Indian Journal of Science and Technology, *Vol 8(11), DOI: 10.17485/ijst/2015/v8i11/71763, June 2015*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Image Encryption using Pseudo Random Bit Generator Based on Logistic Maps with Radon Transform

R. Tamilselvi[1*] and G. Ravindran[2]

[1]Department of Electronics, Communication Engineering, Sethu Institute of Technology, Kariapatti - 626106, Tamil Nadu, India; rts.ece@gmail.com
[2]Centre for Medical Electronics, Department of Electronics and Communication Engineering, Anna University, Chennai - 60001, Tamil Nadu, India; raviguru@annauniv.edu

Abstract

Objectives: To develop a new image encryption algorithm using logistics map and Radon transform. It aims at finding an optimum transformation technique that gives better encryption in terms of encryption quality and entropy. **Methods/ Analysis:** A Pseudo Random Bit Generator (PRBG) is used which outputs a sequence of statistically independent and unbiased binary digits. A novel method is developed using PRBG based on logistics maps and radon transform for DICOM image encryption. Encryption is evaluated based on encryption quality and entropy. **Findings:** The maximum encryption occurs when the angle of rotation is 135. Similarly, the results of entropy value indicate that the there is a higher encryption of 80% for 135 degree of rotation. The key added with the transformed image also increases the randomness and provides authentication of images. **Conclusion/Application**: Encryption quality and entropy are analyzed for the algorithm and the results are compared. Experimental results confirm that the encryption quality and entropy obtained from the images can clearly discriminate between the original and encrypted images.

Keywords: DICOM, Logistic Map, PRBG, Radon Transform and Block Transform

1. Introduction

Medical image security is an important issue while transmitting images and patient information across networks. The increasing adoption of information systems in healthcare has led to a scenario where patient information security is more and more being regarded as a critical issue. A degraded image or tampered image is a potential source of difficulty in diagnosis, treatment or research[1]. Many protection techniques are evolved for the safe and secure transmission of data. It is necessary to find the efficient way of transmission of data because transmission errors are not acceptable in the medical world. If an error has occurred, then the patient's life is highly at risk. Encryption techniques are developed to fulfill the security needs of digital images. During the last decade, numerous encryption algorithms have been proposed in the literature based on different principles. Among them, chaos-based encryption techniques are considered good for practical use as these techniques provide a good combination of speed, high security, complexity, reasonable computational overheads and computational power, etc.

Due to high sensitivity of chaos systems to initial conditions and system parameters, it can be used for strong chaotic cryptosystems that make them robust against any statistical attacks. Therefore, chaos system plays a great and significant role in cryptography system in many areas, including a database, Internet transaction, banking, software, online business and protection of communication channels[2]. The logistic map is one of the simplest forms of

*Author for correspondence

a chaotic process. The logistic map is a very simple mathematical model often used to describe the growth of biological populations. Because of its mathematical simplicity, this model continues to be useful test bed for new ideas in chaos theory as well as application of chaos in cryptography[3]. The simple modified mathematical form of the logistic map is given as,

$$X_n+1 = \lambda X_n (1 - X_n) \ldots\ldots\ldots(1)$$

where X_n is a state variable, which lies in the interval (0,1) and λ is called system parameter, which can have any value between 1 and 4. An example for a logistic map for 40 iterations is shown in Figure 1.

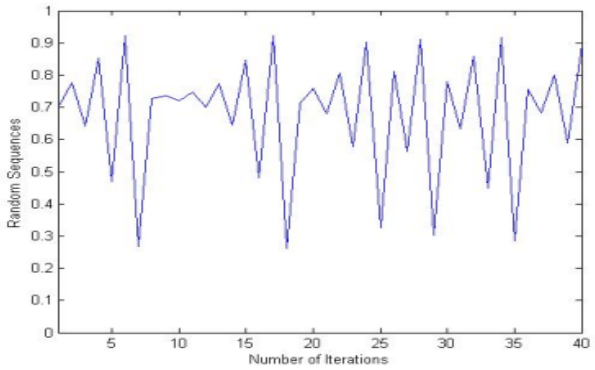

Figure 1. Logistic map sequences.

