

## Anatomical Structural Analysis and Automatic Segmentation and Encryption Methods for MR Images

P. Muthu Krishnammal<sup>1\*</sup> and P. Raju<sup>1</sup>

<sup>1</sup>Assistant Professor, Sathyabama University, Chennai, India

<sup>2</sup>Senior analyst, Google Pvt Ltd, Hyderabad, India

doi: <http://dx.doi.org/10.13005/bbra/2250>

(Received: 10 May 2015; accepted: 07 August 2015)

The secrecy of the multimedia data like video imaging is now becoming very essential because of the huge exchange of information in the form of images is done very frequently over the modern communication network world. Hence it is very necessary to maintain network security and to use the efficient authentication algorithms to maintain the high degree of confidentiality in the applications such as Internet communication, military communication, Geographic information systems, sensitive visual aids, and confidential images used in telehealth technologies etc. This paper presents the literature survey on the different encryption and decryption methods addressed in the previous papers. Also, the automatic segmentation of the MR images using K-means and Fuzzy Clustering Means (FCM) are done and thereby, the encryption and decryption using two methods namely Chaos and Selective encryption and decryption methods are proposed. Then the performance analysis is done using the probabilistic parameters like area, mean, standard deviation and entropy is done. Finally the comparison of the methods is done.

**Keywords:** Automatic segmentation, K-Means, Fuzzy C means, Chaos encryption, Selective encryption, MR imaging

---

The modern age network technologies and communication media services provide very convenient channels for individuals and the various organizations to share and collect videos or images using the wireless or multimedia networks. So it is more unprotected by the duplication of digital images and is being re-distributed by the hackers. Hence image security becomes a major challenging issue to be considered in transmission and storage applications. The significant points to be considered in the transmission of digital images are: images having the special properties like bulk data capacity, high degree of correlation between the adjacent pixels, and their higher redundancy

rate. So the best solution to send the images securely leads to the efficient use of cryptographic algorithms.

The secure transfer techniques can be categorized into steganography and cryptography. Steganography is the art or practice of protecting or covering a message, image, or file within another message, image, or file. Cryptography includes two processes namely: encryption and decryption. Encryption is the conversion of ordinary information (plaintext) into unintelligible text (cipher text). Decryption is the reverse, which is moving from the unintelligible cipher text back to plaintext<sup>1</sup>. It can be done in two ways: Private-key and public-key encryption methods. The private-key encryption is based on the principle that the transmitter and the receiver agree on a common secret key before they can communicate. Without the aid of the secret key, the cipher text is indiscernible. This unintelligible data can be

---

\* To whom all correspondence should be addressed.

converted back to original plaintext by the receiver by the process of using the same commonly shared key. The disadvantage of the scheme is that the secure channel between the two parties is critical. In public-key encryption method, the secret keys are shared over the communication or public channel. Instead of this, both sender and receiver have a pair of keys like public key and private key. Here, the public key is reported openly, but the private key for decryption is kept strictly secret. Moreover, it is computationally impossible to obtain the concerned private key from the public key. Hence all communications can be carried with public key only so that the secure communication is possible<sup>3</sup>.

Traditionally the cryptographic methods were dealt only with the secure transfer of textual data and the encryption of textual data was mostly related to one dimensional data. But nowadays it is very capable of handling any type of data. The conventional encryption algorithms such as DES, AES, and RSA etc focused on changing the 2D data into 1D data and the applying encryption on it. But this method was less efficient because of the internal features of image data like bulk data capability and high redundant data and was not desirable to be used as the standard style of encryption on digital imaging<sup>1-2</sup>. There are a number of encryption algorithms have been proposed for encrypting the digital images. Among them, chaos based encryption methods are preferred to accomplish the need for secure and reliable protection, transmission and storage of the digital images over the public communication channels or networks. As the chaotic signals have the desirable features like high randomness, high sensitivity to initial conditions and long periodicity<sup>2</sup>.

