Secure Selective Image Encryption Technique for Real Time Applications

Kiran
Dept. of ECE, Vidyavardhaka College of Engineering, Mysuru

Parameshachari B.D.
Department of Telecommunication Engineering, GSSS Institute of Engineering & Technology for Women, Mysuru

ABSTRACT
With the advent of medical imaging tools and telemedicine technology, patient information, medical imaging data is subject to strict data protection and confidentiality requirements. This raises the issue of sending medical image data within an open network due to the above issues, along with the risk of data / information leakage. Potential solutions in the past included the use of information hiding and image encryption techniques. However, these methods can cause problems when trying to restore the original image. In this work, developed an algorithm that protects medical images based on the pixels of interest. Image histogram peak detection for calculating peaks in medical images. Threshold value processed pixels of interest in medical images. The average of all peaks in the histogram indicates the threshold. These pixels are then encoded with interest values using a Sudoku matrix. The proposed scheme will be evaluated using various statistical tests and these results will be compared to existing benchmarks. The results show that the proposed algorithm has better security performance compared to existing image encryption schemes.

General Terms
Security, Real time applications

Keywords
Pixels of Interest, Medical Images, Encryption, Histogram, Peak Detection

1. INTRODUCTION
Medical imaging research has made remarkable progress as a result of increased and improved investment in multimedia technology. The medical image contains the patient's important personal privacy information. Medical images are usually encrypted to protect sensitive content. Common encryption methods such as Advanced Encryption Standard (AES), Data Encryption Standard (DES) International Data Encryption Algorithm (IDEA), Triple DES to protect text data is commonly used. Medical image data has an uneven distribution of image pixels, obvious regional features, and high resolution. Traditional cryptography is not suitable for protecting images from digital imaging and communication (DICOM) in medical care due to the inefficiency of bulk data.

2. RELATED WORK
Medical imaging is an essential and effective secondary source of information when medical personnel need to diagnose a patient [1]. Unfortunately, the quickest (and generally most efficient) way to share medical images is usually through open networks such as file sharing and email. These types of transfers expose images to activities such as content manipulation, illegal copying, and copyright loss [2]. As a result, research into medical image security focused on image encryption and information hiding has grown [3]. Dong xie [4] explained a simple but efficient method by using matrix multiplication to alter the pixel values in the image, which made the algorithm very simple but also made it very difficult for intruders to extract the information in the images. 5-D hyper chaotic map discussed by Shuqin Zhu and Congxu Zhu [5] was actually the result of combining logistic map with 3D Lorenz, which exhibited dual operating modes. One of the modes focuses only on the pixels obtained from clear text images while the other mode performs diffusion twice in order to obtain secured images. The security issue addressed by Mohammed [6] made the confidential data from the web users to be shared on web applications without fear and hence preserving their privacy. 1-D chaotic map was improvised by Ming Li et.al [7] to obtain more security by identifying its drawbacks, followed by the introduction of modified version of chosen plain text attack. Manjula and Mohan H S [8] showed the secret data hiding in a part of an image by choosing an important part in medical image which can be normally done by selecting the more used parts of the image. WonyoungJangand Sun-Young Lee [9] proposed an algorithm for partially encryption of confidential data in images with the help of FF1 and FF3-1. The confidential data will be encrypted without increasing the data size which may leads to wastage of storage space. VeeramalaiSankaradass et.al [10] introduces the gray scale encryption technique based on ROI with chaos. Initially the ROI part has to be identified using Sobel edge detection method. Then the image has to be classified into important and unimportant parts using the edges in the blocks. The Lorenz system encrypts the ROI part and Sine maps are used to encrypt the unimportant region. SeyedMojtaba Mousavi et.al [11] presents a self-generating region of interest (ROI) method for watermarking application in biomedical images. This technique is robust enough to prevent many attacks such as Gaussian, median, sharpening and wiener filters, which is the major advantage over other methods. Jinqing Li et.al [12] discussed a new method in which he demonstrated how to determine the region of interest (ROI) to the perfect accuracy, also to avoid information leakage in ROI part, and how to recover the information lossless from encryption in transform domain. So here we come across a novel lossless game theory based medical image encryption scheme with optimised ROI parameters along with ROI hidden positions. The process of encryption involves the pixel level transformation of ROI to recover the medical image lossless and also to protect the loss of the information in the medical image. Various methods are used for chaos based encryption techniques that are discussed here [13]. Kumar [14] et al to improve the hidden capacity, we proposed an improved HS reversible watermark algorithm for medical images. Divide the image into smaller blocks for data embedding based on HS technology. Yang et al. [15] prioritizes integrating data into texture regions by means of

