BBRC
Bioscience Biotechnology
Research Communications

Steganography in Medical Images Using Advanced Reversible Data Hiding Scheme Based Encryption System

B.Chitradevi[1] and S.Manikandan[2]

[1]*Research & Development, Periyar University, Salem.*

[2]*Department of Information Technology, K.Ramakrishnan College of Engineering, Trichy.*

ABSTRACT

With the advancement of computer as well as biomedical equipment, medical images encompass the patients' private data also the safety of the private data entices excessive care. Reversible data hidden in encrypted medical images fascinated care from data secrecy also security communities. The sensitive and secret information of patients is passed through a number of a network to reach a particular point. To transfer them securely, there are many mechanisms available. However, the middlemen present in the system is capable of reading the secret information and can perform any malicious activity. To safeguard the information, the key based methods are used in the area, but not suitable because of the higher readability. By capturing the data, the malicious user can perform any guessing attack and could obtain the original information. Steganography is employed to hide the secret data, so as to provide privacy protection of patient data in medical images. Reversible Data Hiding (RDH) is a method to reverse the marked media (Image, audio and video) back to the original cover media once the hidden information were mined. In this research, data hiding methods were implemented also outcomes are compared. Experimental results illustrates that the proposed system can and perform superior than the other steganography methods.

KEY WORDS: STEGANOGRAPHY, REVISABLE DATA HIDING, MEDICAL IMAGES, DATA EMBEDDING, ENCRYPTION, DECRYPTION.

INTRODUCTION

Digital medical imaging system have grown increasingly major in recent days with the fast development of the biomedical system. Medical information can be transferred appropriately over the networks for the purposes of various specialists' consultations. Meanwhile medical scan images cover the patients' private data, information also confidentiality security have become significant through communicating medical scan images over the Internet. Consequently, steganography is familiarized to afford security also confidentiality for medical images also it could create the patients' data untraceable (Thinn A. et al 2019).

ARTICLE INFORMATION

**Corresponding Author: citradevi.b@gmail.com*
Received 19th Oct 2020 Accepted after revision 29th Dec 2020
Print ISSN: 0974-6455 Online ISSN: 2321-4007 CODEN: BBRCBA

Thomson Reuters ISI Web of Science Clarivate Analytics USA and Crossref Indexed Journal

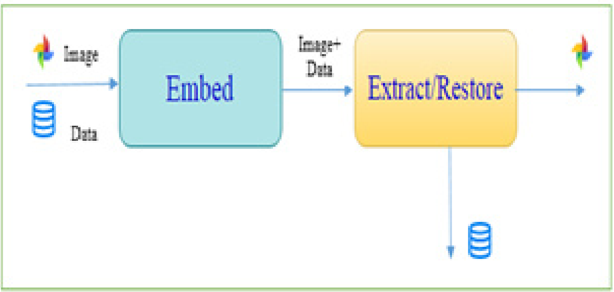
Clarivate Analytics   crossref

NAAS Journal Score 2020 (4.31)
A Society of Science and Nature Publication,
Bhopal India 2020. All rights reserved.
Online Contents Available at: http//www.bbrc.in/
Doi: http://dx.doi.org/10.21786/bbrc/13.13/41

Steganography is the skill of hiding a data it may be text, image or video within another media file [Parameshachari, B.D et al 2020], Prabu, S. et al 2019]. Digital steganography is the one type of data hiding methodology to offer concealed communication as well as authentication (Norouzi B et al 2014). The objective of steganography is to conceal a private data inside innocuous medium so that it is preposterous even to identify that there is a mystery message. The vehicle for information stowing away is additionally called as cover, cloud and transporter. [Prabu, S.et al 2020] RDH can regenerate the original digital image from the stego-image without any misrepresentation when the implanted secret message is exactly extracted. Digitization and data transmission have become increasingly evident characteristics in the rapid development of the economic society. However, the communication of complex data through an Internet channel rises the risk of interception. Thus many methods have been proposed to solve this problem. Data hiding plays a significant role in data (information) security (Kumari M et al 2017). For content authentication also perceptual directness, the principle thought of information stowing away is to hide the secret information into the cover medium and along these lines to try not to draw in the reflection of assaulters in the Internet channel.

Most of the penetrating services use multimedia contents for communication especially digital images e.g. medical, forensic, military, astronomic images containing sensitive and private information. These images need special care during transmission for security and maintaining image quality. The problem of data hiding is about how efficient the data hidden in the image could be retrieved in efficient manner. Encryption and data hiding are efficient methods for data hiding. Whereas the encryption methods translate plaintext into scrawled ciphertext. The data hiding techniques embed additional data into digital images that process is illustrated in the below figure,

Figure 1: Process of data hiding system



Various RDH techniques have been proposed in this research that can be classified into three types: Lossless Compression (LC) based techniques, Difference Expansion (DE) techniques and Histogram Modification (HM) techniques (Zahmoul R et al 2017). In practical aspect, many RDH techniques have emerged in recent years.