2. Psuedo Random Bit Generator

2.1 Architecture Model

A PRBG is developed which is based on two logistic maps, starting from random independent initial conditions (X_0, Y_0 ε (0,1) and $X_0 \neq Y_0$).

$$X_n+1 = \lambda_1 X_n (1-X_n) \ldots\ldots\ldots(2)$$

$$Y_n+1 = \lambda_2 Y_n (1-Y_n) \ldots\ldots\ldots(3)$$

The outputs of the logistic maps are compared with their respective median in the decision devices. Because an important observation is made that the median is the most suitable statistical characteristic that may split the domain into two equally filled sub-domains and in this way randomness is achieved. Because of this statement, the criterion for the final output of the logistic map is as follows:

$a_k = 1$, if $X_n > \text{median}_1$

0, if $X_n < \text{median}_1$

$b_k = 1$, if $Y_n > \text{median}_2$

0, if Y_n <median2 Where Median1 denotes the median of the values generated by the logistic map 1. Median2 denotes the median of the values generated by the logistic map 2.a_k and b_k are the outputs from the two decision devices. The final bit sequence is generated by sending the outputs of the decision devices to the logical device which performs logical Exclusive - OR operation between two sequences. The schematic block diagram of the PRBG is shown in Figure 2.

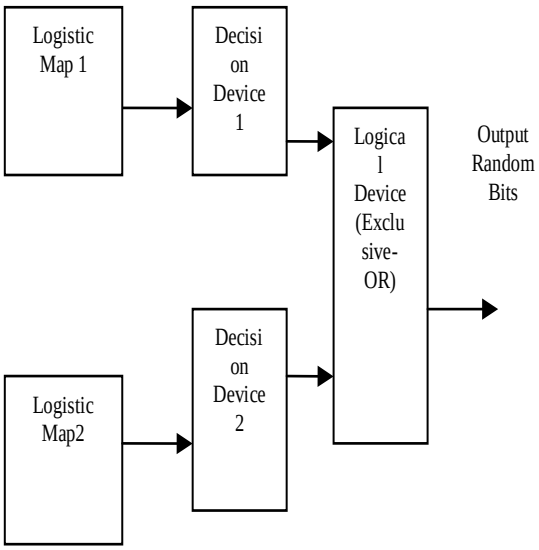

Figure 2. Block diagram of developed methodology.

3. Key

The generated sequences are stored in a table as a random key[9]. The iteration in the logistic map depends on the size of the key to be added. And the sequences are stored in the table (various sizes depending on the iterations). The 128 sequence is considered as a 128 bit key.

4. Dicom Image Security

The DICOM image is taken as an input image and the size of the image is 128 × 128, 256 × 256 etc., in the developed algorithm, the image size is 512 × 512. The image is segmented without any background information. Then the 128 byte zeros which are unused are taken in the format of the DICOM image and the randomly generated key from the PRBG is added where the security of the DICOM image is considered.

5. Radon Transform

A projection of a two-dimensional function f(x,y) is a set of line integrals. The radon function computes the line integrals from multiple sources along parallel paths, or beams, in a certain direction. To represent an image, the radon function takes multiple, parallel-beam projections of the image from different angles by rotating the source around the centre of the image. Applying the radon transform on an image, f(x, y) for a given set of angles can be considered as computing the projection of the image along the given angles4. The various angle of rotation is considered for the transformation and radon transformation is performed on the key added image.

The angle of rotation is taken as 0–45, 0–90 and 0–135. For each angle of rotation the image pixel values will be rotated.

6. Scrambling Algorithm

6.1 Pixel Column Transformation

The key value is expanded similar to the image size. Now the pixel value in the first column of the image is XORed with the bits stored in the first column of the key value. Then the remaining column values are XORed with the column values in the key shifted as one circular shift for 2nd column and two circular shifts for 3rd column and so on. This type of transformation is called column transformation. The same procedure is repeated for all the remaining columns. The process is depicted in Figure 3.

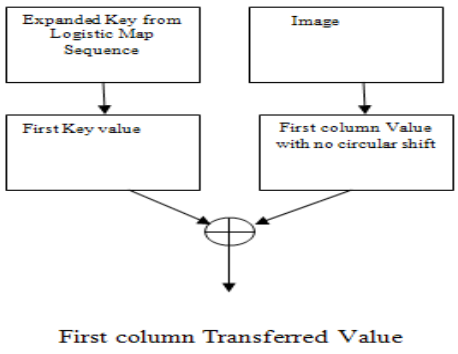

Figure 3. Pixel column transformation.