HS and contrast enhancement, improving texture area contrast and improving subjectively perceived image quality. Wu et al. [16] use reversible image masking scheme for HS to protect patient information, then two parameters of linear prediction with weight and threshold are applied to improve image quality. Economy and rate 'integrated. Huang et al. [17] proposes an HS method to examine the hidden lossless data in high-resolution medical images. Use high correlation for the smooth surface of medical imaging anatomy in the local block pixels of the image. It is very easy to adjust the capacity, signal-to-noise ratio (PSNR) according to block size, partition level and number of embedded bits. Many of the goals of the above methods are to ensure copyright protection of the image and to minimize distortion in the image quality of the embedded image. Image histogram peak detection is a fundamental technique for digital image processing that can be used directly and effectively for image segmentation, quality assessment, enhancement, data reduction, etc. Common peak detection methods can be divided into direct and indirect methods. When using the direct method, peaks can be obtained by directly analysing the discrete data [18-19]. The conventional indirect method consists of two steps. The first step is to fit the data to obtain a probability density function (PDF) [20–23]. The second step is to calculate the derivative of the PDF to obtain significant peaks. The indirect method is said to be more stable, although it has some disadvantages: B. Inaccurate peak position and noise from local spurious peaks. Rashmi p and. al [24-26] proposes Advanced Chaos Cryptography (ICE) is applied to improve chance-based security. The average energy is calculated on the image and compared with the adaptive threshold to segment the Lorenz 96 model applied with Chaos encryption algorithm to improve the security of the model and also explain the encryption technique ROI-based imaging based on two-plane decay.

Rest of the sections as follows. Section 3 explains the basic concept of Sudoku used in the proposed encryption method. Section 4 gives the explanation of proposed work. Section 5 gives the performance analysis and finally section 6 gives the conclusion of work.

3. SUDOKU MATRIX

Here we define a Sudoku matrix as an X * X matrix containing numbers from 1 to N, but since X is the square of the number and N = X, each number occurs only once in each row. Increase only once in each column, only once in each block. Figure 1 below shows an example of a Sudoku puzzle and a solution for X = 9. The solution of the Sudoku puzzle is called the Sudoku matrix.

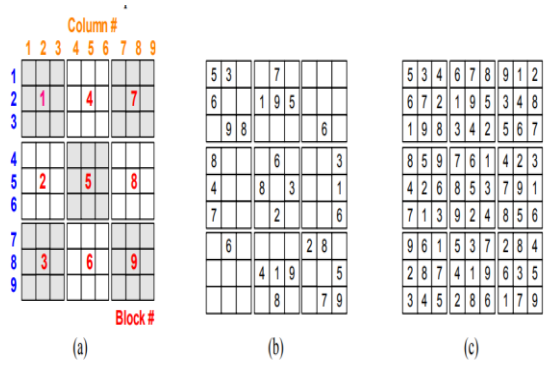

Figure 1: A sample Sudoku puzzle and its solution (a) Row#, Column # and Block# notation; (b) A sample Sudoku puzzle; (c) The solution to Sudoku puzzle (b)

Sudoku puzzles are usually generated from the Sudoku Matrix by removing some elements, but they contain some tips for their own solutions. Researchers have endeavored to create a variety of possibilities. In this article, we will use the Latin square method to generate a Sudoku matrix. The disadvantage of this fast and systematic method is that the set of Sudoku matrices generated by this method is a subset of the universal set of all possible Sudoku matrices.

