International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 15 (2018) pp. 12353-12363

Medical Image Steganography using Dynamic Decision Tree, Piecewise Linear Chaotic Map, and Hybrid Cryptosystem

Mamta Jain

Department of Computer Science and Engineering,
Amity School of Engineering and Technology, Amity University, Rajasthan, Jaipur, India.

Abstract

New security system has been proposed for insensitive data of patient medical records. Medical records of patient are secured by concealing data with the help of dynamic decision tree, piecewise linear chaotic map (PWLCM), and hybrid cryptosystem. The proposed algorithm comprises of five stages, diffusion and confusion of secret data, generation of pseudo-random sequences (Pseudo-random sequences is generated by linear feedback shift register, non-linear forward feedback shift register, and piecewise linear chaotic map), permutation and XORing using pseudo-random sequences, encryption of keys using RSA cryptosystem, and steganography using dynamic decision tree. Security analysis of proposed technique has been carried out. Performance analysis is observed using MSE, PSNR, maximum embedding capacity as well as by histogram analysis between various medical grey stego and cover images.

Keywords: Dynamic decision tree, confusion, diffusion, steganography, cryptography, encryption, decryption, embedding.

INTRODUCTION

Medical systems are rapidly shifting into the cloud and mobile environments for data security. In the era of the healthcare, the doctor tests the medical image along with the patient information, which is sent from remote areas, that helps in receiving medical treatment by proper diagnosis and immediate care. Security parameters such as authentication, integrity, confidentiality and availability have to be considered for secure transmission, Department of Health and Human Services (DHHS) forced regulations for data security and privacy under the health insurance portability and accountability act (HIPAA) of 1996 [1].

Along with traditional cryptosystem schemes[13], chaos based techniques are also used these days, because of properties such as ergodicity, mixing property, sensitivity to initial conditions, system parameters and which can be considered analogous to ideal cryptographic properties such as confusion, diffusion, balance and avalanche properties. Hence, many chaos-based encryption systems also proposed [4, 7, 9].

Steganography, hiding of secret data in cover image, such that the changes made to the image are imperceptible [2, 3, 5, 6, 8, 10, 12, 13]. Steganography methods efficiency can be measured by the three valuable specifications: secrecy, capacity, and visual imperceptibility.

Thiyagarajan *et al.* proposed steganography methodology for hiding patient information inside a medical cover image using a dynamic key produced by graph 3 coloring problem [11].

Jain *et al.* recently proposed steganography technique for hiding secret medical record in their medical image using the concept of diagonal queue. In this technique, the secret cipher blocks and sub-blocks are assigned dynamically to selected diagonal queues for embedding [12].

Jain *et al.* [13] proposed a security system which utilized RSA, Decision tree, Dynamic keys and Grey-alpha medical cover image. The dynamic keys were considered as the secret key for the algorithm, and public key for RSA. The algorithm is comprises of three rounds. The first round encryption using RSA Cryptosystem, the outcome is organized in various blocks (using dynamic keys). The second round, alpha channel will be separated from the RGBA image and merged to the medical grey image to improve the hiding capacity, and organized the grey-alpha channel medical cover image into various blocks using dynamic key. In third Round, Secret cipher blocks are assigned to grey-alpha channel medical cover image blocks using decision tree. In fourth round, steganography process is done using two bit per channel in grey/alpha channel (5^{th} to 8^{th} bit), where channel is decided in third round.

We have found that, the article proposed the concept of decision tree for selection of channel for data embedding, which is static in nature. So that same input bit sequence select the same channel for data embedding.

In this paper, we have proposed a hybrid (symmetric and public key) cryptosystem with stego security system by using the modern cryptography (diffusion, confusion and RSA), PWLCM, linear feedback shift register (LFSR),Non-linear forward feedback shift register (NLFFSR) and dynamic decision tree. The proposed algorithm comprises five stages, viz. (i) Diffusion and confusion of secret data bits (ii) Generation of pseudo-random sequences (Pseudo-random sequences is generated by LFSR, NLFFSR and chaotic map) (iii) Permutation and XORing using pseudo-random sequences (iv) Encryption of key using RSA (iv) Steganography using the grey channel and dynamic decision tree matching concept.

This novel approach can be understood by referring the following divisions. In division 2, brief description of piecewise linear chaotic map, LFSR, NLFFSR, RSA, and decision tree are discussed. In division 3, the proposed method is discussed. In division 4, security analysis is done. The

performance analysis is done in division 5. Finally the work is concluded in division 6.

BRIEF DESCRIPTION OF PIECEWISE LINEAR CHAOTIC MAP, LFSR, NLFFSR, RSA CRYPTOSYSTEM, DECISION TREE, BREADTH FIRST SEARCHING

In this section, various techniques have been discussed as follows:

A. Basics of piecewise chaos theory, LFSR, and NLFFSR

- **Piecewise linear chaotic sequence:** Chaos is a pseudo-random process produced in nonlinear dynamical systems. It is non periodic in nature, non convergent, and extremely sensitive to the initial condition. The chaos theory was developed in the early 1960s from many research disciplines such as mathematics, physics, biology, chemistry, and engineering. There exists relationship between the chaos and cryptography [7] such as 1) ergodicity and confusion, 2) sensitivity to initial condition and diffusion with a small change in the secret key or plain text, 3) mixing property and diffusion,4) deterministic dynamics and deterministic pseudo randomness, and 5) structure complexity and algorithm complexity.

The PWLCM (piecewise linear chaotic map) denoted as following equation

$$x(n+1) = \begin{cases} C_\mu(x(n)) & \\ \frac{x(n)}{\mu} & if\ x(n)\epsilon[0,\mu); \\ (x(n)-\mu)\times\frac{1}{0.5-\mu} & if\ x(n)\epsilon[\mu,0.5]; \\ C_\mu\big(1-x(n)\big) & if\ x(n)\epsilon[0.5,1); \end{cases} \quad (1)$$

Where μ is the control parameter $0 < \mu < \frac{1}{2}$.

