Analysis and Computation of Encryption Technique to Enhance Security of Medical Images

Kiran1,2, Parameshachari BD3, Panduranga HT4 and Silvia liberata Ullo5

1VTU, Belagaum, India.  
2Department of ECE, Vidyavardhaka College of Engineering, Mysuru, India.  
3Department of TCE, GSSSIETW, Mysuru, India.  
4Department of ECE, Govt. Polytechnic, Turvekere, Tumkur, India.  
5Engineering Department, University of Sannio, Italy.  
1,2kiran.mtech12@gmail.com, 3parameshbkit@gmail.com, 5silvullo@unisannio.it

Abstract. Recently, there are many advanced techniques used in the medical fields, such as smart health, e-health and telemedicine applications. These techniques rely on open source networks to transmit the digital medical images. These images have very sensitive and confidential information about the patients. Regrettably, most of the regularly used algorithms provide very less security and present a high communication overhead, with high computation costs. Due to these issues, a Region of Interest (ROI) method, based on selective image encryption, is proposed in this paper. An active contour image segmentation is first used to divide the ROI and the Region of Background (ROB). Then, a Hilbert curve, with a Skew Tent map are used to implement the Permutation and diffusion techniques. Namely, the ROI part is permuted according to a Hilbert scan pattern, to decrease the similarities between the inside adjacent pixels. Then pixels in the permuted ROI part are XOR pixel-wise with random numbers, generated based on a predefined threshold value from a Skew Tent map. Finally, encrypted ROI and ROB blocks are combined to generate encrypted images. Given the obtained experimental results, the proposed method is very likely to improve image security, through the employment of correlation checking, key sensitivity, entropy, diffusion characteristic and histogram tools.

1. Introduction

In time critical applications such as internet banking, medical imaging, pay TV, military communication, confidential video conference, satellite security, corporate communication, etc. where the security is utmost important, the selective image encryption plays a vital role. Advanced Encryption Standard [AES] and Triple Data Encryption Standard [DES] are the strong encryption techniques used to secure the images from unauthorized access. The process of encrypting the whole image is a tedious process using these techniques. Partial/Selective Encryption [PE/SE] is the process of encrypting the selected portions from the input image. This process decreases the encrypting and decrypting time. It also increases the robustness of the image.

Zhijuan Deng and Shaojun Zhong [1] introduced a chaotic mapping based digital image encryption algorithm. In this algorithm the number of iterations used is reduced and the cryptographic space is highly expanded by this algorithm. Akram belazi muhammad Talha et.al [2] explained a new method for encryption for medical images based on chaos, it is the combination of both DNA and chaos, it has two encryption rounds, after which the key generation layer is done. Hossein [3] described image
security algorithm where image encryption is classified into bit-level and pixel-level. Histogram of the image can be changed by bit-level permutation, because it is bit-level computing it is time consuming. M bin younas and Jawad ahmad [4] presented a new technique in wavelet transform domain that is fusion technique. Here the components of high and low frequencies are merged to get improved image content. Four asymmetric keys are generated with respect to each image. Aqeel ur rehman et.al [5] presented two major technologies. They have tested and estimated the scheme of encryption of image using different parameters. This method will more efficient than the previous methods. Lisungu oteko tresor et.al [6] described a new technique for image encryption. This method is suitable only for gray scale images. The speed will be more but the method is restricted only to gray scale images. Ping et.al [7] described a new method known as digit-level permutation, the image is divided and converted into a matrix form, this pixel matrix is decomposed into three digital matrices. Using Henon map this pixel will be shuffled, pixel level permutation is combined with bit level permutation by digit-level permutation. High-speed diffusion operation will be designed. Tresor Oteko Lisungu et.al [8] explained about development of new encryption scheme, where in this method the characteristics of image is changed and compressed. This increases the complexity and makes this method more efficient. Martin Rieger and Andreas Uhl [9] introduced image encryption technique which is restricted to JPEG2000. Uses of this method makes it more efficient and it be used widely for many applications. The security and speed of this method will also increase and give good performance. Xingbin liu and cong liu [10] explained a technique which is used to encrypt image and restricted only for gray images. It considers pixel gray value and information about image blocks position. This scheme is reliable and the security of image is good. Dong xie [11] describe simple method to manipulate image by using matrix multiplication. Crypto system provides great security to the information where it will be hard to crack this image. Hence, this makes it more efficient. Shuqin zhu and congxu zhu [12] explained about 5-D hyper-chaotic map, which is designed by merging 3D Lorenz and logistic map. This scheme includes two types of operations. where in the 1st method which is only related to the pixels of clear text images and the 2nd method undergoes 2 rounds of diffusion and this paper says that theoretical and experimental results ensures the security. Mohammed [13] to overcome the security problem, introduced the privacy preserving data mining. Currently the web users are sharing their confidential data or tasks without risk. Ming li et.al [14] it shows that the newly introduced scheme has higher security due to the improvisation of the 1D chaotic map along with higher performance. They have found few loophole problems in this technique and then they introduced a new attack strategy which uses chosen plain text attack. The newly introduced methods are verified theoretically and practically. Various chaos based encryption techniques were discussed using different methods [15-18, 30]. Dr. Parameshachari B D et.al [19-20] explained about side management and optimization methods in the secure communication system.