6.2 Pixel Row Transformation

After the column transformation, the pixel value in the first row of the image is XORed with the bits stored in the key. Then the remaining row values are XORed with the values in the key shifted as one circular shift for 2nd row and two circular shifts for 3rd row and so on. This type of transformation is called row transformation. The same procedure is repeated for all the remaining rows. The row transformation is shown in Figure 4.

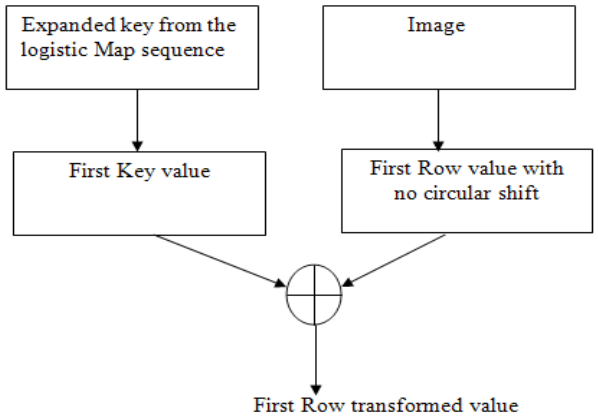

Figure 4. Pixel row transformation.

6.3 Block Transformation

After the scrambling algorithm, block transformation is performed on the image. That is, the image is divided into random number of blocks and transformation is performed. The original image is converted into encrypted image. The encrypted image is entirely different from the original image.

The input image and the segmented image are shown in Figure 5 and 6.

Figure 5. Input image.

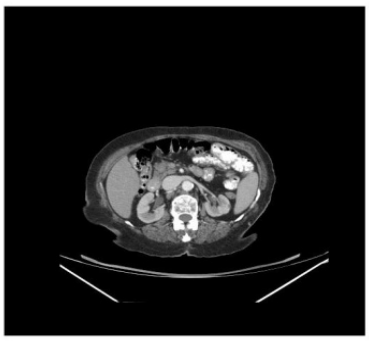

Figure 6. Segmented image.

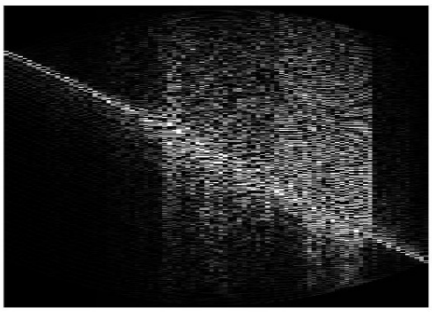

Figure 7. Radon projected image.

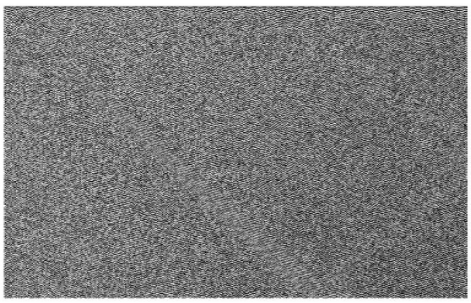

Figure 8. Transformed image for 45 degree rotation.

After the background separation, the logistic map output random generated key is taken to the radon transform. Then scrambling algorithm with block transformation is performed. The result is shown in Figure 7 and Figure 8.

7. Statistical Analysis of the Developed Algorithm

7.1 Histogram Analysis

The technique gives the data security to provide authentication of the medical images. The histogram of the image gives the frequency distribution of the intensity levels or grey values. The histogram of the original image and encrypted image are analyzed[8]. From the histogram graph, it is seen that the histogram of encrypted image is entirely different from the original Image. The histogram of the original and the encrypted image for 45 degree transform is shown in Figure 9 and Figure 10.

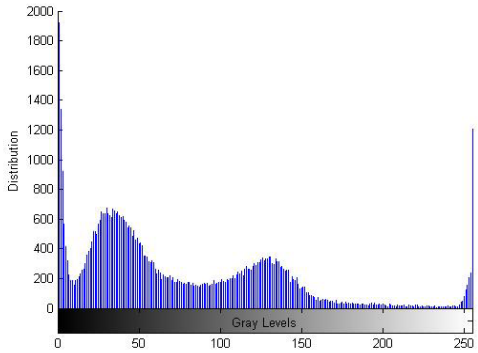

Figure 9. Histogram of the original image.