The PWLCM has uniform invariant density function and $\delta - like$ correlation. It can be easily realized by both hardware and software, since its iterations only involve divisions and additions.

- **Linear feedback shift register:** A Linear feedback shift register (LFSR) is a method for generating binary sequences [7]. Figure 1 shows a general model of an n-bit LFSR. LFSR are extremely good pseudo-random binary sequence generators. It generates pseudo-random binary sequence , which has very good randomness and statistical properties .

An example of 4-bit LFSR is considered to demonstrate the functioning of LFSR with the feedback function

$$f = 1 + x + x^4 \quad (2)$$

Its initial bit values are used (1111). The output sequence Z_n: 011111000000001. . . Generated by LFSR in is periodic of period 15. The pseudo-random sequence depends upon the initial seed value and feedback function [9].

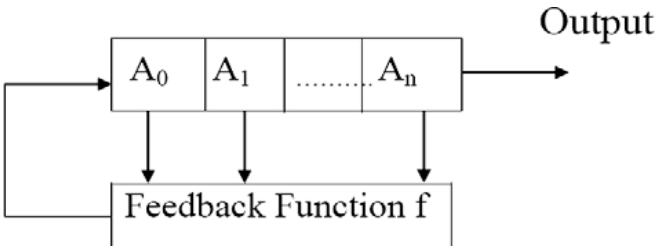


Figure 1: A general model of n bit linear feedback shift register [7]

- **Non-linear forward feedback shift register:** A Non-Linear forward feedback shift Register (NLFFSR) is a mechanism for generating pseudo random binary sequences [4]. Figure 2 shows a general model of a 4-bit NLFFSR. It is a Non-linear forward feedback shift register with a feedback function f. NLFFSR are extremely good pseudo random binary sequence generators.

A model of 4-bit NLFFSR is considered to demonstrate the functioning of NLFFSR with the feedback function using equation (2) and the non-linear function g defined by $a_{n-1}.a_{n-3} \oplus a_{n-2}.a_{n-4}$ forming non-linear feed forward shift register generator. Its initial bit values are used (1111). The output sequence Z_n : 011111000000001 generated by NLFFSR in are periodic of period 15.

The usefulness of these sequences depends in large part on their having nearly randomness properties. Therefore such sequences are termed as pseudorandom binary sequences. The balance, run and correlation properties of these sequences make them more useful in the selection of secret keys. The NLFFSR generated sequences are of great importance in many fields of engineering and sciences.

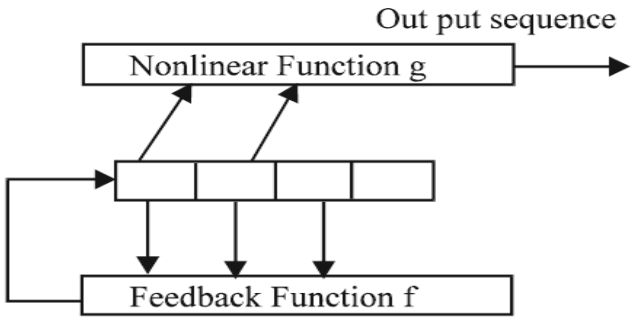


Figure 2: A General model of 4-bit NLFFSR [4]

B. RSA cryptosystem with security concern

The RSA cryptosystem is a public-key encryption method. This cryptosystem involves three steps, which are key generation, encryption and decryption. The security of the RSA cryptosystem is fundamentally based on, the factoring of large prime numbers [13].

C. Decision tree

A decision tree is used for classification, prediction and facilitating decision making rules in linear decision issues. It is a graphical representation, which shows decisions and feasible outcomes [13].

D. Breadth first search (BFS) technique

BFS is a data structure algorithm for traversing or searching tree or graph. It starts by the root of the tree or graph. It explores the neighbor nodes first, after that move to the next level neighbors.BFS algorithm can be used to find a shortest path between two vertices x and y[13].

PROPOSED WORK

In the proposed security system, it includes the input medical secret data of patient, pseudorandom numbers, diffusion, confusion, secret keys and grey channel medical cover image to create a secure hybrid crypto-stego algorithm with the help of dynamic decision tree. Figure 3 and 4 shows the architecture and work flow of this algorithm.

A. Cover Image and Secret Message

In this system select a grey medical image as a cover image and a secret message of patient information, which will be embedded in the cover image.