The remaining paper is organized as follows: In section II, active contour, Hilbert scan and skew tent maps are briefly explained. Section III shows the proposed ROI based encryption scheme. The experimental analysis and security are presented in section IV and we conclude the paper in Section V.

2. Related Work

2.1 Active Contour Method

For many applications such as motion tracking and image segmentation over the last decade the active contour is the most popularly used method. The deformable contours are used to match the motions and various shapes of the objects. Here we explain how the active contours are set theoretically and also information about the present methods of active contour. Mathematical implementation based approaches: Snakes and setting the levels are used in active contours. Using Energy minimization method, the pre-defined snake points are explicitly shifted by the snakes. The level set approach moves the contour as a function of a particular level completely. Based on the force evolving contours, there are two active contour models in image segmentation: Edge based and region based. Edge detector which uses the image gradient is used in the active contours based on Edge to find the sub-regions boundaries and also to draw the detected boundaries contours. Edge based segmentation is almost similar to the Edge based approach. Instead of searching for geometrical boundaries, the statistical information of image intensity inside each subset is applied in Region based active contours approach. Region based segmentation is almost similar to the region based approach [21-22].
2.2 Hilbert Scan Pattern

Overall, $2^m \times 2^m$ array of points are scanned using Hilbert curve. In a square grid the scan path can be started either from left bottom (LB), left top (LT), right bottom (RB) or right top (RT) [23]. Here the scrambled is obtained by Hilbert curve which shuffles the pixels position in the original image.

The order 0 of the Hilbert Curve is always empty. With the help of three straight line connectors along with four zero order curves, the first order Hilbert curve is obtained. All other higher order curves are obtained similarly. Hilbert curve of order 1, 2, 3 and 4 corresponding to are shown in Fig. 1(a), (b), (c) and (d) shows the first, second, third and fourth order Hilbert curves which corresponds to square grids of $2 \times 2$, $4 \times 4$, $8 \times 8$, $16 \times 16$.

![Hilbert curve of order 1, 2, 3, 4 corresponding to 2x2, 4x4, 8x8, 16x16 square grids](image1.png)

**Figure 1.** Hilbert curve of order 1, 2, 3, 4 corresponding to 2x2, 4x4, 8x8, 16x16 square grids respectively

2.3 Skew Tent Map

The skew tent map is one of the popular chaotic maps which is dynamic, simple, nonlinear equation along with a complex chaotic behaviour, is as shown below [24]:

![8x8 matrix permutation using Hilbert scan pattern](image2.png)

**Figure 2.** 8x8 matrix permutation using Hilbert scan pattern

The skew tent map is one of the popular chaotic maps which is dynamic, simple, nonlinear equation along with a complex chaotic behaviour, is as shown below [24]:
Where $X_{n+1}$ is the chaotic system state, $b \in [0,0.5] \cup [0.5,1]$ is a control parameter, and $X_n \in [0,1]$ where $n$ is iteration number which generates iterative values.

