

Research Journal of Pharmaceutical, Biological and Chemical Sciences

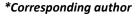
An efficient Image scrambling technique for Medical Images using Circular Filling and LSB substitution.

Anusuya N¹, Renuga Devi G¹, Saraswathi Divya M¹, Rajesh Kumar N¹*, Bala Krishnan R¹, and Raajan NR².

¹Department of CSE, Srinivasa Ramanujan Centre, SASTRA University, Kumbakonam, India – 612 001.
 ² Senior Assistant Professor, School of Electrical & Electronics Engineering, SASTRA University, Thanjavur, India – 613 401.

ABSTRACT

Information Security is an important issue in the present multimedia communication. Especially, image protection is most challenging task in the field of Internet communications, media identification, tracking, health care and biomedical applications. Image scrambling is a prominent technique to shuffle all the pixels in the original image into different index positions to change the order of the pictorial arrangement. The appearance of resultant image is fully non-recognizable format to the outside viewers. This is a preliminary and final process of security related applications such as information hiding, cryptography and network security. In this paper, an efficient image scrambling technique has been proposed for medical images. A Secret image has transformed into two dimensional matrix formats and generate key file by arranging the pixel intensities sequentially. The circular fill technique is used to compute the new structure of matrix and perform the binary transformation of all index positions. Finally, we implement the LSB substitution technique to obtain the scrambled image. We have also proposed some quality metrics to measure the quality of restored image. Our experimental results emphasize the high level protection of medical images and restored with high visual quality. **Keywords:** Medical images, Image scrambling, binary transformation, LSB substitution





INTRODUCTION

Secrecy of digital information and expressway communication plays a vital role in the present generation of internet technology. Medical imaging [2-10] is an excellent platform to analyze the human body to perform many useful clinical applications. X-ray based medical content, molecular imaging, magnetic resonance imaging (MRI) and ultrasonic images are used in wide variety of clinical applications to visualize the medical report. These medical reports are highly confidential while transferring and retrieving the internet. In clinical applications image protection is needed to maintain the secrecy of medical information. Generally cryptography is a technique to convert the secret information into unreadable format. Especially, Image scrambling is a prominent technique to shuffle all the pixels in the original image into different index positions to change the order of the pictorial arrangement. The scrambling technique is more suitable for image pattern applications on information security. It is mostly used in the field of information hiding and digital watermarking [1-3]. Partial image scrambling, multi level block scrambling, space bit plane image scrambling, rotation based scrambling, color image scrambling are more potential techniques under scrambling. Many scrambling algorithms are designed to protect the digital images in the past few years. The implementation process is differing based on type of application. All the existing scheme used single way encryption process to scramble the digital image. In this paper we proposed, an efficient Image scrambling technique for Medical Images using Circular Filling and LSB substitution [9]. This is double scrambling process in fast manner to protect the medical images without content loss.

RELATED WORK

Panduranga [4] H T et al. proposed a selective image encryption for Medical and Satellite Images. Two methods are used to compute the encryption process. Additionally morphological operations are used to perform the object recognition. A Novel Image encryption algorithm invented by G. A. Sathiskumar [7-8] et al. Chaos based circular mapping technique is applied to scramble the medical images. Med Karim Abdmouleh [5] , Ali Khalfallah and Med Salim Bouhlel proposed a new watermarking technique for medical image using hierarchical encryption. The next level image protection is presented by W. Puech for images, videos and 3D objects. Mixed chaotic approach sequence is designed by Wenqing [6] Chen et al. This is key based approach to scramble the image, but the user may choose the maximum length to improve the security. Recently many researchers involved the development of security systems to defend multimedia content, especially for medical images. Considering any other multimedia content, medical images contain crucial attribute in dimension, quality, entropy information and processing modules. Due to the variation of image attributes, the researchers still lack to provide a better methodology for image encryption. To address the various security related issues of medical information a novel Image scrambling technique based on circular filling and LSB substitution is proposed.