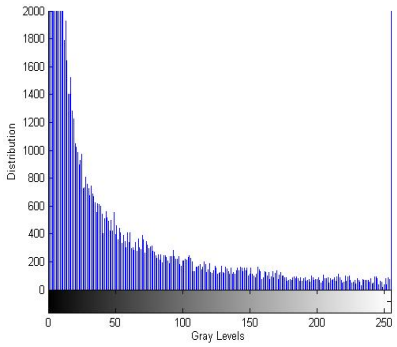

Figure 10. HHistogram of the encrypted image.

7.2 Encryption Quality Analysis

The Encryption quality of the image is calculated as follows:

Let F and F' denote the original image (plain image) and the encrypted image (cipher image) respectively, each of size M*N pixels with L grey levels. F(x, y), F'(x, y) ε {0,.., L −1} are the grey levels of the images F and F'at position (x, y) (0≤ x ≤ M −1, 0 ≤ y ≤ N −1). Let HL(F) denote the number of occurrences of each grey level L in the original image (plain image) F. Similarly, HL(F') denotes the number of occurrences of each grey level L in the encrypted image (cipher image) F'.

$$Encryption\ Quality = \frac{\sum_{L=0}^{255} |H_L(F') - H_L(F)|}{256} \quad \text{.....(4)}$$

Since the radon transforms the image in various degrees of rotation, in this work all the analysis of the image is done in terms of angles. Encryption qualities for the image using so many shifts in the angle for the given image are shown in Table 1 below.

Table 1. Encryption quality with a different angle of transform

Angle	Encryption Quality
0–45	804.5742
0–90	814.6680
0–135	820.2852

7.3 Entropy Analysis

Entropy is a measure of the uncertainty or randomness associated with a random variable. Entropy is defined by[6] as,

$$H_e = -\sum_{k=0}^{G-1} P(k)\log_2(P(k)) \quad \text{.....(5)}$$

Where He: entropy
G: grey value of input image (0….255)
P(k): is the probability of the occurrence of symbol k.

Entropy for the image using so many shifts in the angle for the given image is shown in Table 2.

Table 2. Entropy with a different angle of Transform

Angle	Entropy
0–45	4.6071
0–90	4.6201
0–135	5.6573

Performing block transformation alone does not give high encryption quality and entropy. So in order to improve the encryption quality and entropy, the image is projected for different angles, and then block transformation is performed[11]. This found to give improved results. Since an appreciable improvement in both encryption quality and entropy indicates combination of radon and block transformation provides better security compared to Block transformation alone.

To quantify the above said results in mathematical terms the Maximum Deviation Measuring Factor[7] is utilized. The factor measures the quality of encryption in terms of how it maximizes the deviation between the original and the encrypted images. The higher the value of Dev, the more the encrypted image is deviated from the original image.

The Dev calculated for the algorithm based on Radon and block transformation is given in the Table 3.

Table 3. Dev for algorithm based on Radon and Block transformation

Angle	Dev
0–45	16.4245x104
0–90	17.0393x104
0–135	20.9713x104

While using radon and block transformation, 209713 pixels out of 262144 pixels differs between original and encrypted image. This reaches a maximum of 80.30% of pixels difference during 135 degree rotation. So an algorithm is developed with the combination of radon and block transform. Higher the value of deviation factor, higher the encryption[10].

8. Conclusion

In a 512 * 512 sample image, from the histogram data how many pixels differ from the original image is computed. For this image, 209713 pixels has been altered from the original image of 262144 pixels which amounts to 80% of the pixels difference between the original and encrypted image during the 135 degree angle of rotation .Similarly 170393 pixels has been altered which indicate 65% of the pixels are altered between the original and encrypted image during the 90 degree angle of rotation whereas in 45 degree rotation, 164245 pixels are altered which amounts to 63% of pixels difference between the original and encrypted image. Since the 80% of pixels are altered at 135 degree of rotation, this angle can be taken as best angle for transformation. Normalizing these values with Maximum value of entropy the parameters will be 0.57, 0.58 and 0.72 for 45, 90 and 135 degree rotation.

The normalized parameter seems to increase with increase in angle of rotation and reaches maximum at 135 degree rotation.