3. Proposed Technique

Architecture of proposed ROI based advanced encryption scheme is as shown in Figure 2. Throughout this paper, $P \times Q$ represents the size of a medical image. The plain text image pixel value at location $i$th row and $j$th column is represented as $P(i,j)$. Three important steps are involved in the proposed scheme.

In first step, ROI part of the original image is extracted using active contour method, whereas in the second step, the Hilbert scan pattern employed to change the location of every pixels in the ROI part.

In the last step, for diffusion purposes, skew tent map are utilized to get a random matrix $R$. More details regarding these steps are as mentioned below:

**Step 1:**

i) The original medical image of size $P \times Q$ is undergo active contour based image segmentation to extract ROI and ROB binary image.

ii) Then ROI part is obtained from multiply original medical image and ROI binary image and size of ROI is $M \times N$.

$$ROI\_Part = \text{Original Medical image} \times \text{ROI binary image}$$

**Step 2:**

iii) Starting from the right bottom (RB) position we have to construct a $N$th order Hilbert curve. For eg. Fig 2(a) gives the third order Hilbert curve which starts from right bottom (RB) cell in $(8 \times 8)$ square grid. Fig 3(b) gives the scan coordinates of this operation.

iv) The pixels of the original image are scrambled based on this scan pattern.

**Step 3:**

v) Initial condition for Sine is set i.e., $b=0.2838$ and $X_0 = 0.73846$.

vi) Iterate the Equation 1 $M \times N$ times to obtain random vector $X$.

vii) Update the random vector $X$ by multiplying it with $10^{14}$.

viii) To obtain a new random number within the range (0-255), Modulo 256 operation is used.

$$\alpha = \text{Modulo}(X, 256)$$

(ix) To get the matrix $R$ we have to arrange the new random finite precision vector $\alpha$ in a matrix form.

x) The ROI block pixels are XORed bitwise with matrix $R$.

$$\text{Diff\_Block} = \text{bitxor (ROI, R)}$$

where Diff\_Block is the diffused block.

xi) At last combined diffused ROI block and ROB block to form encrypted image.
4. Performance Analysis of Proposed Scheme
The overall performance of the proposed scheme is analysed with the help of different parameters. The following parameters are involved as follows.

4.1 Histogram Analysis
Based on the intensity levels, the graphical representation of pixel distribution is the histogram of an image. A good encryption algorithm for any plain image will generate a cipher image of the uniform histogram. Table 4 gives the various original medical images histograms and their respective cipher images. The histogram of an encrypted image is almost close to uniform distribution.

4.2 Entropy Analysis
Entropy is a measure of degree of randomness in the encryption system. Entropy is calculated using the formula [26]:

$$H(S) = \sum_{i=0}^{M-1} P(s_i) \log_2 \frac{1}{P(s_i)}$$  \hspace{1cm} (5)

Where $P(s_i)$ represents the occurrence probability of the $i^{th}$ gray level in an image. The ideal value of entropy is 8 for random image. If it is less , the chance of predictability is more. Table 1 shows entropy of some sample images along with their respective cipher images.