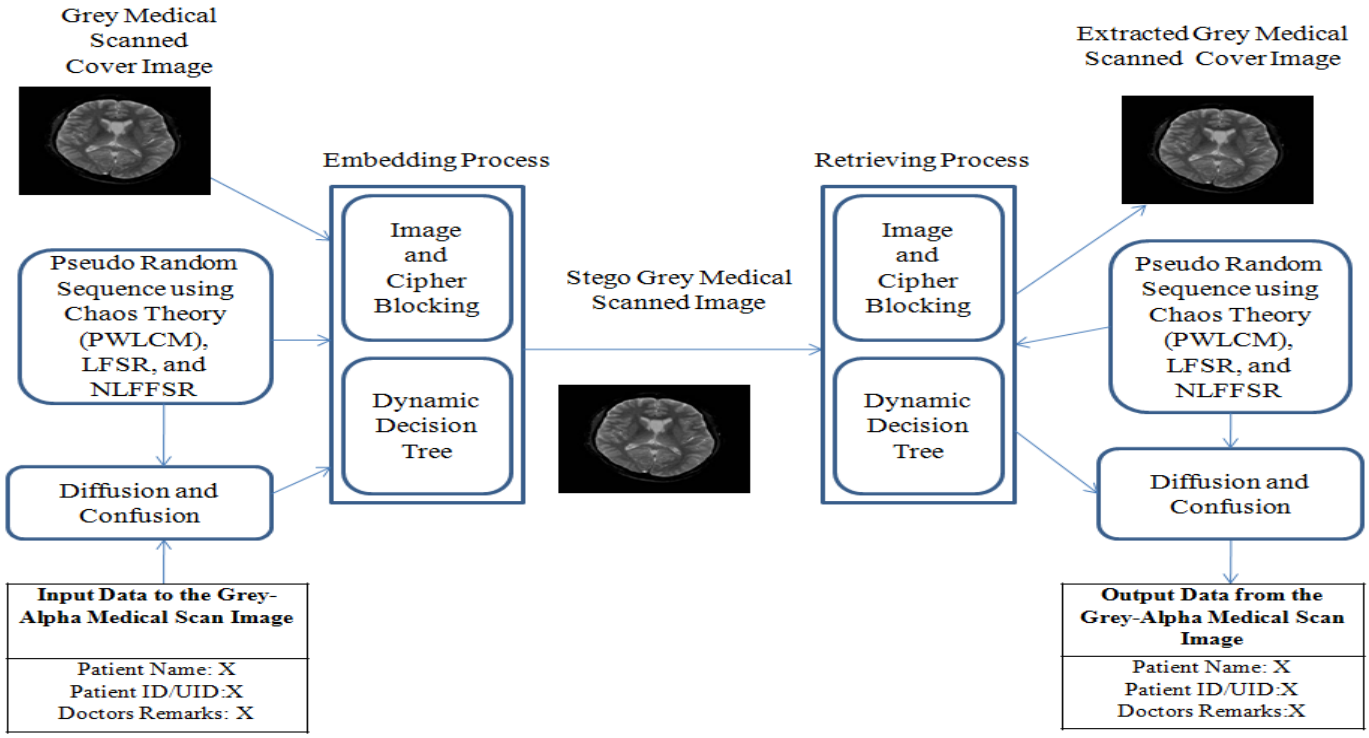


Figure 3: Architecture of proposed algorithm

B. Random number generation using piecewise linear chaotic map

Here, generation of pseudo-random sequences is discussed.

- The secret key consist of floating-point numbers $\mu_x$as well as $\mu_y \in$(0,0.5), and initial value of x_0,y_0.
- By iterating Eq. (1) 2 times size of the secret data, the pseudo-random sequence generated as $XKey$ and $YKey$.
- and$Y1$ will be generated from $Xkey$ and $YKey$ as follows:

$$For i = 1 \text{ to } 20 * sizeofthesecretdata$$
$$X1(i) = \lfloor Xkey(i) * 256 \rfloor; \quad (3a)$$
$$Y1(i) = \lfloor YKey(i) * 256 \rfloor; \quad (3b)$$
$$End$$

Divide $X1$ and $Y1$into blocks as $X2$ and $Y2$, each block is size $256 * 256$.

Divide $X1$ and $Y1$into blocks as $X4$ and $Y4$, each block is $sizeofthesecretdata$.

Reshape the $X2$ and $Y2$ to $X3$ and $Y3$ as follows,

$$For\ i = 1\ to\ size\ of\ secret\ data/(total\ number\ of\ blocks)$$
$$X3(i) = \text{reshape}(X2(i),256,256) \quad (4a)$$
$$Y3(i) = \text{reshape}(Y2(i),256,256) \quad (4b)$$
$$End$$