4. PROPOSED SELECTIVE ENCRYPTION WORK

Block diagram of proposed selective image encryption system as shown in figure 2. Proposed system consists of various stages to select and encrypt the region of intrest in the medical image. Firstly compute the histogram peak of original image and as shown in the figure 3.The peak detection algorithm first generates a peak detection signal from the image histogram. The peaks in the histogram are then identified using the extrema between the zero and zero intersections of the peak detection signal. Convolution using a differentiator approximates the first derivative. For an ideally smooth histogram, the peak can be determined from the sign and zero intersection of the signal resulting from the h and S convolution. Zero intersection estimates the extrema of the histogram and the position of the turning point. Symbol '*' in figure 3 indicates the peak values of original medical image. Threshold value for segregating the significant pixels of medical image can be calculated by taking the average of all the peak values obtained in histogram peak detection. Then compare every pixel of original medical image with threshold value and if it is greater than threshold values then grouping into significant pixel block. Sudoku matrix of multiple random 16*16 generated for diffusing operation. By using pixels in the sudoku matrix randomly encrypt the significant pixel block by performing XOR operation.

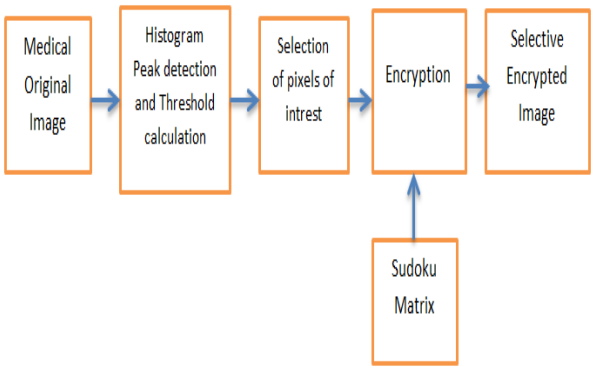

Figure 2: Architecture of Proposed Visible Image encryption method

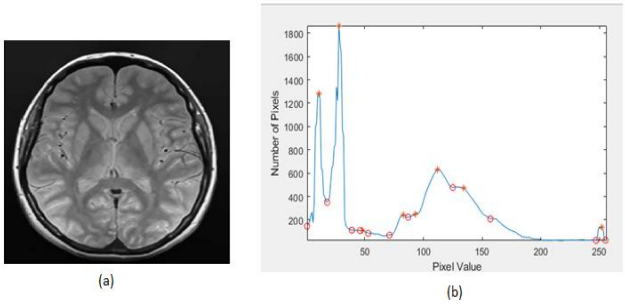

Figure 3: (a) Original MRI image (b) Peak detection using Histogram

5. RESULT AND DISCUSSION

Different parameters should be evaluated to analysis the performance of proposed scheme. The following parameters are involved as follows.

a. Entropy Analysis

Entropy is a measure of the degree of randomness in a cryptographic system. Entropy is calculated using Equation [27-28]:

$$H(S) = \sum_{i=0}^{2^M-1} P(si)\, log_2 \frac{1}{P(si)} \quad (1)$$

Where P (si) represents the probability of the i[th] gray level occurring in the image. The ideal entropy value for a random image is 8. If it is low, it is more predictable. Table 1 shows the entropy of some sample images and their corresponding cryptographic images.

b. Mean Square Error (MSE)

MSE is generally analyzed by averaging the squares of the differences between plain and scrambled images. The higher the value of MSE, the higher the encryption and the more noisy the clear image. The formula for MSE [29] given by.

$$MSE = \frac{1}{MXN} \sum_{i=1}^{M} \sum_{j=1}^{N} [inp(i,j) - enc(i,j)]^2 \quad (2)$$

c. Peak Signal to Noise Ratio (PSNR)

Peak signal to noise ratio is always the reciprocal of the mean squared error (MSE). Cryptographic image quality is usually measured by the amount of PSNR. Increase MSE and reduce PSNR for better image security. Mathematically, the PSNR is given as follows [29].

$$PSNR = 10\, log_{10} \frac{255}{MSE} \quad (3)$$

d. UACI and NPCR

Peak signal to noise ratio. This is always the reciprocal of the mean squared error (MSE).