4.3 Mean Square Error (MSE)
Generally MSE is analysed between plain image and cipher image by taking mean of the squared difference between them. More value of MSE leads to higher encryption and more noise in the plain

---

**Figure 3.** Architecture of proposed ROI based selective image encryption

---

**Table 4**
| Original Medical Image | Cipher Image |
|------------------------|--------------|
|                        |              |

---

**Table 1**
| Sample Images | Entropy |
|---------------|---------|
|               |         |
image. Let $I_1$ represents plain image where $E_1$ denotes cipher image after encryption operation. Mathematical equation for $MSE$ [26] given by.

$$MSE = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} [X(i, j) - Y(i, j)]^2$$  \hspace{1cm} (6)

4.4 Peak Signal to Noise Ratio (PSNR)

Peak signal-to noise ratio which is always opposite to Mean Square Error (MSE). Cipher image quality generally measured by PSNR quantity. For good security of image, more $MSE$ and Less PSNR. Mathematically $PSNR$ is given as below [26].

$$PSNR = 10 \log_{10} \frac{255}{MSE}$$  \hspace{1cm} (7)

4.5 UACI and NPCR

The sensitivity of proposed encryption technique with respect to secret key and plain image can be checked using two tests. Namely: Unified average changing intensity (UACI) and Number of pixels change rate (NPCR) [25]. The equation 4 is used to calculate UACI.

$$UACI = \frac{1}{N} \left[ \sum_{i,j} |C_1(i,j) - C_2(i,j)| \right] \frac{255}{255}$$ \hspace{1cm} (8)

where, ‘m’ indicates No. of rows, ‘n’ represents No. of columns. $C_1(i,j)$ represents original image and $C_2(i,j)$ represents cipher image. Equation 5 shows the calculation of NPCR.

$$NPCR = \frac{\sum_{i,j} D(i,j)}{MN} \times 100\%$$ \hspace{1cm} (9)

where, ‘M’ indicates No. of rows, ‘N’ represents No. of columns and $D(i,j)$ is defined as follows

$$D(i,j) = \begin{cases} 1, & C_1(i,j) \neq C_2(i,j) \\ 0, & \text{otherwise} \end{cases}$$

where $C_1(i,j)$ and $C_2(i,j)$ are Original image and Cipher image respectively.

**Table 1.** Performance parameters for proposed ROI encrypted system

| Image Name | Entropy_In (Bit) | Entropy_Enc(Bit) | MSE     | PSNR(db) | NPCR(%) | UACI(%) |
|------------|------------------|------------------|---------|----------|---------|---------|
| Baby       | 2.6682           | 3.2067           | 5.6701  | 40.5949  | 29.6270 | 12.3073 |
| Baby Womb  | 3.5540           | 6.8615           | 34.9602 | 32.6951  | 75.8653 | 32.0196 |
| MRI        | 4.5016           | 4.7368           | 36.2388 | 32.5391  | 47.5328 | 15.5345 |
| Hand       | 4.1229           | 4.3455           | 57.6363 | 30.5238  | 36.2294 | 11.7870 |
| Foot       | 3.7588           | 3.8080           | 37.8616 | 32.3488  | 28.6262 | 8.1099  |
Table 2. Efficiency of proposed ROI encrypted system

| Image Name | Image Size  | Encryption Time (sec) | Time (%) Saving compared to full image encryption |
|------------|-------------|-----------------------|-------------------------------------------------|
| Baby       | 761*1024    | 4.74                  | 70.38                                           |
| Baby Womb  | 72*1280     | 5.31                  | 34.14                                           |
| MRI        | 720*960     | 4.26                  | 52.47                                           |
| Hand       | 881*750     | 3.39                  | 73.78                                           |
| Foot       | 750*297     | 2.70                  | 71.38                                           |

Table 3. Timing analysis comparison for existing methods

| Image Name | Image Size  | Proposed Method | Jan Sher Khan et al. (2019)[29] | Ayoup et al. (2015) [28] | Ullah et al. (2013)[27] |
|------------|-------------|-----------------|-------------------------------|--------------------------|--------------------------|
| Gray image | 256*256     | 0.43 sec        | 0.55 sec                      | 7.21 sec                 | 3.12 sec                 |