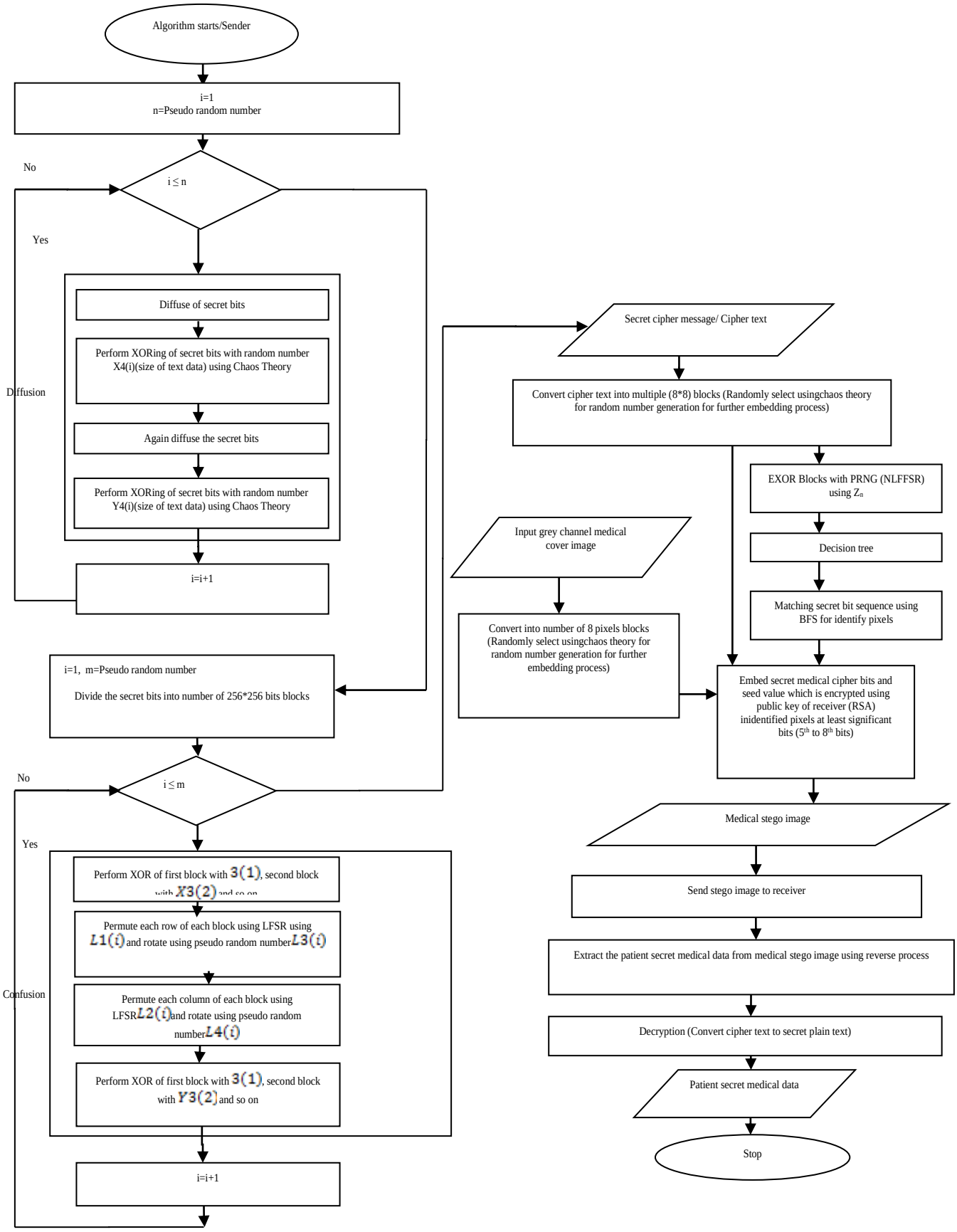


Figure 3: Flow diagram of work methodology

C. Pseudo random sequence generation using NLFFSR

Using feedback function by equation (2) and the non-linear function g defined by $a_{n-1}.a_{n-3} \oplus a_{n-2}.a_{n-4}$forming non-linear feed forward shift register generator, the pseudo random sequences generated as follows:

$For\ i = 1\ to\ (secret\ data\ size)$

Generate the pseudo-random sequences $(NL(i))\ and\ combine\ 8bits\ to\ form\ NLL(i)$using the seed value $(Y1(i) * X1(i))mod14 + 1$.

End

D. Pseudo random sequence generation using LFSR

Here, the various pseudo random sequences are generated as follows:

- $For\ i = 1\ to\ (secret\ data\ size)$
  - Generate the pseudo-random sequences $(L1(i))$ using the primitive root, $f = 1 + x^4 + x^5 + x^6 + x^8$, and the seed value is $X1(i)$.
  - Generate the pseudo-random sequences $(L2(i))$ using the primitive root, $f = 1 + x^4 + x^5 + x^6 + x^8$, and the seed value is $Y1(i)$.
  - Generate the pseudo-random sequences $(L3(i))$ using the primitive root, $f = 1 + x^2 + x^3$, and the seed value is $(X(i) - Y1(i))mod7 + 1$.
  - Generate the pseudo-random sequences $(L4(i))$ using the primitive root, $f = 1 + x^2 + x^3$, and the seed value is $(Y1(i) + X1(i))mod7 + 1$.
  - Generate the pseudo-random sequences $(L5(i))$ using the primitive root, $f = 1 + x + x^2$, and the seed value is $(Y1(i) * X1(i))mod3 + 1$.

End

E. XORING of secret data

- Perform XOR operation from left to right bits of secret data $t = t_1\, t_2 \ldots . t_n$ to $t' = t_1, t'_2 \ldots . t'_n$ using following equation:

  For $m = 1\ to\ n - 1$

  $$t'_{m+1} = t_{m+1} \oplus t_m \qquad (5)$$

- Perform XOR operation from right to left bits of secret data $t = t_1, t_2 \ldots . t_n$ to $t' = t'_1 t'_2 \ldots . t_n$ using following equation:

  For $m = n\ to\ 2$

  $$t'_{m-1} = t_{m-1} \oplus t_m \qquad (6)$$

- Perform XOR operation between pseudorandom sequence $X1$ generated using equation (3a)and secret data, S using following equation:

  $$S' = S(\oplus)X1 \qquad (7)$$

- Perform XOR operation between pseudorandom sequence $Y1$ generated using equation (3b)and secret data, S using following equation:

  $$S'' = S(\oplus)Y1 \qquad (8)$$

F. Diffusion technique

Let the secret data is S, and following steps are used for diffusion process.

- Generate pseudo random sequence using following equation:

  $$N = NLL(1) \qquad (9)$$

- $For\ i = 1\ to\ N$
  - Perform XOR of secret data from left to right using equation (5)and called as S'.
  - Perform XOR of S' with $X4(i)$ which is generated using equation(3a) and called as S''.
  - Perform XOR of secret data from right to left using equation (6) and called as S'''.
  - Perform XOR of S''' with $Y4(i)$ which is generated using equation (3b) and called as S''''.
  - $i = i + 1$

  End

G. Confusion technique

Let the secret data is S, and following steps are used for diffusion process.

- Generate pseudo random sequence using following equation:

  $$N = NLL(2) \qquad (10)$$

- Divide the secret data S into blocks of 256*256 bytes.

For each secret data block repeat the following steps:

- $For\ i = 1\ to\ N$
  - EXOR secret data block with $X3(i)$, which is generated

using equation (4a)

- Permute first row elements using pseudo random sequence $L1(1)$, second row with $L1(2)$ and so on.
- Rotate first row elements using pseudo random sequence $L3(1)$, second row with $L3(2)$ and so on.
- Permute first column using pseudo random sequences $L2(1)$, second column using $L2(2)$ and so on.
- Rotate first row elements using pseudo random sequence $L4(1)$, second row with $L4(2)$ and so on.
- EXOR secret data block with $Y3(i)$, which is generated using equation (4a)
- $i = i + 1$

  End

- Combine the entire blocks as S.

H. Secret cipher data blocking

- Convert cipher text into multiple (8*8) blocks.
- Permute first block elements using pseudo random sequences $L3(1)$, second block with $L3(2)$ and so on.
- Permute first 8 blocks using pseudo random sequences $L4(1)$, next 8 blocks using $L4(2)$ and so on.

I. RSA cryptosystem

- RSA cryptosystem is used to encrypt the size of the data along with seed values D of chaos theory for random number generation using public key of receiver.

$$D' = RSACryotsystem\,(D, Publickeyofreceiver) \quad (11)$$

- Encrypted seed values will be embedded in medical cover image.

J. Decision tree

Decision tree will be used as a reactive mechanism, for giving decisions to select the particular pixel in grey channel [13]. All the eight terminal nodes in decision tree are assigned a number from 1 to 8 from left to right direction as shown in Figure 4.