PROPOSED SYSTEM

IMAGE ANALYSIS

In our proposed method, we have analyzed the input image to identify which type of medical images is acquired for image scrambling. In this preliminary procedure, it is clearly noted whether it is binary image, gray scale image and color image. In this preliminary stage, the input image is converted into matrix format. All the pixel intensities of gray image are arranged properly into matrix index position. All index positions are started from the values [1, 1] to $[M \times N]$, where $M \times N =$ Width × Height. System architecture is shown in Figure 1.

CIRCULAR FILL

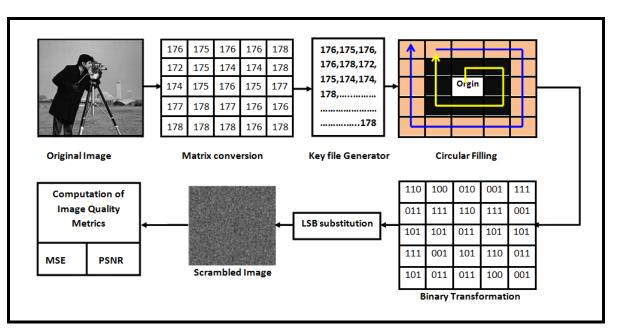
After preprocessing, the pixel intensities of original Image are extracted sequentially from the matrix index position and arranged properly to generate a key file. The key file contains all the secret information about the medical images. The informations are filled circularly to complete the circular filling process. It is started from the center of the newly created matrix and filled by various computation levels. It is shown in the Table 1.

July - August 2016 RJPBCS 7(4) Page No. 2769

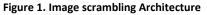


Table 1. Circular Level Computation

S. No	Dimension of the Image	Circular Level Computation
1.	64 × 64	32
2.	128 × 128	64
3	256 × 256	128
4	512 × 512	256



PROPOSED SYSTEM ARCHITECTURE



BINARY TRANSFORMATION AND LSB SUBSTITUTION

In this section, the circularly filled matrix is transformed into binary format in each level. Now, the pixel intensity ranges [0-255] are expanded into binary data format. After the completion of binary transformation, least significant bit (LSB) of the every binary formatted cell is replaced by the value either zero or one based on the LSB value. If the LSB value is zero replace with the value one and vice versa. Finally the medical image is scrambled by our proposed double layer encryption scheme.

Image Reconstruction

An efficient image scrambling has performed based on the binary transformation and popular LSB substitution. The secret image is effectively ready to send the receiver through the transmission medium. The image has encrypted twice however, it is ensured the size of the image and speed of transmission is much better than the previously implemented methodology. To reveal the secret image, a reverse LSB substitution has performed on the scrambled image. Now reverse the binary transformation process to regenerate the key file and original matrix. Finally, the reversed process reconstructs the original image without content loss. In explaining, the correct working principle of the proposed scrambling scheme, we have developed a windows application (.exe) file. The detailed algorithmic procedure is explained in the following section.

ALGORITHM DESCRIPTION

Step 1: Upload an input 2-D grayscale image I and convert into Matrix Transformation.
Step 2: Determine the dimension of input image matrix M × N and compute the circular level.
Step 3: Convert the 2-D image array into 1-D image array and generate a key file.

July - August 2016 RJPBCS 7(4) Page No. 2770



Step 4: Considering the circular level computation, extract the pixel intensity values form the key file and start the circular fill operation to generate a scrambled matrix S with same size of M × N.

Step 5: Convert all the values of scrambled matrix into binary format and adjust the pixel positions based on the LSB substitution.

Step 6: The LSB substitution of binary scrambled image is described as

$$S_{b} = \begin{cases} 1 & \text{when LSB } [S_{(x,y)}] = 0; \\ 0 & \text{otherwise} \end{cases}$$

Step 7: After the successful completion of LSB, the original image is completely scrambled in an unintelligible format for secured image transmission.

Step 8: Unscramble the encrypted image using the reverse of the previous operations and revert into 2-D image matrix to show the original Image.