Hence 135 degree of rotation is considered as a best angle of transform.

9. Results and Discussion

The current work allows the trust worthiness of the medical image without corrupting the image data. The DICOM image with 128 bytes is used and the scrambling algorithm with the chaotic sequence is used.

When the random transform projection angle is varied for 45 degree, 90 degree and 135 degree, the encryption quality gets increased which is shown in the experimental results. The experimental results show that the randomness of the pixel values increases the encryption quality and the entropy.

The results show that the maximum encryption occurs when the angle of rotation is 135. So the maximum randomness occurs when the angle of rotation is 135 degree. Similarly, the results of entropy value indicate that the there is a higher encryption of 80% for 135 degree of rotation. The key added with the transformed image also increases the randomness and provides authentication of images.

The encrypted image is highly uncorrelated with the original image so that probability of attack is very less. The uncorrelation between the original and encrypted image is calculated from the histogram data.

The differences in the number of pixels from the grey levels 0 to 255 are taken for original and encrypted image. The total number of pixels altered is calculated. For a sample image, 209713 pixels are altered out of 262444 pixels and this amounts to 80% of uncorrelation between original and encrypted image.

If the image is eavesdropped somewhere it looks like a noisy image to the attacker. The security is improved by the projection of data for various angles by the radon transformation.

Encryption quality and entropy are analyzed for the algorithm and the results are compared. Experimental results confirm that the encryption quality and entropy obtained from the images can clearly discriminate between the original and encrypted images. To clearly discriminate between original and encrypted data, the parameter called Maximum deviation measuring factor can be used as an index, which clearly discriminate between original and encrypted data and indicate the percentage of total pixels difference existing between the two images.

The DICOM images already have the inbuilt security, but the unused 128 bytes are left free and unused in the images. In order to improve the security and the performance of security level further, the 128 bytes are used for security analysis in the algorithm.

The results show that the encrypted image is entirely different from the original image. This work gives the trustworthiness in terms of security and improvement in the values of the parameters gives the efficiency of the algorithm.

10. Acknowledgement

This work was done in the Centre for Medical Electronics, Department of Medical Electronics, College of Engineering, under the supervision of Professor G. Ravindran. The authors thank the research scholars of Medical Electronics division for their support.

Conflict of Interest: "The author(s) declare(s) that there is no conflict of interests regarding the publication of this paper".

11. References

1. Kobayashi LOM, Furuie SS, Barreto PSLM. Providing integrity and authenticity in DICOM images: A novel approach. IEEE Trans Inform Tech Biomed. 2009; 13(4):582–9.
2. Keshari S, Modani SG. Image encryption algorithm based on chaotic map lattice and Arnold cat map for secure transmission. IJCST. 2011; 2(1):132–5.
3. Patidar V, Sud KK. A pseudo random bit generator based on chaotic logistic map and its statistical testing. Informatica. 2009; 33(4):441–52.
4. Tian H, Zhao Y, Ni R, Pan J-S. Spread spectrum-based image watermarking resistant to rotation and scaling using radon transform. Proceedings of the 2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP'10); 2010. p. 442–5.
5. Krishnamurthy GN, Ramaswamy V. encryption quality analysis and security evaluation of CAST-128 Algorithm and its modified version using digital images. IJNSA. 2009; 1(1):28-33.
6. Bani Younes MA, Jantan A. Image encryption using block-based transformation algorithm. IAENG International Journal of Computer Science. 2008; 35(1):1–9.
7. Abdulsattar FS. On the security of bitmap images using scrambling based encryption method. Journal of Engineering and Development. 2009 Sep; 13(3):147–57.

8. Vijayaraghavan R, Sathya S, Raajan NR. Security for an image using bit-slice rotation method-image encryption. Indian Journal of Science and Technology. Apr 2014; 7(4S):1–7.
9. Ramalingam M, Mat Isa NA. A steganography approach over video images to improve security. Indian Journal of Science and Technology. Jan 2015; 8(1):79–86.
10. Sasi SB, Sivanandam N. A survey on cryptography using optimization algorithms in WSNs. Indian Journal of Science and Technology. Feb 2015; 8(3):216–21.
11. 11. Ramalingam M, Mat Isa NA. Video steganography based on integer Haar Wavelet transforms for secured data transfer. Indian Journal of Science and Technology. Jul 2014; 7(7):897–904.