Table 4. Histogram analysis of proposed ROI Encryption system

| Medical Image | Histogram | Encrypted Image | Histogram |
|---------------|-----------|-----------------|-----------|
| ![Image](image1.png) | ![Histogram](histogram1.png) | ![Encrypted Image](encrypted1.png) | ![Histogram](histogram2.png) |
| ![Image](image2.png) | ![Histogram](histogram3.png) | ![Encrypted Image](encrypted2.png) | ![Histogram](histogram4.png) |
| ![Image](image3.png) | ![Histogram](histogram5.png) | ![Encrypted Image](encrypted3.png) | ![Histogram](histogram6.png) |
4.6 Time analysis
Matlab 2019b is used to test the proposed scheme on gray medical images of various sizes with the system configuration having Intel Core i5 CPU @ 2.53 GHz and 4.0 GB RAM on Windows 10 OS. The encryption time is much lower in the proposed scheme than the other three regularly used encryption techniques; the same can be seen in Table 3 ((25-27)). The proposed encryption technique is a single round image encryption technique which is used for real time, online communication.

From the table 1 we concluded that entropy values of cipher images are more than original plain image. MSE values are increases according to different image that will give the amount of encryption. Because of selective encryption proposed method NPCR values is not much varied that indicates that reduction in computation cost and time.

Table 2 gives the efficiency of proposed method in-terms of execution speed and cost. Compared full image encryption this method saves 70% of computational cost and achieves fast execution time to encrypt image.

5. Conclusion
In this paper, we presented a ROI based selective image cryptographic system to encrypt only ROI part from medical image using the concepts of Hilbert scan and Skew Tent map. Proposed scheme can encrypt any medical image in an effective manner with limited resource utilization and better security. Through active contour method ROI part is extracted. Then ROI part is permuted using Hilbert scan pattern and diffused using skew tent map with predefined threshold values. We can conclude that the proposed technique can be used in real time medical image encryption with limited resource utilization based on the security analysis of the proposed encryption technique.

Acknowledgement
This work is supported by VTU Belagaum, Karnataka and Electronics and communication Research centre, GSSSIETW, Mysuru, Karnataka

References
[1] Zhijuan D and Zhong S 2019 A digital image encryption algorithm based on chaotic mapping Journal of Algorithms & Computational Technology 13 1748302619853470.
[2] Belazi A, Talha M, Kharbech S and Xiang W 2019 Novel medical image encryption scheme based on chaos and DNA encoding IEEE Access 7 36667-36681
[3] Ghadirli HM, Nodehi A, Enayatifar R 2019 An overview of encryption algorithms in color images Signal Processing 164 163-85
[4] Younas MB, Ahmad J 2014 Comparative analysis of chaotic and non-chaotic image encryption schemes Int. Conf. on Emerging Technologies (ICET) 81-86

[5] Rehman AU, Wang H, Shahid MM, Iqbal S, Abbas Z, Firdous A 2019 A Selective Cross-Substitution Technique for Encrypting Color Images Using Chaos, DNA Rules and SHA-512 IEEE Access 7 162786-802

[6] Tresor LO, Sumbwanayambe M 2019 A Selective Image Encryption Scheme Based on 2D DWT, Henon Map and 4D Qi Hyper-Chaos IEEE Access 7 103463-72

[7] Ping P, Fan J, Mao Y, Xu F, Gao J 2018 A chaos based image encryption scheme using digit-level permutation and block diffusion IEEE Access 6 67581-93

[8] Lisungu TO, Sumbwanayambe M 2019 Image Compression-Encryption Scheme Based on 2D DWT, SPIHT and Qi Hyper-chaos Southern African Universities Power Engineering Conference/Robotics and Mechatronics/Pattern Recognition Association of South Africa (SAUPEC/RobMech/PRASA) 177-182

