International Journal of ChemTech Research
CODEN (USA): IJCRGG ISSN: 0974-4290
Vol.8, No.6, pp 843-846, 2015

Comparison of Encryption Efficiency in DICOM Images based on Radon and Block Transform

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

[1]Sethu Institute of Technology, Pulloor, Kariapatti, India
[2]Anna University, Chennai, India

Abstract : This paper explains the comparison of encryption efficiency of an algorithm involving chaotic sequences in DICOM images based on Radon with block transform and Block transform alone. A novel method is developed using Pseudo Random Bit Generator (PRBG) based on logistic map with radon and block transform for encryption of DICOM images. To evaluate the performance level of the algorithm, various parameters are analyzed and their results are compared. The experimental results shows that the performance level of the algorithm is increased using radon in addition with block transform when compared with block transformation only. The computed results show that the encryption level increased up to 80% by using radon with block transform and the results show that the encrypted image is entirely different from the original image.
Key words: Encryption level, Radon Transform, Block Transform and PRBG.

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.

The Digital Imaging and Communication in Medicine (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 this algorithm.

Methodology:

The developed algorithm includes radon with block transform and block transform alone. 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 $X_0 \neq Y_0$)

$X_{n+1} = \lambda_1 X_n (1 - X_n)$ (1)
$Y_{n+1} = \lambda_2 Y_n (1-Y_n)$ (2)

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. The outputs of the logistic maps are compared with their respective median in the 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 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 input 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.

Encryption Method with Radon with Block Transform

The radon function computes the line integrals from multiple sources along parallel paths, or beams, in a certain direction.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 angles [2]. 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. After radon transformation, scrambling of the pixel values along column and row values is performed.

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.

Encryption Method with Block Transform

The DICOM image of size 512 × 512 is taken as an input image. The 128 unused bytes are used and the key from the PRBG is added with the DICOM image. Then, the block transformation is performed. Then, the pixel column and pixel row transformations are performed. The original image is converted into encrypted image. The encrypted image is entirely different from the original image.

Comparison of Encryption methods based on Radon and Block Transform

The encryption quality represents the average number of changes to each grey level L and is expressed mathematically by [3] as

$$Encryption\,Quality = \frac{\sum_{L=0}^{255} |H_L(F') - H_L(F)|}{256} \qquad (3)$$

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

Entropy Analysis

Entropy is a measure of the uncertainty or randomness associated with a random variable. Entropy is defined by [4] as

$$H_e = -\sum_{k=0}^{G-1} P(k)\log_2(P(k)) \qquad (4)$$

Where H_e : 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

To quantify the above said results in mathematical terms the Maximum Deviation Measuring Factor[5] is utilized. The factor measures the quality of encryption in terms of how it maximizes the deviation between the original and the encrypted images. 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. 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	16.4245×10^4
0-90	17.0393×10^4
0-135	20.9713×10^4

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.

The encryption quality for the image using number of blocks such as 8 × 8, 16 × 16, 32 × 32 and 64 × 64 for the given image are shown in Table 4 below.

Table 4: Encryption quality for various number of blocks

Number of blocks	Encryption quality
8 × 8	825.532
16 × 16	831.435
32 × 32	839.321
64 × 64	846.876

The entropy for the image using number of blocks such as 8 ×8, 16 × 16, 32 × 32 and 64 × 64 for the given image is shown in Table 5

Table 5: Entropy for various number of blocks

Number of blocks	Entropy
8 × 8	7.141
16 × 16	7.162
32 × 32	7.231
64 × 64	7.323

Dev for algorithm based on Block transformation is shown in Table 6.

Table 6: Dev for a sample image using Block transform

Number of blocks	Dev
8 × 8	14.1557×10^4
16 × 16	14.4179×10^4
32 × 32	15.2043×10^4
64 × 64	15.8123×10^4

Dev for algorithm based on Block transformation varies from 14.1557x 104 to 15.8123x104Due to the high randomness of the values, the entropy also increases when the number of blocks increases.

Conclusion:

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. 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.

References:

1. Luiz Octavio Massato Kobayashi, Sergio Shiguemi Furuie and Paulo Sergio Licciardi Messeder Barreto "Providing Integrity and Authenticity in DICOM Images: A Novel Approach", IEEE Transactions on Information Technology in Biomedicine, Vol.13, No.4, pp. 582-589, 2009.
2. Huawei Tian ,Yao Zhao, Rongrong Ni and Jeng-Shyang Pan "Spread Spectrum- Based Image Watermarking Resistant to rotation and scaling using Radon Transform", IIH-MSP '10 Proceedings of the 2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp. 442-445, 2010.
3. Krishnamurthy, G.N. and Ramaswamy, V. "Encryption Quality Analysis and Security Evaluation of CAST-128 Algorithm and its Modified Version Using Digital Images", International Journal of Network Security and its Applications (IJNSA), Vol. 1,No.1, pp. 28-33, 2009.
4. Mohammad Ali Bani Younes and Aman Jantan "Image Encryption Using Block-Based Transformation Algorithm", IAENG International Journal of Computer Science, Vol. 35, No. 1, 2008.
5. Fatimah Shamsulddin Abdulsattar "On the security of Bitmap Images using Scrambling based Encryption Method", Journal of Engineering and Development, Vol. 13, No. 3, pp. 147-157, September 2009.

*****