Step 9: Illustrate the histogram between original image and encrypted image.

Step 10: Finally, Visual quality and scrambling efficiency is carried out by computing the MSE and PSNR value of the secret medical image, scrambled image and unscrambled image.

EXPERIMENTAL RESULTS AND DISCUSSION

The following figures show that the implementation of our proposed image scrambling system.

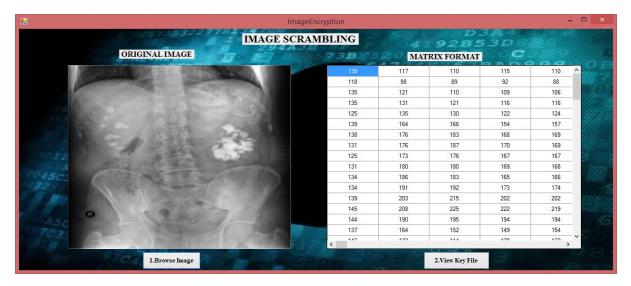


Figure 2. Image upload and Transformation

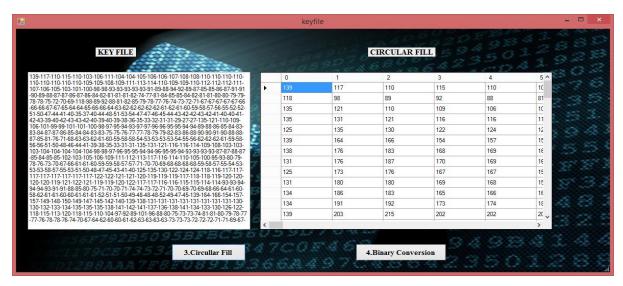


Figure 3. Construct Key file and Circular Fill

July – August

2016



ISSN: 0975-8585

				bina	aryconver				- 🗆 ×	
	BIN	2500 g			LSB SUBST	ane				
	0	1	2	3 '		0	1	2	3 ^	
• •	10001011	1110101	1101110	1110011	20	10001000	1110110	1101101	1110000	
V	1110110	1100010	1011001	1011100		1110101	1100001	1011010	1011111	
8	10000111	1111001	1101110	1101101		10000100	1111010	1101101	1101110	
1	10000111	10000011	1111001	1110100	8	10000100	1000000	1111010	1110111	
	1111101	10000111	10000010	1111010		1111110	10000100	10000001	1111001	
	10001011	10100100	10100110	10011010	Contraction of the local division of the loc	10001000	10100111	10100101	10011001	
22	10001010	10110000	10110111	10101000	1	10001001	10110011	10110100	10101011	
20	10000011	10110000	10111011	10101010	IE.	1000000	10110011	10111000	10101001	
5	1111101	10101101	10110000	10100111	10	1111110	10101110	10110011	10100100	
	10000011	10110100	10110100	10101001	11	1000000	10110111	10110111	10101010	
	10000110	10111010	10110111	10100101	n .	10000101	10111001	10110100	10100110	
5.2	10000110	10111111	11000000	10101101		10000101	10111100	11000011	10101110	
	10001011	11001011	11010111	11001010	See.	10001000	11001000	11010100	11001001	
	10010001	11010000	11100001	11011110	1	10010010	11010011	11100010	11011101 ~	
<	_			>					>	
		5.LSB	Substitution							
		1				6.Show Encrypted Image				