#### **Literature survey**

According to the challenges mentioned in protecting the multimedia content, the objective of the paper is the analysis of chaos based encryption methods. In the previous works, both the analog and digital chaotic encryption methods had been proposed and analyzed. The main characteristics of chaos are: (1)The chaos signals appears like noise for the illegal users.(2)The properties like sensitivity to the initial conditions and mixing, that can be connected to the cipher operations such as confusion and diffusion. Apart

from these advantages, the generation of chaotic signals is of low cost by simple iterative operations which also make it desirable for the stream cipher construction. The pseudo-random key generation which is used to encrypt the original plaintext is done by using the chaotic systems<sup>4</sup>.

R.Gopinath et al proposed the lossless encryption method for color images using two algorithms that are: Bitplanecrypt and Edgemapcrypt algorithms. In the Bitplanecrypt method, the color images were taken and the different color components (R, G, B) were splitted. The keys were generated and the size of the key-image was the same as the original image. Then xor operation was performed between the each bit-plane of the original image and the key-image. Then the order of all the bit-planes was inverted. The resulting image is scrambled using the selective scrambling to get the encrypted image. On the receiver end, the exact keys should be provided for the authorized user, in order to generate the key-image and the order of bit-planes are reverted to get the original order for each bit-plane. Then all bit-planes are combined to reconstruct the original image. In the edgemapcrypt algorithm, the edge map from the existing image is calculated and its size is of the same as original image. Then original color image is decomposed into binary bit plane and the xor operation is applied between the bitplane and the edge map. Then, the 3D image is obtained by combining all the bit planes together. Then the resulting image is scrambled using a selected scrambling method thereby the encrypted image is generated. The advantage of these two methods is, as the algorithms operate on binary levels, it is very easy to implement in hardware<sup>5</sup>.

Christos K volos proposed an image encryption scheme based on a true random bits generator. The two identical nonlinear circuits which are mutually coupled that produce double scroll chaotic attractors were included in the chaotic generator. The keys of cryptographic system are the values of the system parameters and the initial conditions. The two different types of synchronization (complete to represent the state '0' and inverse  $\delta$ -lag synchronization to represent '1') methods were used, as the dynamic characteristics of the coupled system are uncertain. The bit sequence produced by adapting FIPS for testing the distribution of the bits sequence was

used for the encryption and decryption of the images. The security analysis demonstrated the high security level for the proposed method<sup>6</sup>.

K. DeerghaRao et al proposed a new cryptosystem based on chaos and BB (Brahmagupta- Bhaskara) equation for image encryption and decryption. Here, for every pixel of the image, the root pair of the BB equation was found for the given primary key. Then, a mod operation was done on the root pair of the BB equation according to the binary sequence that is being generated by the chaotic generator. Then XNOR or XOR operation was done bit-by-bit basis on each root pair to any one of the predetermined keys. Thereby the encrypted image was generated. The same binary sequence was applied to the decryption unit and the exact modulo inverse operations were done to get the original image. Here by choosing the greater values of key bit lengths the security of the cryptosystem was guaranteed against the cipher attacks<sup>7</sup>.

Ramesh Kumar yadava et al proposed a chaotic encryption method based on Henon mapping. In this method, the encryption is done in the following steps: Firstly, the colour transformation was done to separate the R, G, B components. Then, Henon like chaotic map is converted to 1-D chaotic map. Then random bit stream is generated by the way in which 1D Henon chaotic map takes the R component of the image. The original pixel values of the R component is bit XORed with the bit values resulted in the last step. To produce the cipher image, the G and B components of the transformed colour image and the bit vector matrix from the last step obtained produces the cipher image. In the decryption stage, the 1D chaotic map was the same as the encryption stage. Then the colour transformation to separate the RGB components is done. Then the secret key and the parameters are chosen which generates the transform matrix for the R component's pixel values of the colour image. Then the XOR operation was done between the transform matrix of R component image and the R component of the cipher image. The decryption returns a value of RGB using the image transformation in order to produce the original image. The work proposed has the large key-space to get resisted for all possible types of attacks<sup>8</sup>.