[9] Rieger M, Hämmerle-Uhl J, Uhl A 2019 Selective JPEG2000 Encryption of Iris Data: Protecting Sample Data vs. Normalised Texture IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) 2602-2606

[10] Liu X, Xiao D, Huang W, Liu C 2019 Quantum block image encryption based on arnold transform and sine chaotification model IEEE Access 7 57188-99

[11] Xie D 2019 Public Key Image Encryption Based on Compressed Sensing IEEE Access 7 (2019): 131672-131680

[12] Zhu S, Zhu C 2019 Plaintext-related image encryption algorithm based on block structure and five-dimensional chaotic map IEEE Access 7 147106-18

[13] Binjubeir M, Ahmed AA, Ismail MA, Sadiq AS, Khan MK 2019 Comprehensive survey on big data privacy protection IEEE Access 8 20067-79

[14] Li M, Wang P, Liu Y, Fan H 2019 Cryptanalysis of a Novel Bit-Level Color Image Encryption Using Improved 1D Chaotic Map IEEE Access 7 145798-806

[15] Kiran, Parameshachari BD, Sahana VS, Apoorva C, Thanuja BS 2018 Auto-Blocking based Image Encryption using ECG Signal IJCA Proceedings on National Conference on Electronics, Signals and Communication NCESC 2017 33-35

[16] Parameshachari BD, Panduranga HT, Naveen kumar SK 2017 Partial encryption of medical images by dual DNA addition using DNA encoding International conference on recent innovations in signal processing and embedded systems (RISE) 310-314

[17] Parameshachari BD, Kiran, Rashmi P, Supriya MC, Rajashekarappa, Panduranga HT 2019 Controlled partial image encryption based on LSIC and chaotic map ICCSP 60-63

[18] Kiran, Rashmi P and Supriya M C 2019 Encryption of Color image to enhance security using Permutation and Diffusion Techniques International Journal of Advanced Science and Technology 28 375-384

[19] Subramani P, Rajendran GB, Sengupta J, Pérez de Prado R and Divakarachari PB 2020 A Block Bi-Diagonalization-Based Pre-Coding for Indoor Multiple-Input-Multiple-Output-Visible Light Communication System Energies 13 3466

[20] Puttamadappa C and Parameshachari BD 2019 Demand side management of small scale loads in a smart grid using glow-worm swarm optimization technique Microprocessors and Microsystems 71 102886

[21] Chan TF and Vese LA 2001 Active contours without edges IEEE Transactions on image processing 10 266-77

[22] Caselles V, Kimmel R, Sapiro G 1997 Geodesic active contours International journal of computer vision 22 61-79

[23] Sivakumar T and Venkatesan R 2014 Image encryption based on pixel shuffling and random key stream Int. J. Comput. Inform. Technol. 3

[24] Kadir A, Hamdulla A, Guo WQ 2014 Color image encryption using skew tent map and hyper chaotic system of 6th-order CNN Optik. 125 1671-5

[25] Wu Y, Noonan JP and Agaian S 2011 NPCR and UACI randomness tests for image encryption. Cyber journals: multidisciplinary journals in science and technology Journal of Selected Areas in Telecommunications (JSAT) 1 31-8
[26] Ahmad J and Ahmed F 2010 Efficiency analysis and security evaluation of image encryption schemes *Computing* \textbf{23} 25.

[27] Ullah I, Iqbal W and Masood A 2013 Selective region based images encryption \textit{2\textsuperscript{nd} National conference on information assurance (NCIA)} 125-128

[28] Ayoup AM, Hussein AH and Attia MA 2015 Efficient selective image encryption *Multimedia tools and applications* 1–16

[29] Khan JS, Ahmad J 2019 Chaos based efficient selective image encryption *Multidim Syst Sign Process* \textbf{30} 943–961

[30] Ramesh GP and Kumar NM 2018 Radiometric analysis of ankle edema via RZF antenna for biomedical applications *Wireless Personal Communications* \textbf{102} 1785-1798