Figure 4. Double Layer Encryption Process

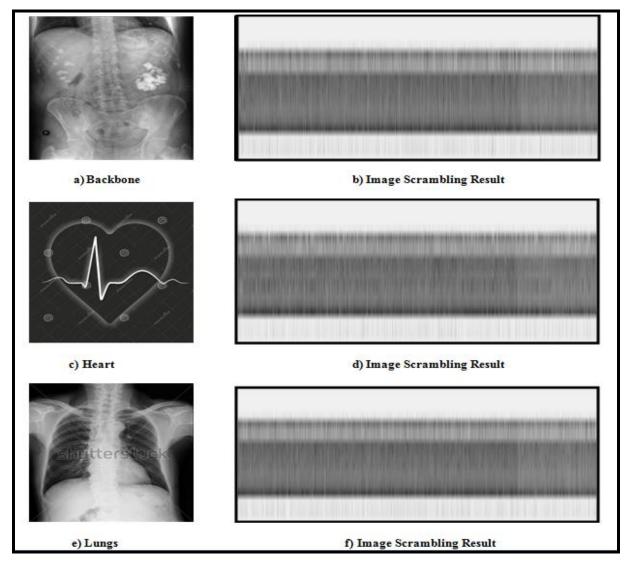


Figure 5. Results of various input images



		-	ANTER 227	7BUSICE	Contraction of the	No. of Lot of Lo	MARCH STORE	TOWNS TO DO TO DO TO	
		D	ECYPTION PR	OCESS	94A38	NE SE		DECRY	YPTION IMAGE
09-108-1 38-94-92- 79-79-78- 5-66-66- 16-45-44- 10-109-1 4-84-83-8	09-111-113-114- 89-87-85-85-86-8 78-75-72-70-3-11 64-63-62-62-62-6 43-42-42-43-42-4 06-101-99-99-10 33-75-75-76-77-7 53-54-55-56-62-6	110-109-109-110 37-91-91-90-89-8 8-98-89-92-88-8 52-62-61-62-61-6 1-40-40-41-42-4 1-101-100-98-97 7-78-79-79-82-8 52-62-61-59-58-5	D-112-112-112-111-10 8-87-87-86-87-86-84 1-82-85-79-78-77-76- 0-59-58-57-56-55-52- 3-39-40-42-43-43-42- 95-94-93-97-97-96-99 95-94-93-97-97-96-99 6-56-51-50-48-46-44-	7-106-105-103-101-1 32-81-81-82-74-77 32-72-71-67-67-67 52-51-50-47-44-41-40 40-39-40-39-38-36-35 5-95-95-94-94-89-88 8-88-87-85-81-76-71 41-39-38-35-33-31-3-	110-110-110-110-110- 100-98-98-93-93-93-93-97 781-84-85-85-84-82-87 787-67-66-66-66-67-67-66 755-37-40-44-48-51-55 733-32-31-31-29-27-3 86-85-84-83-83-84-87 68-65-63-63-62-61-60-55 135-131-121-116-116 10-20-27-20-00-75 00-20-77-00-75 00-20-77-00-00-75 00-20-77-00-00-75 00-20-77-00-00-75 00-20-77-00-00-75 00-20-77-00-00-75 00-20-77-00-75 00-20-77-00-75 00-20-77-00-75 00-20-77-00-75 00-20-77-00-75 00-20-77-00-75 00-20-77-00-75 00-20-77-00-75 00-20-77-00-75 00-20-77-00-75 00-20-77-00-75 00-20-77-00-75 00-20-77-00-75 00-20-77-00-75 00-20-77-00-75 00-20-77-00-75 00-75	3-93-91-89 31-81-80-80 37-65-64-64 3-54-47-47 3-135-121- 7-87-86-85- 9-58-58-54 3-114-109-	477 89 38 15 17		
02-103-1 7-71-70-7	70-69-68-68-68-68-68-68-68-68-68-68-68-68-68-	112-113-117-110 8-59-58-57-55-54 -117-117-117-11	5-114-110-105-100-95 4-53-53-53-58-57-55-5 7-122-122-121-121-12	-93-80-79-78-76-73-7 3-51-50-48-47-45-43- 20-119-119-119-117-	13-33-87-87-87-88-87-83- 70-67-66-61-61-60-59- -41-2-125-135-130-12 118-118-119-120-120 4-93-91-91-88-85-80-7	-59-58-57- 22-124-124 0-120-120- 75-71-70-	A 14	-A	
02-103-1 7-71-70-7 118-116- 19-121-1	05-106-109-111- 70-69-68-68-68-68 117-117-117-117-	112-113-117-110 8-59-58-57-55-54 -117-117-117-11	5-114-110-105-100-95 4-53-53-53-58-57-55-5 7-122-122-121-121-12	-93-80-79-78-76-73-7 3-51-50-48-47-45-43- 20-119-119-119-117-	70-67-66-61-61-60-59- -41-2-125-135-130-12 118-118-119-120-120	-59-58-57- 22-124-124 0-120-120-	A5 3		
02-103-1 7-71-70-3 118-116- 19-121-1	05-106-109-111- 70-69-68-68-68-68-61 17-117-117-117- 22-121-119-119-	112-113-117-11(8-59-58-57-55-5- -117-117-117-11 120-122-117-11	S-114-110-105-100-95 4-53-53-53-58-57-55-5 7-122-122-121-121-12 7-116-116-115-115-11	-93-80-79-78-76-73-7 3-51-50-48-47-45-43- 20-119-119-119-117- 4-114-93-93-94-94-9	70-67-66-61-61-60-59- -41-2-125-135-130-12 118-118-119-120-120 4-93-91-91-88-85-80-7	-59-58-57- 22-124-124 9-120-120- 75-71-70-	A5.7		