Suganya G et al proposed a joint

encryption and watermarking technique for verifying the reliability of medical images. By the combined watermarking algorithm and QIM (Quantization Index Modulation), with an encryption algorithm, the medical image integrity control is achieved. In this method, two encryption techniques RC4, AES as Stream cipher, Block cipher algorithm were used. The first step involved is the construction of codebooks. Then the insertion of message in spatial and encrypted domain is performed. The joint encryption and watermarking involves two steps: Firstly, the image is divided into non-overlapping blocks of N pixels. The message is formed according to the authenticity code and inserted to the encryption domain using the secret key. The messages embedding and encryption are done together for each block. Using the sub-codebooks, one bit of spatial message and one bit of encrypted message are inserted jointly. After computing the encrypted and watermarked version, using selective encryption the encryption is done. The watermark and the message extraction is done independently using the secret watermarking key which is done in the verification stage. Then in the encryption domain, the encrypted image is decomposed in N bytes for each block. The spatial message is extracted using QIM in the spatial domain and a function is applied to extract one bit of encryption message. This method guarantees better integrity control as it uses joint techniques<sup>9</sup>.

Ahmed Mahmood et al proposed symmetric encryption technique which can be applied to the medical images. Here, genetic algorithm is used which makes it highly adaptive. The segmentation of DICOM images done based on entropy and pixel intensity which yields a number of regions. Then the selective encryption is applied to all the regions separately. The encryption is done by a low processing algorithm such as the Gold code, low information regions are encrypted and by using a standard algorithm like AES, high information regions encrypted. The other methods like DES or Blow Fish methods can also be to encrypt the remaining regions. Hence the processing time is reduced and the quality of the encrypted image is also maintained. This method is a faster, more robust encryption that can adapt to the information content of each individual image<sup>10</sup>.

### Proposed Method

#### Block Diagram

In the Proposed method, the MRI images are collected from the internet and the noise is removed from the images. Then the two different segmentation algorithms namely K-Means clustering and Fuzzy C Means clustering are applied. It is a process of partitioning an image into different regions having same features and is often used to extract region of interests (ROI). In medical imaging field, this technique is mostly used to detect tumors from MRI images of brain and mammograms. Then from the segmentation results, an image is selected and the encryption and decryption are done using the two techniques namely Chaos encryption and Selective encryption. Then the performance of the segmentation methods and encryption methods are evaluated in terms of PSNR, Correlation coefficient, processing time and also with the histogram analysis, keyspace analysis for the different types of possible attacks.

#### Segmentation methods

##### K-Means segmentation algorithm

K-means<sup>11-13</sup> algorithm is a simple segmentation method. The advantages of K-means algorithm are simplicity, very high execution speed. But the drawback is that if the initial cluster centers are not chosen correctly, this algorithm may not converge. This happens mostly in the case of noisy images. It is an unsupervised clustering algorithm that classifies the input data points into multiple classes based on their euclidean distance from each other. The points are clustered around centroids  $\zeta_i \forall i=1,2,\dots,k$  which are obtained by minimizing the objective

$$V = \sum_{i=1}^k \sum_{x_j \in S_i} (x_j - \zeta_i)^2 \quad \dots(1)$$

Where k clusters are there for  $s i=1,2,3,\dots,k$  and  $\zeta_i$  is the mean point or the centroid. The steps involved in K-Means clustering algorithm are as follows:

- i) The intensity distribution which is also called as the histogram intensity is computed.
- ii) The centroids with k random intensities are initialized.
- iii) The points in the dataset are clustered based

on distance of the intensities from the centroid intensities using

The new centroid for each of the clusters is calculated by

$$\zeta_i = \frac{\sum_{i=1}^m 1\{c_i = j\} x^i}{\sum_{i=1}^m 1\{c_i = j\}}$$

Where k is the number of clusters to be assigned, 'i' iterates over the all intensities and 'j' iterates over all the centroids and  $\zeta_i$  are the centroid intensities.

- v) Repeat steps (iii) and (iv) until the entire region converges.