Cryptographic image quality is usually measured by the amount of PSNR. Increase MSE and reduce PSNR for better image security. Mathematically, the PSNR is given as follows [29].

$$UACI = \frac{1}{N} \left[\sum_{i,j} \frac{|C1(i,j) - C2(i,j)|}{255} \right] (4)$$

Where m is the number of rows, n is the number of columns, and C1 (i, j) and C2 (i, j) are the original image and the encrypted image, respectively. According to the formula. Five

$$NPCR = \frac{\sum_{i,j} D(i,j)}{MXN} X100\% \ (5)$$

Where, m represents number of rows, n indicates number of column and where D(i,j) defined as follows

$$D(i,j) = \begin{cases} 1, C1(i,j) \neq C2(i,j) \\ 0, \quad otherwise \end{cases} (6)$$

where C1(i,j) and C2(i,j) are the original and cipher image respectively.

e. Universal Image Quality Index (UIQ)

Universal index quality is used for calculating similarity between original image and cipher image. Range of UIQ is [-1,1] where value 1 indicates more similarity and value -1 indicates less similarity. UIQ is defined as in [32].

$$UQI(x,y) = \frac{\sigma xy}{\sigma x \sigma y} * \frac{2\mu x \mu y}{\mu x^2 + \mu y^2} * \frac{2\sigma x \sigma y}{\sigma x^2 + \sigma y^2} (7)$$

f. Structural Similarity Index Measure (SSIM)

The SSIM is the extended version of the UIQ index. Range of SSIM is [-1,1] where value 1 indicates more similarity and value -1 indicates less similarity. SSIM is defined as in [32]

$$SSIM(x,y) = \left[\frac{(2\mu x \mu\, y + C1) \quad (2\sigma xy + C2)}{(\mu x^2 + \mu y^2 + C1) \quad (\sigma x^2 + \sigma y^2 + C2)} \right] (8)$$

Where C1, C2 are two constants and are used to stabilize the division with weak denominator.