02-103-1 7-71-70-7 118-116- 19-121-1	05-106-109-111- 70-69-68-68-68-68 117-117-117-117- 22-121-119-119- 0	112-113-117-11(8-59-58-57-55-54 -117-117-117-11 120-122-117-117 1	2 -114-110-105-100-95 4-53-53-53-53-58-57-55-5 7-122-122-121-121-1 7-116-116-115-115-11 2	-93-80-79-78-76-73-7 3-51-50-48-47-45-43 20-119-119-119-119-117- 4-114-93-93-94-94-9- 3	20-67-66-61-61-60-59- 41-2-125-135-130-12 118-118-119-120-120 4-93-91-91-88-85-80-7	-59-58-57- 22-124-124 9-120-120- 75-71-70-	A53 414		
02-103-1 7-71-70-7 118-116- 19-121-1	05-106-109-111- 70-69-68-68-68-68 117-117-117-117- 22-121-119-119- 0 39	112-113-117-11(8-59-58-57-55-54 -117-117-117-11 120-122-117-11 120-122-117-11 120-122-117-11	2 114-110-105-100-95 4-53-53-53-58-57-55-5 7-122-122-121-121-12 7-116-116-115-115-11 2 110	-93.80.79.78.76.73.7 3.51.50.48.47.45.43 20-119-119-119-117- 4.114-93-93-94.94.9 3 115	70-67-66-61-61-60-59- 41-2-125-135-130-12 118-118-119-120-120 4-93-91-91-88-85-80-7 4 110	-59-58-57- 22-124-124 9-120-120- 75-71-70-	A53 414		
02-103-1 7-71-70- 118-116- 19-121-1 19-121-1 1 1 1 1 1	05-106-109-111- 70-69-68-68-68-68 117-117-117-117- 22-121-119-119- 0 39 18	112-113-117-11(8-59-58-57-55-55 -117-117-117-11 120-122-117-11 1 1 1 1 98	2 114-110-105-100-95 453-53-53-58-57-55-5 7-122-122-121-121-1 7-116-116-115-115-11 2 110 89	93-80-79-78-76-73-7 3-51-50-48-47-45-43 20-119-119-1117- 4-114-93-93-94-94-9 3 115 92	20-67-66-61-61-60-59- 41-2-125-135-130-12 4-93-91-91-88-85-80-7 4 4 110 88	-59-58-57- 22-124-124 9-120-120- 75-71-70-	70 4 A53 414		
02-103-1 7-71-70-7 118-116- 19-121-1 19-121-1 1 1 1 1 1 1 1	05-106-109-111- 10-69-68-68-68-68- 117-117-117-117- 22-121-119-119- 10- 39- 18- 35-	112-113-117-11(8-59-58-57-55-5- -117-117-117-11 120-122-117-117-11 1 117 98 121	5-14-110-105-100-92 453-53-53-58-57-55- 7-122-122-121-121-12 7-116-116-115-115-11 2 110 89 110	93-80-79-78-76-73-7 3-51-50-48-47-45-43 20-119-119-117- 4-114-93-93-94-94-9 3 115 92 109	70-67-66-61-61-60-59 -41-2-125-135-130-12 118-118-119-120-120 4-93-91-91-88-85-80-7 4 110 88 106	-59-58-57- 22-124-124 9-120-120- 75-71-70-	A53 414 4 9		
02-103-1 7-71-70-7 118-116- 19-121-1 19-121-1 1 1 1 1 1 1 1 1 1 1 1 1	05-106-109-111- 0-69-68-68-68-68- 17-117-117-117-117- 22-121-119-119- 0 39 18 35 35 35	112-113-117-11(8-95-86-75-55-65 117-117-117-111 120-122-117-11 117 98 121 121 131	5-14-110-105-100-92 453-53-53-58-57-55- 7-122-122-121-121-12 7-116-116-115-115-11 2 110 89 110 121	-93-80-79-78-76-73- 3-51-50-48-47-45-43 0-119-119-119-119-119-117- 4-114-93-93-94-94-9 3 115 92 109 116	70.67.66.61.61.60.59 41.2.125-135-130-12 118-118-119-120-120 4-93-91-91-88-85-80-7 4 110 88 106 116	-59-58-57- 22-124-124 9-120-120- 75-71-70-	A53 414 4 9 F7	0 11.Show	12.Quality