##### FCM segmentation algorithm

FCM clustering<sup>13-15</sup> is an unsupervised clustering method used to segment images into clusters with similar spectral properties. The FCM algorithm uses fuzzy memberships to assign pixels to each category using. To compute the membership function, it uses the distance between pixels and cluster centers in the spectral domain. Let an image with N pixels be denoted as  $X = (x_1, x_2, \dots, x_N)$  and is to be partitioned into 'c' clusters and  $x_i$  be representing the multispectral (featured) data. This algorithm is an iterative optimization that minimizes the cost function which can be defined as:

$$J = \sum_{j=1}^N \sum_{i=1}^c u_{ij}^m \|x_j - v_i\|^2$$

Where  $u_{ij}$  is the membership of the pixel  $x_j$  in the  $i^{\text{th}}$  cluster,  $v_i$  is the  $i^{\text{th}}$  cluster center, and 'm' is a constant. Here, the parameter m controls the fuzziness of the resulting partition. The membership function is representing the probability that a pixel belongs to a particular cluster. In the FCM algorithm, this probability depends on the distance between the pixel and each individual cluster center in the feature set. By assigning high membership values to the pixels that are close to the centroid of their clusters and low membership values to the pixels that are far from the centroid, the cost function can be minimized. The membership functions are updated by using

$$u_{ij} = \frac{1}{\sum_{k=1}^m \frac{\|x_j - v_k\|}{\|x_j - v_k\|^{2/(m-1)}}}$$

And the cluster centers are updated by using the equation

$$v_i = \frac{\sum_{j=1}^N u_{ij}^m x_j}{\sum_{j=1}^N u_{ij}^m}$$

**Encryption Methods**

**Chaos Encryption and Decryption**

The encryption is done on the basis of chaotic logistic map. It is an iterative mathematical system which can be used for random numbers generation, defined by following iterative equation:

$$f_x = \mu * f_x * (1 - f_x)$$

Where  $\mu$  is growth rate parameter. Once the chaotic map is generated using the above iterative equation, the sequence is converted to binary by using a threshold function by using the condition i.e. value  $>(i/255)$  && value  $<((i+1)/255)$  and thereby random binary sequence is generated. In this method, two random numbers sequences are generated based on chaotic logistic map. One sequence is used for row pixels, another for column pixels. This is done by taking both the random sequences together. Then a masking operation that is bitwise xor operation is done between adjacent rows and columns. The reverse process is done to get the decrypted image.

**Selective Encryption**

Long keys are required for the encryption algorithms in order to achieve high level of security

and also to maintain security for the medical images. But the use of long encryption keys makes the method inefficient because of the increased processing time. Therefore, an encryption scheme called selective encryption by AES is applied to improve the robustness and also reduce the processing time of the images. Selective encryption is an important technique which is applied to the encryption to the single subset of the data. Here, the level of security is also maintained.

**RESULTS**

**Results for segmentation stage**

The results of segmentation by the two different methods namely K-Means clustering and Fuzzy C-means clustering and the detected tumor regions are displayed here in the tabular format. The image 1 belongs to normal case where the second and third images are with tumor belonging to benign and malignant classes.