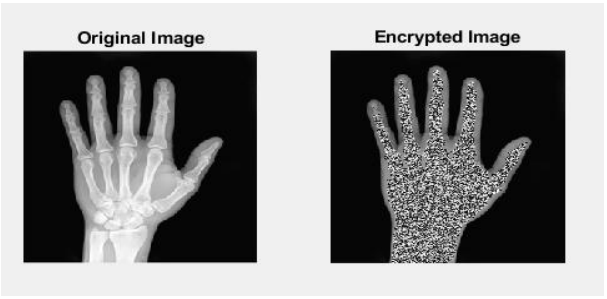

Figure 4: Input Hand image and Corresponding ROI encrypted Hand image

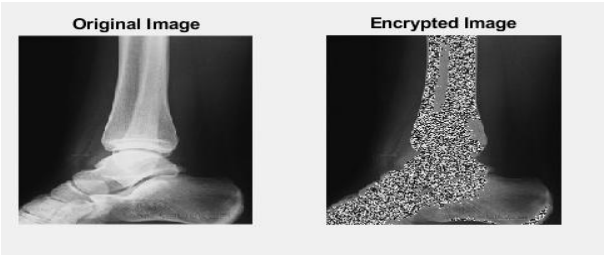

Figure 5: Input Leg image and Corresponding ROI encrypted Leg image

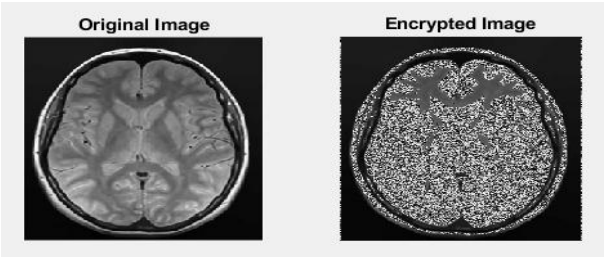

Figure 6: Input MRI image and Corresponding ROI encrypted MRI image

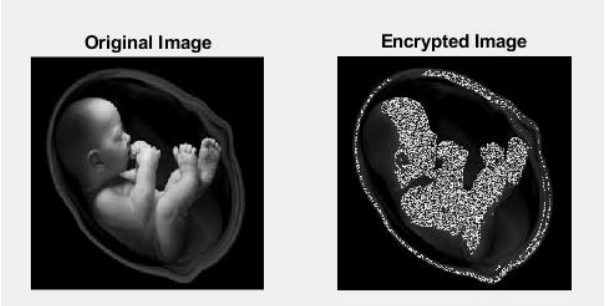

Figure 7: Input Fetus image and Corresponding ROI encrypted Fetus image

Table 1: Performance parameters for proposed ROI encrypted system

Image Name	Entropy_In (Bit)	Entropy	MSE	PSNR(db)	NPCR (%)	UACI (%)	UQI	SSIM
Baby	4.9216	6.4233	46.1371	23.9582	47.8984	26.6886	0.6060	0.4654
MRI	4.5597	5.9973	53.7087	42.8534	44.0204	19.6988	0.6826	0.4718
Hand	4.4401	6.0011	76.6292	59.8942	49.0779	25.1082	0.7421	0.4208
Foot	3.7644	5.0888	89.1270	72.2060	46.9583	30.6299	0.8139	0.5437

Table 2: Efficiency of proposed ROI encrypted system

Image Name	Encryption Time (sec)	Time (%) Saving compared to full image encryption
Baby	0.171694	44.7969
MRI	0.17435	45.6094
Hand	0.15953	46.6563
Foot	0.198069	39.5000

From Table 1, we conclude that the entropy value of the encrypted image is higher than the entropy value of the original simple image. The MSE score is incremented based on the image showing the level of encryption. With selective encryption, the NPCR values of the proposed method do not change significantly, the computational cost and time are reduced, and the similarity index measurements are reduced to zero. That is, the lower the value, the higher the dissimilarity between them. Input image and encrypted ROI image. Table 2 shows the efficiency of the proposed method in terms of execution speed and cost. Compared to full-frame encryption, this method saves about 50% of the computational cost and provides fast execution time for encrypting images. Analyzing the entropy values of the various medical images in Table 1 reveals the high entropy of the new cryptographic algorithms. The theoretical value is 8, and the above analysis shows that the entropy value of the encrypted image is close to the theoretical value, indicating that the encrypted image is highly random.

The SSIM value between the original image and the encrypted image should be as small as possible. This shows the effectiveness of the encryption algorithm. Table 1 calculated the SSIM values between the final encrypted medical image and the original medical image. Obviously, our method yields a smaller SSIM value. From Table 2, we can see that the encryption time for various medical images has been reduced. This is achieved because it performs selective encryption of the image rather than fully encrypting it, and because it is a lightweight encryption technology, it takes less time to perform bit plane encryption.

Table 3: Parameters comparison with existing method for MRI Image

Parameters	Proposed Method	Existing Method[30]
MSE	53.7087	86.2657
PSNR	42.8534	10.0881
NPCR	44.0204	0.5147
UACI	19.6988	12.4579
SSIM	0.4718	0.4620
Encryption Time	0.17435	72.50

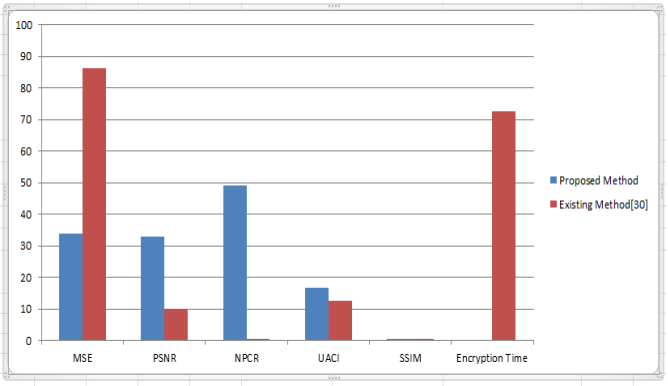

Figure 8: Graphical analysis of parameters comparison with existing method [30]

Our method significantly reduces encryption time, guarantees the reliability of images sent to the cloud, and guarantees security with a two-level encryption scheme. To verify the validity of the selective encryption scheme, calculate various parameters such as NPCR, MSE, PSNR, SSIM, encryption time and compare those values with the values obtained using existing methods. Table 3 shows that selective encryption schemes are an effective method because they give better results compared to existing methods.