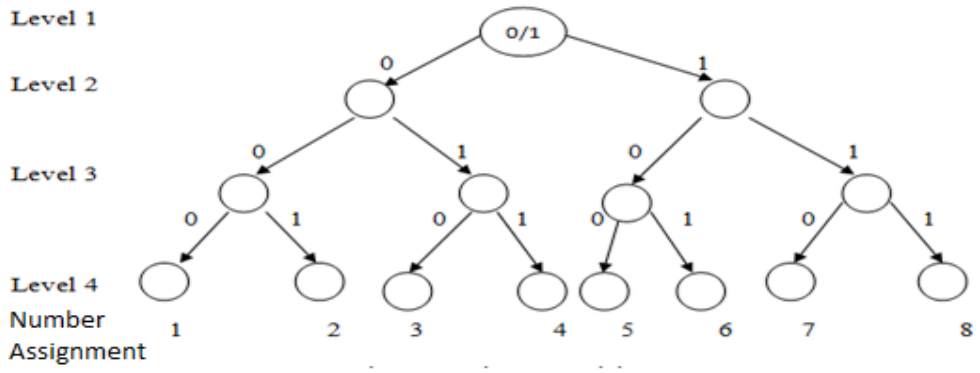


Figure 4: Binary Decision Tree

K. Matching Process

In this process, secret cipher and pseudo random sequences are input to the decision tree for selection of pixel for embedding secret cipher data.

- Grey cover image will be divided into blocks, and each block has eight pixels.

  $For\ i = 1\ to\ (secret\ data\ size * 2)$
- Now select one block at a time using the pseudo-random sequence $(L3(i)(mod2))$.
- Select the four bits B using random number $L5(i)$ in ascending order.
- Encrypt the selected cipher bits as:

  $$B' = B(\oplus)NL(i) \quad (12)$$
- Encrypted four bits are matched in decision tree at fourth level using breadth first search.
- One assigned number out of eight in decision tree is matched at fourth level by following exactly same bits sequence as encrypted secret cipher bit sequence.
- This process continues till all the secret cipher bits are not finished.

End

Example of matching process and identification of pixel has shown in Table 1.

Table 1: Example for Matching Process

Binary sequence (Starts with 0)	0000	0001	0010	0011	0100	0101	0110	0111
Integer Value	0	1	2	3	4	5	6	7
Number Assignment	1	2	3	4	5	6	7	8
Binary sequence (Starts with 1)	1000	1001	1010	1011	1100	1101	1110	1111
Integer Value	8	9	10	11	12	13	14	15
Number Assignment	1	2	3	4	5	6	7	8

Here, we are taking the same input bit sequence, but we are getting different number assignment value, which may select different pixels for data embedding as discussed below:

i)

- If suppose first four secret cipher bits are taken 0100, and generated pseudorandom sequence is 1010.
- So, encrypted bits are 1110.
- The matched node at level 4 in decision tree using breadth first search is 1110 and its integer value is 14 and number assignment value is 7.
- So in cover image $((14 \ mod \ 8) + 1)$i.e7thpixel is used for data embedding.

ii)

- If suppose next four secret cipher bits are also 0100, and generated pseudorandom sequence is 1110
- So encrypted bits are 1010.
- The matched node at level 4 in decision tree using breadth first search is 1010 and its integer value is 10 and number assignment value is 3.
- So in cover image $((10 \ mod \ 8) + 1)$i.e 3rdpixel is used for data embedding.

L. Cover Image Embedding:

Secret cipher insertion at various LSB positions in cover image is done as follows:

- Encrypt seed values along with data size using public key of receiver as $F = E((Seed + Secret\ Data\ Size), Public\ key\ of\ Receiver)$, and embedded in cover image reserved location.
- Pixels are selected for embedding using dynamic decision tree as discussed in previous section.
- Now embed the secret data into LSB positions (5th to 8th) of selected pixel from previous step.

Continue this process until all the cipher data block is not empty and all secret cipher text is not embedded in grey channel medical cover image and send resultant stego image to the receiver.

M. Extraction Process

Extraction of the secret medical data can be obtained as exact reverse of the encryption and embedding as discussed in above sections.

SECURITY ANALYSIS

Security of the proposed system is discussed as follows:

- Starting Seed values are encrypted using, public key of the receiver (RSA), which increase the complexity.
- As, we know slight change in seed values will generate the complete different pseudo random sequences (using chaos).
- Seed values, for the LFSR is depending upon the pseudo random sequence generated by the chaos.
- Hence, slight change in starting seed value will generate different pseudo random sequences of the LFSR.
- Seed values, for the NLFFSR is depending upon the pseudo random sequence generated by the chaos.
- Hence, slight change in starting seed value will generate different pseudo random sequences of the NLFFSR.
- Permutation is depending upon the pseudo random sequences.

- The complexity of the chaos is very high, and it is next to impossible to break, with existing systems.
- Decision tree will be depending upon the pseudorandom sequence generated using NLFFSR.

PERFORMANCE ANALYSIS

The simulation and experimentation have been done using MATLAB. Resultant simulated outcome for different medical cover images and their stego images are being displayed in Figure 6. Histograms also show the negligible amount of difference between histogram of original cover image and stego image. Histograms for various cover images and their stego images are also shown in Figure 6.

The patient information used in this work is listed in Table 2.

Table 2: Patient medical record

Input Data to the Medical Scanned Cover Image	Output using Proposed Methodology
Patient Name: XXX Patient ID/UID: XX Doctors Remarks: X	Patient Name: XXX Patient ID/UID: XX Doctors Remarks:X

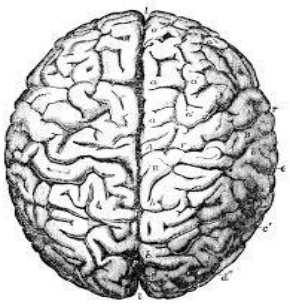
The clause PSNR (Peak Signal to Noise Ratio) is a technical terminology that defines the ratio between the maximum power of a signal and the power of damaged noise. An important index to readjust the quality of reformation of steganography images is peak signal to noise ratio. The original cover image acts like a signal, and the noise is the defect included by some steganography mechanism. The PSNR, MSE (Mean Square Error) and maximum embedding volume values at divergent payloads for different cover images of various sizes is given in Table 3. PSNR is calculated in decibels (dB). A high quality stego image should aspire for 40 dB and above [15].