Figure 6. Decryption Process

In this section we present our experimental results of the proposed scrambling system. It is implemented in Visual studio 2012 C# DOTNET platform on a personnel computer with 3.40 GHz Intel Core i3 processor, 2 GB internal memory and 160 GB Hard disk capacity. A grayscale medical image size of 256 × 256 is considered as a secret image and applied our proposed image scrambling methodology to construct a fully scrambled image. Correlation coefficients are calculated to show the similarity between original image and encrypted image. It is computed in horizontal, vertical and diagonal directions and shown in Table 2. Mean Squared error and Peak Signal Noise ratio also calculated between the original image and encrypted image. These statistical and quality metrics show the performance of the proposed scheme. Histogram analysis also presented in Figure 7 (a), (b), (c) and (d). The histogram is represented for the original medical image and its corresponding scrambled image.

Image quality metrics and Correlation coefficient of adjacent pixel on the medical segments is calculated by using the formula:

$$MSE = \frac{1}{MN} \sum_{j=1}^{M} \sum_{k=1}^{N} (x_{j,k} - x'_{j,k})^{2} \cdots (1) \quad PSNR = 10 \log \frac{(2^{n} - 1)^{2}}{MSE} = 10 \log \frac{255^{2}}{MSE} \cdots (2)$$
$$E(x) = \frac{1}{L} \sum_{i=1}^{L} x_{i} \qquad \cdots (3) \qquad D(x) = \frac{1}{L} \sum_{i=1}^{L} (x_{i} - E(x))^{2} \cdots (4)$$

	Medical	Image Size	MSE		Scrambled Image - Correlation			
S. No	Image			PSNR (db)	Horizontal	Vertical	Diagonal	
1	Backbone	230 × 230	4095	12	0.9814	0.9986	0.9800	
2	Heart	230 × 230	15147	6.3	0.9905	0.9976	0.9881	
3	Lungs	230 × 230	7348	9.4	0.9950	0.9976	0.9927	
4	Spinal	230 × 230	8755	8.7	0.9946	0.9976	0.992	