6. CONCLUSION

In this article, we have proposed a method for partially encrypting personal information such as tumors and fetal parts. Traditional image protection technologies have problems such as padding and increased data volume due to wasted storage space over time. Also, because the entire image is encrypted, the image cannot be recognized before decryption and sensitive information is disclosed after decryption. Conventional sub-picture encryption has the problem that unnecessary parts are encrypted by encrypting a rectangular area that covers information that requires confidentiality. The proposed method solves this problem. The proposed method has detected the significant pixels using histogram peak detection method and encrypts it using Sudoku matrix. In this study, we measure the encryption speed of the proposed method and determine the most suitable block unit for encryption in order to improve the encoding and decoding speed of the image part.

7. REFERENCES

[1] Satoh H, Niki N, Eguchi K, Ohmatsu H, Kusumoto M, Kaneko M, Moriyama N. Teleradiology network system on cloud using the web medical image conference system with a new information security solution. In: SPIE medical imaging, vol. 8674. Lake Buena Vista (Orlando Area): SPIE; 2013.

[2] Avudaiappan T, Balasubramanian R, Pandiyan SS, Saravanan M, Lakshmanaprabu SK, Shankar K. Medical image security using dual encryption with oppositional based optimization algorithm. J Med Syst. 2018;42(11):208.

[3] Wang C, Wang X, Xia Z, Zhang C. Ternary radial harmonic Fourier moments based robust stereo image zero-watermarking algorithm. Inf Sci. 2019;470:109–20.

[4] Xie, Dong. "Public Key Image Encryption Based on Compressed Sensing." IEEE Access 7 (2019): 131672-131680.

[5] Zhu, Shuqin, and Congxu Zhu. "Plaintext-Related Image Encryption Algorithm Based on Block Structure and Five-Dimensional Chaotic Map." IEEE Access 7 (2019): 147106-147118.

[6] Binjubeir, Mohammed, et al. "Comprehensive survey on big data privacy protection." IEEE Access 8 (2019): 20067-20079.

[7] Li, Ming, et al. "Cryptanalysis of a Novel Bit-Level Color Image Encryption Using Improved 1D Chaotic Map." IEEE Access 7 (2019): 145798-145806.

[8] Manjula and Mohan H S, "Probability based selective encryption scheme for fast encryption of medical images." (2019). SJBIT.

[9] Jang, Wonyoung, and Sun-Young Lee. "Partial image encryption using format-preserving encryption in image processing systems for Internet of things environment." International Journal of Distributed Sensor Networks 16.3 (2020): 1550147720914779.

[10] Sankaradass, Veeramalai, P. Murali, and M. Tholkapiyan. "Region of Interest (ROI) based image encryption with sine map and lorenz system." International Conference on ISMAC in Computational Vision and Bio-Engineering. Springer, Cham, 2018.

[11] Mousavi, SeyedMojtaba, AlirezaNaghsh, and S. A. R. Abu-Bakar. "A heuristic automatic and robust ROI detection method for medical image warermarking." Journal of digital imaging 28.4 (2015): 417-427.

[12] Zhou, Jian, Jinqing Li, and Xiaoqiang Di. "A Novel Lossless Medical Image Encryption Scheme Based on Game Theory With Optimized ROI Parameters and Hidden ROI Position." IEEE Access 8 (2020): 122210-122228.

[13] Kiran , Rashmi P, Dr. Supriya M C "Encryption of Color image to enhance security using Permutation and Diffusion Techniques", International Journal of Advanced Science and Technology Vol. 28, No. 12, (2019), pp. 375-384.

[14] Zhicheng N, Yun-Qing S, Ansari N, Wei S. Reversible data hiding. IEEE Trans Circuits Syst Video Technol. 2006;16(3):354–62.

[15] Kumar CV, Natarajan V, Bhogadi D. High capacity reversible data hiding based on histogram shifting for medical images. In: 2013 international conference on communication and signal processing: 3–5 April 2013; Tamilnadu; 2013, p. 730–3.

[16] Yang Y, Zhang W, Yu N. Improving visual quality of reversible data hiding in medical image with texture area contrast enhancement. In: 2015 international conference on intelligent information hiding and multimedia signal processing (IIH-MSP): 23–25 Sept 2015; Adelaide; 2015. p. 81–4.