PSNR outcome is defined by the mean square error (MSE) for two $P * Q$ $m$onochrome images, where x as well as y are image coordinates, SG_{xy} (stego image) and CV_{xy} (cover image), one of the images is approved a noisy surmise of the other is defined as:

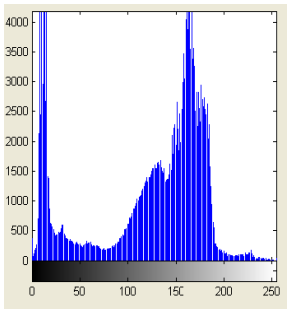
$$MSE = \frac{1}{PQ}\sum_{x=1}^{P}\sum_{y=1}^{Q}(SG_{xy} - CV_{xy}) \quad (12)$$

$$PSNR = 10\ \log_{10}\left(\frac{CV_{max}^2}{MSE}\right) \quad (13)$$

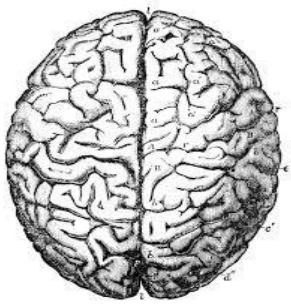
Where CV_{max}= the maximum 255 pixel value, for 8-bit cover images [15].



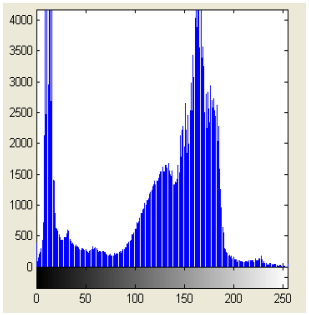
(a) Cover Image of Brain



(b) Histogram of Cover Image

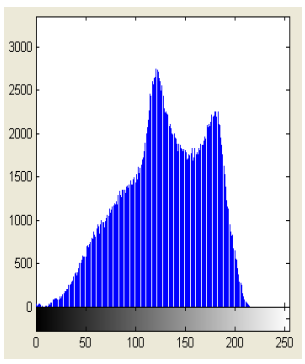


(c) Stego Image of Brain



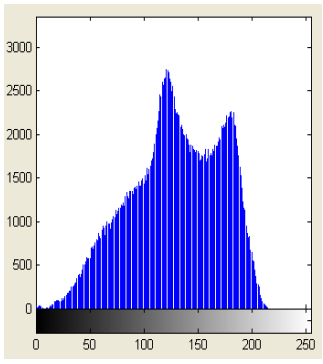
(d) Histogram of Stego Image

(e) Cover Image of Kidney

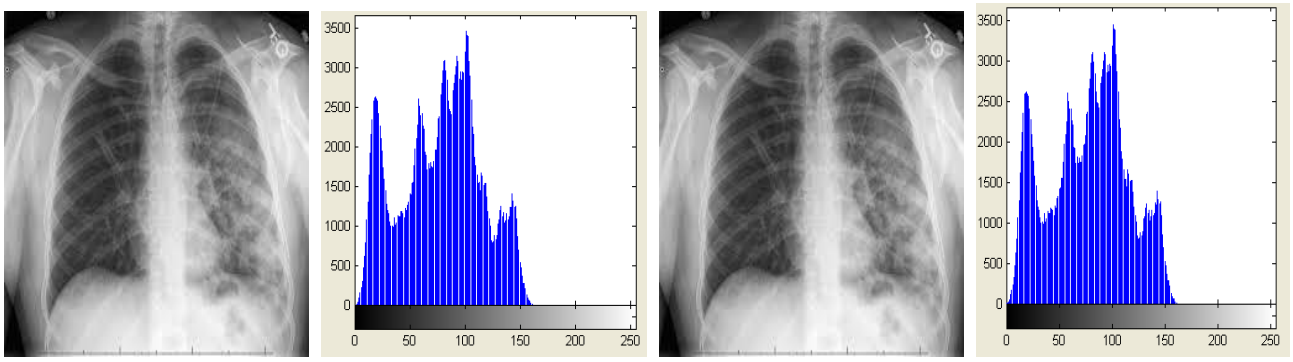


(f) Histogram of Cover Image

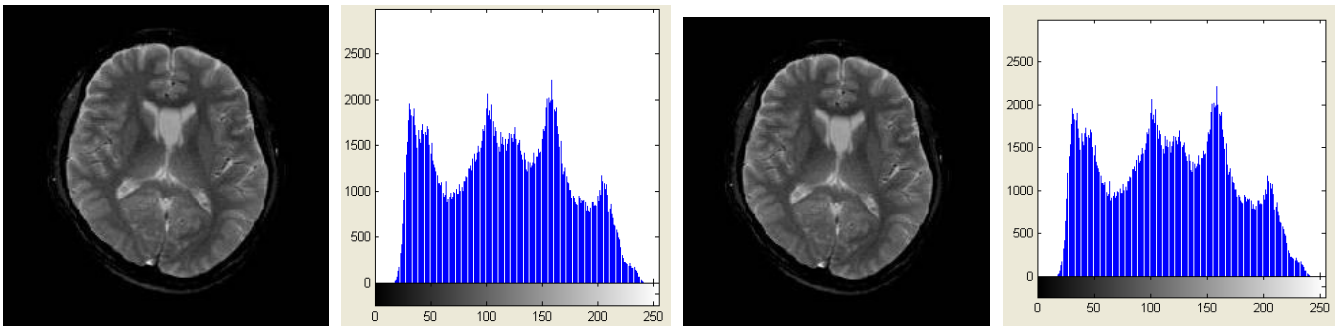
(g) Stego Image of Kidney



(h) Histogram of Stego Image



(i) Cover Image of Lungs (j) Histogram of Cover Image (k) Stego Image of Lungs (l) Histogram of Stego Image