Table 2. Image Quality Metrics

July - August

2016



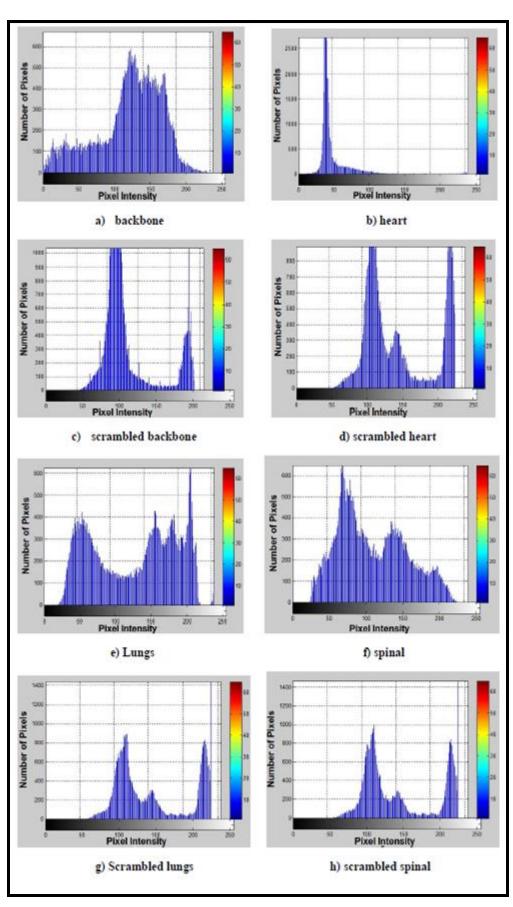


Figure 7. Histogram Representation

July – August



CONCLUSION

In this study, we have proposed an efficient image scrambling technique for medical images using circular filling and LSB substitution has proposed. The proposed scheme is very expressive and highly secure method to protect the digital images. Protection of medical image is a major part of the proposed scrambling system. It provides the best solution for medical images which is not available in the existing scheme. Medical image is fully scrambled that ensures with high level protection of the content. The experimental results shown the proposed scheme is a novel technique and well suitable for medical image and scrambled image. Correlation coefficients and image quality metrics has computed through the standard mathematical equations. Image quality metrics show that the scrambling algorithm works fine and the computation speed and level encryption accuracy is high. Regarding future enhancement, we suggest in this technique to focus on more DICOM images and apply stenographic methodologies to improve the standard of the proposed scheme. We have also planned to extend the proposed image scrambling technique for color images. We will also implement various techniques of image smoothing to remove the noise level on the image.

REFERENCES

- Divya Bharathi J, Deepa C. Research Journal of Pharmaceutical, Biological and Chemical Sciences 2016; 7(3): 399-404.
- [2] Suhashini M, Veeramuthu A. Research Journal of Pharmaceutical, Biological and Chemical Sciences 2016; 7(2): 1471-1479.
- [3] A Stephy Anisha Mary, A Ronald Doni, Research Journal of Pharmaceutical, Biological and Chemical Sciences 2016; 7(3): 777-784.
- [4] Panduranga H T , NaveenKumar S K. International Journal of Engineering and Technology 2013; 5(1): 115-121.
- [5] Med Karim Abdmouleh, Ali Khalfallah and Med Salim Bouhlel. International Journal of Computer Science 2014; 11(4): 27-32.
- [6] W. Puech, IPTA'08: 1st International Workshops on Image Processing Theory, Tools and Applications 2008; 1-2.
- [7] GA Sathishkumar, K Bhoopathybagan, N Sriraam, SP Venkatachalam, R Vignesh. Advanced Computing 2011; 133: 290-299.
- [8] Rajesh Kumar N et. al. Global Journal of pure and applied mathematics 2015; 11(5): 3763-3775.
- [9] Bala Krishnan Raghupathy, N. Rajesh Kumar and N.R. Raajan. International Journal of Applied Engineering Research 2014; 9 (1): 145-15.
- [10] N. Rajesh Kumar and N.R. Raajan. Far East Journal of Electronics and Communications 2016; 1: 79 88.