[17] Wu M, Zhao J, Chen B, Zhang Y, Yu Y, Cheng J. Reversible data hiding based on medical image systems by means of histogram strategy. In: 2018 3rd international conference on information systems engineering (ICISE): 4–6 May 2018; Shanghai; 2018. p. 6–9.

[18] Huang L-C, Tseng L-Y, Hwang M-S. A reversible data hiding method by histogram shifting in high quality medical images. J SystSoftw. 2013;86(3):716–27.

[19] Yue XD, Miao DQ, Zhang N, Cao LB, Wu Q (2012) Multiscale roughness measure for color image segmentation. InfSci 216(24):93–112

[20] Sastry SS, Mallika K, Rao BGS, Tiong HS, Lakshminarayana S (2012) Liquid crystal textural analysis based on histogram homogeneity and peak detection algorithm. LiqCryst 39(4): 415–418

[21] Boukharouba S, Rebordao JM, Wendel PL (1984) An amplitude segmentation method based on the distribution function of an image. Comput Vis Graph Image Process 29(1):47–59

[22] Elguebaly T, Bouguila N (2011) Bayesian learning of finite generalized gaussian mixture models on images. Sig Process 91(4):801–820.

[23] Azam M, Bouguila N (2015) Unsupervised keyword spotting using bounded generalized Gaussian mixture model with ICA. In: IEEE global conference on signal and information processing, pp 1150–1154.

[24] Nguyen TM, Wu QMJ, Zhang H (2014) Bounded generalized Gaussian mixture model. Pattern Recogn 47(9):3132–3142.

[25] P. Rashmi, M. C. Supriya, Qiaozhi Hua, "Enhanced Lorenz-Chaotic Encryption Method for Partial Medical Image Encryption and Data Hiding in Big Data Healthcare", Security and Communication Networks, vol. 2022, Article ID 9363377, 9 pages, 2022. https://doi.org/10.1155/2022/9363377.

[26] Rashmi . P, Supriya. M C and K. Kiran, "Image Encryption Algorithm based on 2D Hyper Chaotic Map and Trigonometric Functions", 2021 IEEE International Conference on Mobile Networks and Wireless Communications (ICMNWC), 2021, pp. 1-4. doi: 10.1109/ICMNWC52512.2021.9688349.

[27] Rashmi P, Supriya M C, Building Enhanced Chaotic Map Encryption Method for Medical Information System, Journal of System and Management Sciences,

Vol. 11 (2021) No. 1, pp. 176-192, DOI:10.33168/JSMS.2021.0111

[28] ArwaBenlashram, Maryam Al-Ghamdi, RawanAlTalhi and Pr. KaoutherLaabidi, "A novel approach of image encryption using pixel shuffling and 3D chaotic map", Journal of Physics: Conference Series 1447 (2020) 012009. 10.1088/1742-6596/1447/1/012009.

[29] Jawad Ahmad and Fawad Ahmed. Efficiency analysis and security evaluation of image encryption schemes. computing, 23:25, 2012.

[30] XuncaiZhang ,Lingfei Wang , Guangzhao Cui , and Ying Niu, "Entropy-Based Block Scrambling Image Encryption Using DES Structure and Chaotic Systems" Hindawi International Journal of Optics, Volume 2019, Article ID 3594534, 13 pages https://doi.org/10.1155/2019/3594534.

[31] Yue Wu, Joseph P Noonan, and SosAgaian. Npcr and uaci randomness tests for image encryption. Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT), pp 31-38, 2011.

[32] Zhou Wang, Alan C Bovik, Hamid R Sheikh, and Eero P Simoncelli. Image quality assessment: from error visibility to structural similarity. IEEE transactions on image processing, 13(4):600-612, 2004.

[33] ZhouWang and Alan C Bovik. Modern image quality assessment. Synthesis Lectures on Image, Video, and Multimedia Processing, 2(1):1-156, 2006.

[34] Sajjad M, Muhammad K, Baik SW, Rho S, Jan Z, Yeo SS, Mehmood I (2017) Mobile-cloud assistedframework for selective encryption of medical images with steganography for resource-constrained devices. Multimed Tools Appl 76(3):3519–3536.