z. H.; Huang, F.; Guan, W. (2005): Chaos-based image encryption algorithm. *Physics Letters A*, vol. 346, no. 1-3, pp. 153-157.

Han, F.; Yu, X.; Han, S. (2006) Improved baker map for image encryption. *International Symposium on Systems & Control in Aerospace & Astronautics*, vol. 2, pp. 1273-1276.

He, B.; Zhang, F.; Luo, L.; Du, M.; Wang, Y. (2009): An image encryption algorithm based on spatiotemporal chaos. *International Congress on Image and Signal Processing*, vol. 1-5.

Lian, S.; Sun, J.; Wang, Z. (2005): A block cipher based on a suitable use of chaotic standard map. *Chaos Solitons & Fractals*, vol. 26, no. 1, pp. 117-129.

Liao, X.; Li, X.; Pen, J.; Chen, G. (2004): A digital secure image communication scheme based on the chaotic Chebyshev map. *International Journal of Communication Systems*, vol. 17, no. 5, pp. 437-445.

Liu, J.; Ma, Y; Li, S.; Lian, J.; Zhang, X. (2017) A new simple chaotic system and its application in medical image encryption. *Multimedia Tools and Applications*, https://doi.org/10.1007/s11042-017-5534-8.

Pareek, N. K.; Patidar, V. (2016) Medical image protection using genetic algorithm operations. *Soft Computing*, vol. 20, pp. 763-772.

Scharinger, J. (1998): Fast encryption of image data using chaotic Kolmogorov flows. *Journal of Electron Imaging*, vol. 7, no. 2, pp. 318-325.

Sokouti, M.; Zakerolhosseini, A.; Sokouti, B. (2016): Medical image encryption: An application for improved padding based GGH encryption algorithm. *Open Medical Informatics Journal*, vol. 10, pp. 11-22.

Yen, J.; Guo, J. (1999): A new image encryption algorithm and its VLSI architecture. *IEEE Workshop on Signal Processing System*, vol. 3, pp. 430-437.

Yoon, J. W.; Hyoungshick, K. (2010): An image encryption scheme with a pseudorandom permutation based on chaotic maps. *Communication in Nonlinear Science & Numerical Simulation*, vol. 15, no. 12, pp. 3998-4006.

Zhang, L; Zhu, Z.; Yang, B.; Liu, W.; Zhu, H. et al. (2015): Medical image encryption and compression scheme using compressive sensing and pixel swapping based permutation approach. *Mathematical Problems in Engineering*, vol. 2015.