(m) Cover Image of Uterus (n) Histogram of Cover Image (o) Stego Image of Uterus (p) Histogram of Stego Image

Figure 4: (a), (e), (i), (m) are original medical cover images and (c), (g), (k), (o) are their stego images respectively, (b), (f), (j), (n) are histograms of original medical cover images and (d), (h), (l), (p) are their stego images histograms respectively

Table 2: Observed Capacity, MSE and PSNR value (different medical cover images of same/different size with various medical secret cipher data of same /different size)

Medical Cover Image (*.bmp)	Medical Cover Image size (in kilobytes)	Quantity of cipher embedded (in bytes)	Maximum Embedding Volume (Kilo Bytes)	Percentage of Embedding Volume(%) w.r.t (Image Size)	MSE	PSNR (in dB)
Brain	262	256	107.59	40	0.0031	78.05
Brain	262	1024	107.59	40	0.0061	73.55
Kidney	262	256	104.95	39	0.0031	76.85
Kidney	262	1024	104.95	39	0.0066	73.95
Lungs	262	256	102.57	39	0.0054	76.23
Lungs	262	1024	102.57	38	0.0042	74.25
Uterus	262	256	104.01	39	0.0028	78.65
Uterus	262	1024	104.01	39	0.0049	74.8
Brain	1048	256	405.37	42	0.0004	86.55
Brain	1048	1024	405.37	42	0.0013	81.55
Kidney	1048	256	401.65	43	0.0005	85.37
Kidney	1048	1024	401.65	43	0.0019	80.4
Lungs	1048	256	396.38	42	0.0005	85.97
Lungs	1048	1024	396.38	42	0.0013	81.86
Uterus	1048	256	398.47	42	0.0004	86.23
Uterus	1048	1024	398.47	42	0.0019	80.87

Using Table 2resultsare analyzed. If medical cover images such as Brain, Kidney, Lungs and Uterus of size 262 kilo bytes and secret data size is 256 bytes, then PSNR and MSE values will be in range from 76.23 to 78.65 dB and 0.0054 to 0.0028 respectively and if data size increases to 1024 bytes then PSNR and MSE values will be in range from 73.55 to 74.8 dB and 0.0061 to 0.0049 respectively. If medical cover images size increases to 1048 kilo bytes and secret data size is 256 bytes then PSNR and MSE values will be in range from 85.37 to 86.55 dB and 0.0005 to 0.0004 respectively and if secret data size increases to 1024 bytes then PSNR and MSE values will be 80.4 to 81.86 and 0.0019 to 0.0013 respectively.

a) In Brain cover image, maximum embedding capacity is 107.59and 405.37 kilo bytes which are 40% and 42% respectively of the image size.

b) In Kidney cover image, it is 104.95 and 401.65 kilo bytes, which is 39% and 43% respectively of the image size.

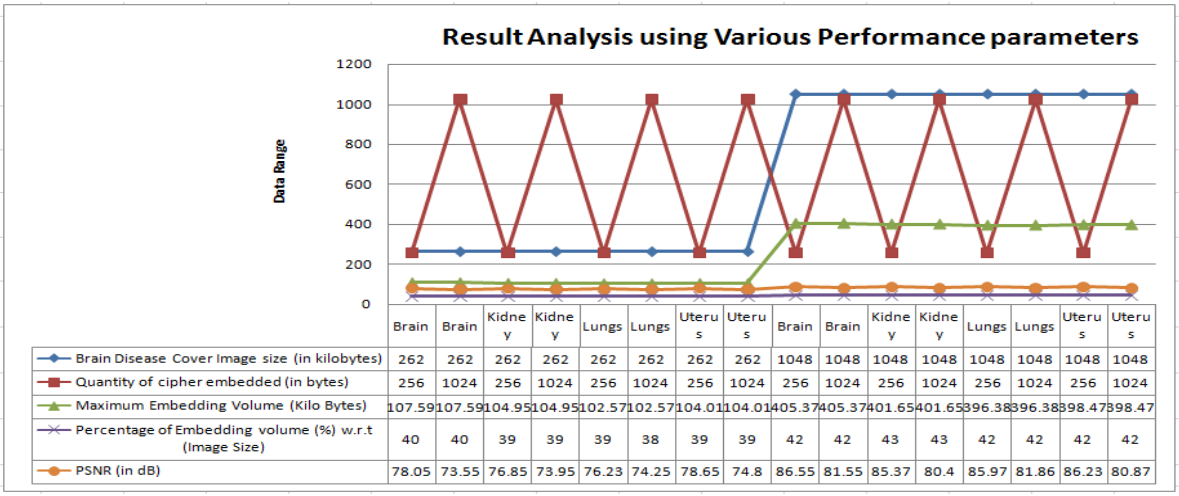
c) In Lungs cover image, it is 102.57 and 396.38 kilo bytes, which is 38% and 42% respectively of the image size.

d) In Uterus cover image, it is 104.01 and 398.47 kilo bytes, which is 39% and 42% respectively of the image size.

So by result analysis, it can be noticed that by increasing the cover image size and decreasing the secret data size PSNR value will be increased up to 86.55 dB and MSE value will be decreased up to 0.0005 as well as maximum embedding capacity is increased up to 43%. So that performance will be high with respect to PSNR, MSE and maximum embedding capacity values. Figure 7 shows the result analysis of proposed algorithm using various performance parameters.

Using Figure 6, one can observe that there is no visual artifacts with the medical stego images and histograms, it is looking exactly same as corresponding original medical cover images.