**Performance Evaluation**

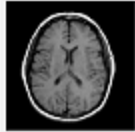
















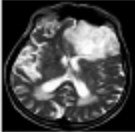


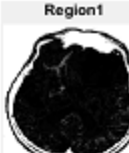













**Segmentation stage**

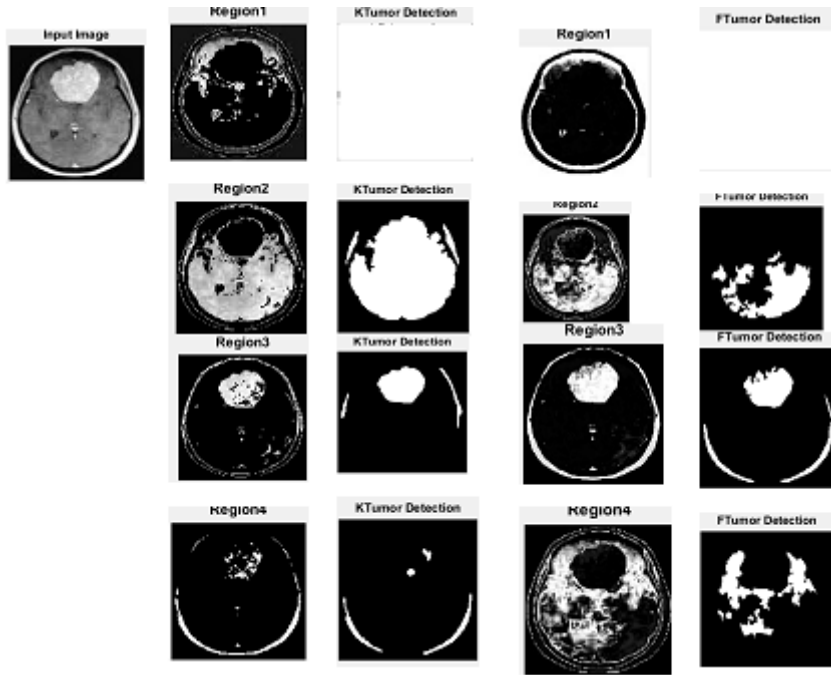
The segmentation methods are validated using the following statistical parameters namely: area of the tumor detected, mean, standard deviation and entropy. The values for K-means segmentation and Fuzzy c means segmentation methods are tabulated for the different clusters of the different images. From the parameters it is evident that the FCM results in better segmentation compared to K-means segmentation.

Input image	K-Means segmentation –Validation Parameters				FCM segmentation –Validation Parameters			
	Area	Mean	Standard deviation	Entropy	Area	Mean	Standard deviation	Entropy
Image1-cluster1	43.2138	0.40884	0.49162	0.97589	2.64	0.0015259	0.039033	0.016476
Image1-cluster2	36.1786	0.28656	0.45216	0.86424	30.7013	0.20636	0.40469	0.73447
Image1-cluster3	0	0	0	0	67.5819	0.99994	0.0078123	0.00094254
Image1-cluster4	3.5518	0.0027618	0.052481	0.027455	60.7617	0.01001	0.099548	0.080858
Image2-cluster1	62.7982	0.86339	0.34344	0.5753	10.2689	0.023087	0.15018	0.15844
Image2-cluster2	14.4043	0.045425	0.20824	0.26664	21.5948	0.1021	0.30278	0.47561
Image2-cluster3	22.4245	0.1100918	0.31301	0.50019	40.154	0.353	0.47791	0.93672
Image2-cluster4	13.6312	0.04068	0.1975581	0.2454	33.3519	0.24353	0.42922	0.80086
Image3-cluster1	67.5675	0.99951	0.022092	0.0060754	67.5819	0.99994	0.0078123	0.00094254
Image3-cluster2	46.0769	0.46481	0.49876	0.99462	28.2048	0.17416	0.37925	0.66714
Image3-cluster3	21.009	0.096558	0.29536	0.45799	22.0294	0.10625	0.30816	0.48849
Image3-cluster4	12.3206	0.033234	0.17925	0.21036	23.9819	0.12592	0.33176	0.54613