Using Table 3, the comparison of the proposed scheme is showing on the basis of minimum calculated PSNR, embedding capacity and visual imperceptibility with the different schemes proposed by other researchers in this field. Compared to other algorithms, shows stronger one and can be used for securing different variety of secret medical data.



	Brain	Brain	Kidney	Kidney	Lungs	Lungs	Uterus	Uterus	Brain	Brain	Kidney	Kidney	Lungs	Lungs	Uterus	Uterus
Brain Disease Cover Image size (in kilobytes)	262	262	262	262	262	262	262	262	1048	1048	1048	1048	1048	1048	1048	1048
Quantity of cipher embedded (in bytes)	256	1024	256	1024	256	1024	256	1024	256	1024	256	1024	256	1024	256	1024
Maximum Embedding Volume (Kilo Bytes)	107.59	107.59	104.95	104.95	102.57	102.57	104.01	104.01	405.37	405.37	401.65	401.65	396.38	396.38	398.47	398.47
Percentage of Embedding volume (%) w.r.t (Image Size)	40	40	39	39	39	38	39	39	42	42	43	43	42	42	42	42
PSNR (in dB)	78.05	73.55	76.85	73.95	76.23	74.25	78.65	74.8	86.55	81.55	85.37	80.4	85.97	81.86	86.23	80.87

Figure 7: Result analysis of proposed algorithm using various performance parameters

Table 3: Comparison with other research work

Research Article	Minimum Calculated PSNR(dB)	Capacity	Visual Imperceptibility
Jain *et al.*[15]	70.24	Good	Better
Thiyagarajan *et al.*[13]	65.53	Medium	Good
Swain *et al.*[12]	50.50	Medium	Good
Wang *et al.*[7]	44.20	Medium	Good
Kumar *et al.*[8]	44.15	Medium	Good
Wu *et al.*[4]	37.90	Low	Average
Zhang *et al.*[5]	36.00	Low	Average
Nag et. al [11]	30.48	Very Low	Not Good
Proposed Algorithm	74.21	Very Good	Best

CONCLUSION

In this article, an improved secretmedical data transmission scheme is proposed with the help ofdynamicdecision tree using pseudo random sequences. The secret message blocks are allocated randomly using pseudo random sequencesby the sender to the grey medical cover image with respect to dynamic decision tree, which increases security levels and gives randomness to proposed algorithm.The proposed algorithmused hybrid cryptosystem (diffusion, confusion, RSA) to provide encryption of secret patient medical data in remote places communication.At steganography level least significant bits substitutions using chaos theory and pixel selection using dynamicdecision tree are usedto protect data. From, security analysis, it is found that complexity of the encryption is very high to break, from existing system.Proposed algorithm hides only secret medical data,

embedding of metadata in grey cover image is not required, so that lot of space are available in the cover image. No clue will be available to the intruders by pseudo random numbers using piecewise linear chaotic map, LSFR, and NLFFSR. By using this algorithm, selection of pixel using decision tree is dynamic, hence most of the pixels selected will not be same.As we are hiding less data comparatively to existing techniques hence,from result analysis, it is concluded that PSNR, MSE values and percentage of maximum embedding capacity are better as compared to others. By histogram analysis it is concluded that, imperceptibility distortion cannot be measured from the corresponding stego images.

REFERENCES

[1] United, S., "Summary of the HIPAA Privacy Rule," United States Department of Health and Human Services, pp.1-19, 2000.

[2] Wu, D. C., and Tsai, W. H., "A steganograhic method for images by pixel value differencing." Pattern Recognition Letters, vol.24, no.9-10, pp.1613-1626, 2003.

[3] Zhang, X., and Wang, S., "Vulnerability of Pixel-Value Differencing Steganography to Histogram Analysis and Modification for Enhanced Security." Pattern Recognition Letters, vol. 25, no.12, pp. 331–339, 2004.

[4] Rajpal, N., and Kumar, A., "Steganography using Non-Linear Forward Feedback Shift Register Technique." IWAIT'2004 in National University of Singapore, Singapore, pp. 117-122,2004.

[5] Wang, R., and Chen, Y., "High Payload Image Steganography Using Two-Way Block Matching." IEEE Signal Processing Letters, vol. 13, no. 3, pp. 161–164, 2006.

[6] Kumar, P.M., and Roopa, D., "An Image Steganography Framework with Improved Tamper Proofing." Asian Journal of Information Technology, vol. 6, no.10, pp.1023–1029, 2007.

[7] Kumar, A, and Ghose, M. K., "Overview of Information Security Using Genetic Algorithm and Chaos." Information Security Journal: A Global Perspective, vol. 18, no.6, 306-315, 2009.

[8] Nag, A., Singh, J. P., Khan, S., and Ghosh, S., "A Weighted Location Based LSB Image Steganography Technique." Springer ACC 2011, CCIS (ISBN: 978-3-642-22714-1), vol. 2, no. 191, pp. 620–627, 2011.

[9] Kumar, A., and Ghose, M. K., "Extended substitution-diffusion based image cipher using chaotic standard map." Communications in Nonlinear Science and Numerical Simulation, vol. 16, pp. 372-382, 2011.

[10] Gandharba, S., and Lenka, S.K., "LSB Array Based Image Steganography Technique by Exploring the Four Least Significant Bits." Springer, *Proceedings of 4th International Conference, Obcom 2011*, *CCIS (ISBN:* 978-3-642-29216-3), vol. 2, no. 270, pp.479-488, 2012.

[11] Thiyagarajan, P., and Aghila, G., "Reversible dynamic secure steganography for medical image using graph coloring." Health Policy and Technology, vol. 2, no. 3, pp. 151–161, 2013.

[12] Jain, M., and Lenka, S. K., "Diagonal queue medical image steganography with Rabin cryptosystem." Brain Informatics, vol. 3,no. 1, pp. 39–51, 2016.

[13] Jain, M., and Kumar, A.,"RGB channel based decision tree grey-alpha medical image steganography with RSA cryptosystem."International Journal of Machine Learning and Cybernetics, in press,DOI: 10.1007/s13042-016-0542-y, 2016.