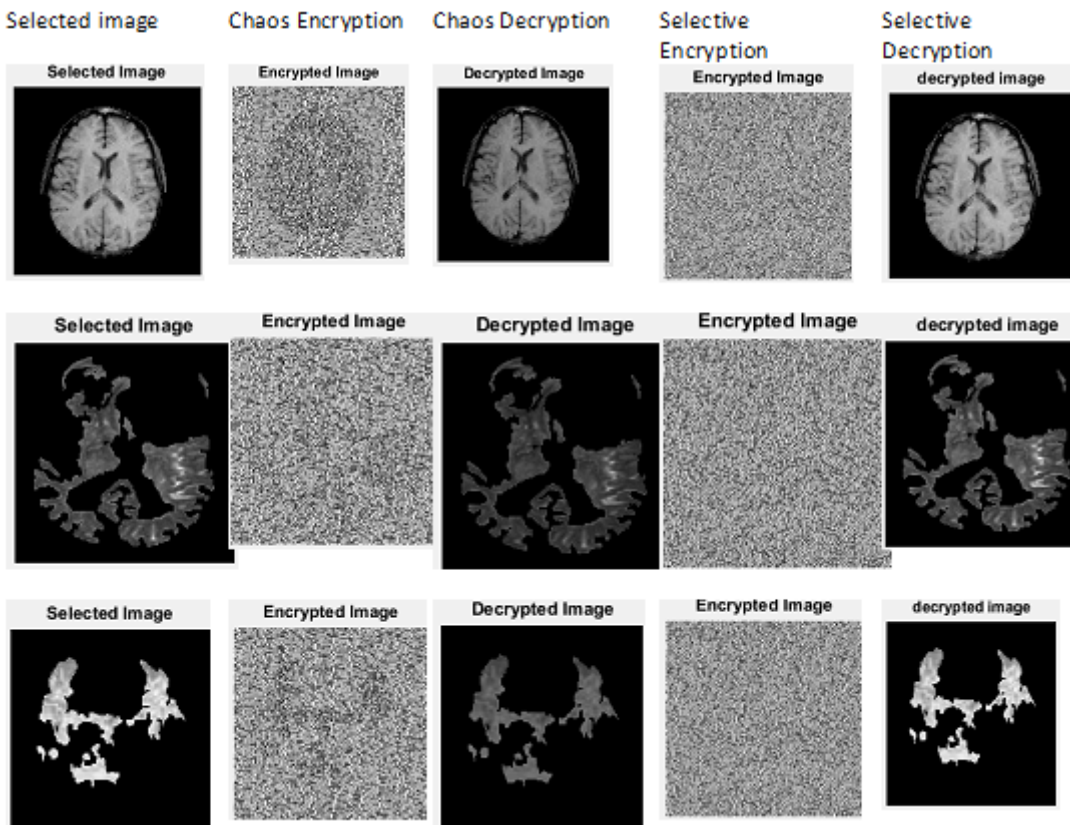


**Table 1.** Results for segmentation stage results for segmentation stage

Input image	Segmentation by K-Means	Tumor detection	Segmentation by FCM	Tumor detection
				
				
				
				
				
				
				
				



Results for Encryption Stage

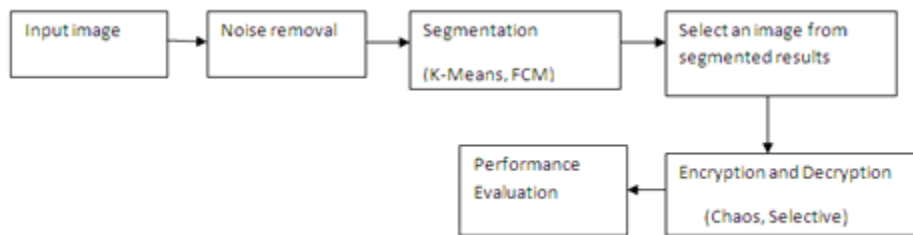


**Encryption stage**

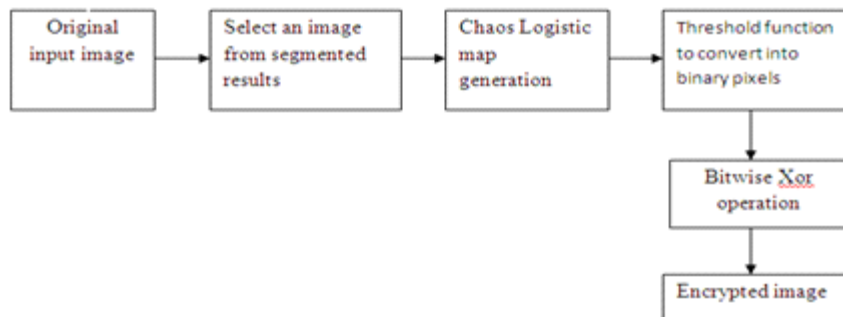
An image is selected from the segmented results and the encryption methods namely Chaos encryption and Selective encryption are applied and the performance of the methods are evaluated using the process time, mean square error and the

correlation coefficient between the adjacent pixels and the values are tabulated. Selective encryption results in better performance in terms of less processing time encryption and close relationship with the keys compared to chaos encryption.

Input image	Chaos encryption- Performance Parameters			Selective encryption- Performance Parameters		
	Process time(sec)	Mean Square Error	Correlation Coefficient	Process time (sec)	Mean Square Error	Correlation Coefficient
Image1	1.0562	35.6249	0.1471	0.1523	81.3274	0.0025
Image2	1.0568	11.8425	0.0855	0.1399	27.1490	0.0013
Image3	1.0573	10.5592	0.1090	0.1406	28.8352	0.0011



**Fig.** Block Diagram of the proposed system



**Fig.** Chaos encryption block diagram

**CONCLUSION**

The complexity of cipher text attack depends on the key length. Therefore the computational complexity can be increased by increasing the key bit length. So the proposed cryptographic method’s performance can be improved by the larger key bit lengths to make the different possible types of attacks like brute-force attacks and differential attacks. Similarly, good encryption method needs high level of sensitivity to cipher keys which means that the cipher text

should have very close correlation with the keys. The analysis show that the proposed encryption methods are highly secure.

**REFERENCES**

1. Akhil Kaushik *et al.*, “ Chaotic image encryption standard” , International journal of computer applications, 2012; 57(8). ISSN:0975-8887, 45-49.
2. Abhishek Misra *et al.*, “Analysing the Parameters of Chaos Based Image Encryption Schemes” World Applied Programming, 2011; 1(5): 294-



- 299,ISSN: 2222-2510
3. SukhjeevanKaur et al , “A review of image encryption schemes based on the chaotic map” *Int.J.Computer Technology &Applications*,Vol 5 (1),144-149,ISSN: 2229-6093
  4. KamelFaraoun,”Chaos-Based Key Stream Generator Based on Multiple Maps Combinations and its Application to Images Encryption”,*The International Arab Journal of Information Technology*, 2010; **7**(3).
  5. R.Gopinath et al, “Image Encryption For Color Images Using Bit Plane And Edge Map Cryptography Algorithm” *International Journal of Engineering Research & Technology (IJERT)*,ISSN: 2278-0181, 2012; **1**(8).
  6. Christos K volos, “Image encryption based on coupled chaotic systems”, *Journal of Mathematics & Bioinformatics*, 2013; **3**, no.1,2013 ,pp 123-149, ISSN: 1792-6602.
  7. K. DeerghaRao, “A New and Secure Cryptosystem for Image Encryption and Decryption” *IETE Journal of Research* | 2011; **57**(2):165-171
  8. Ramesh Kumar yadava et al, “A New Approach of Colour Image Encryption Based on Henonlike Chaotic Map”, *Journal of Information Engineering and Applications*, ISSN 2224-5782 (print) ISSN 2225-0506 (online) 2013; **3**(6): Selected from International Conference on Recent Trends in Applied Sciences with Engineering Applications.
  9. Suganya G, Amudha K, “Medical Image Integrity Control Using JointEncryption and Watermarking Techniques” International Conference on Green Computing Communication and Electrical Engineering (ICGCCEE), 2014, pp1-5
  10. Ahmed Mahmood Et Al, “An Adaptive Encryption Based Genetic Algorithms For Medical Images”, 2013 IEEE International Workshop On Machine Learning For Signal Processing, Sept. 22–25, 2013, Southampton, UK
  11. Mrs.P.Muthu krishnammal, Dr.S.Selvakumar Raja, “Automated Brain Image classification using Neural Network Approach and abnormality Analysis” *International Journal of Engineering and Technology (IJET)* ISSN : 0975-4024; **2015**; **3**(7): 876-886.
  12. ShrutiDalmiya et al , “Application of Wavelet based K-means Algorithm in Mammogram Segmentation” *International Journal of Computer Applications* (0975 – 8887) 2012; **52**(15).
  13. Hartigan, J.A., Wong, M.A.: Algorithm AS136: A K Means Clustering Algorithm. *Applied Statistics* 1979; **28**: 100–108.
  14. Keh-Shih Chuang et al, “Fuzzy c-means clustering with spatial information for image segmentation” *Computerized Medical Imaging and Graphics* 2006; **30**: 9-15
  15. Mrs.P.Muthukrishnammal, Dr.S.Selvakumar Raja, “Clustering And Neural Network Approaches For Automated Segmentation And Classification Of MRI Brain Images” *Journal of Theoretical and Applied Information Technology*, 2015; **72**(3): 322-330.