Literature Survey: To collect data on the study topic were searched in databases Web of Science and Scopus. Material for this study was 34 literature sources given in the bibliography. As methods the studies used a number of methods. Method bibliographic search-method of searching information sources (documents and publications), which have or may contain the desired information. The use of the method to ensure the quality of the work, as he allowed at the optimum time to obtain all the necessary information in the traditional information environment. This method was necessary for the authors to collect adequate information in modern conditions the rapid growth of the information environment of research and development.

In previous years, many RDH algorithms have been proposed. In general, which can be divided into 3 groups: Differential dilation (DE) based algorithms, histogram based shift algorithms, lossless and compression based algorithms, (Liu Hongjun et al 2011). Lossless compression algorithms based on lossless space compression for loss of privacy message, which are Less Significant Bits (LSBs) or quantization residuals (Patro K et al 2018). They can be used for image and watermarking authenticity, but their encryption capacity is limited. DE-based algorithms usually do not shift the neighboring pixel diversity to form a LSB and one additional bit is more secret bit to the vacuum LSB (Guan Zhi-Hong et al 2005 & Ye G, Wong KW et al 2012). HS-based algorithms first move the histogram bins for gray values or prediction errors (Patro K et al 2017) to generate free space also implant secret information in the permitted space.

Patro K et al, proposed RDH algorithm that divides the encrypted image into blocks and implants a clandestine bit into blocks by 3 LSBs in one half of the pixels flipped by the block. In this algorithm extracts secret files by a wave function utilized in spatial correlation of natural images. In order to reduce the bit error rate, in (Hailan Pan et al 2018) is designed a useful measuring block for complexity of adjacent pixels by considering the position.

The extraction of data from image decryption is extracted in (Sravanthi D et al 2019) to compress the encrypted image to make room for data hiding. Distributed source coding is utilized in (Ashraf Odeh et al 2015) to improve the embedding capacity of the RDH algorithm. However, their encryption disorganizes the spatial correlation of pixels, so it is difficult to free up space for data hiding. In another study, was used to preserve spatial redundancy and was used to adaptive block-level prediction-based errors in extended encrypted image blocks to hide secret bits using image permutation of block permutation behavior. Some researchers (Sliman Arrag et al 2013) proposed the concept of image preprocessing for data encryption before embedding.

Need For Preprocessing: In order to prepare the digital images for data transmission, a few preprocessing procedures must be applied to the images. First, a noise filtering methods can applied to remove unwanted noises present in the images. The purpose of the noise removal/ image filtering is to decrease the inconsistency of the confined mean throughout the image in order to use it as an approximately constant reference level. Normalization helps in changing the range or intensity of the unwanted pixels related to the artifacts or noises while increasing the characteristics of the digital images. It is done by changing the level of every image pixel hooked on a level comparative to the signal to local background ratio.

a. Standard Median (SM) filter: The SM filter is a nonlinear method called as median smoother which endeavors to expel motivation clamor by changing the luminance estimation of the inside pixel of the separating window with the middle of the luminance estimations of the pixels contained inside the window. Despite the fact that the middle channel is straightforward and gives a sensible commotion expulsion execution, it evacuates thin lines and hazy spots image points of interest even at low noise densities.

The best-known request insights filter is the median filter, which replaces the estimation of a pixel by the middle of the gray levels in the area of that pixel. The definition of median value is listed as follows, A group of numbers: x1, x_2... xn, arranged in order of size: $x_{i1} \leq x_{i2} \leq \leq x_{in}$.

$$Y = \text{Median}\{x_1, x_2 \ldots Xn\}$$

$$= \begin{cases} x_{i(n+1)/2} & ,n is odd \\ [x_{i(n/2)} + x_{i(n/2+1)}]/2 & ,n is even \end{cases}$$

Where Median {...} expressed the process of computing the median from the sequence {xn}, Y indicates this median. We called a neighborhood of a pixel's specific length in a sequence or shape in an image as a filtering window (R. Senthilnathan et al 2018)

The noisy value of an input image is restored by the center of the noise filter mask in the input image. The each pixels in the filter mask are graded in the imperative of their gray levels of input image pixel and the median value of the filter mask is stored to substitute the noisy value in the filter mask. The median filter output is illustrated with below equation,

$$g(x,y) = \text{med}\{f(x-i, y-j), i, j \in W\}$$

In the above Equation, f (x, y) and g(x, y) is the original input medical image and the output noiseless image, respectively. 'W' denotes a two-dimensional mask of the image, the size of the mask is n× n such as 3× 3, 5× 5, and so on. The median filter implementation of uneven inspiration scream is superior to the normal method execution. Before, steganography process all input digital images are preprocessed with this filter.

Methodology of Reversible Data: The reversible data hiding method consists of image encryption, data embedding and data extraction/image restoration. They are described as follows,

a. Image Encryption: While an encryption binary image can be compressed inexpensively for detection of infections of low-density parity check indices, the encrypted gray image lossless compression method is developed for the use of progressive decomposition and rate-compatible non-slotted turbo codes. Provided by the loss compression method, the encrypted grayscale image can be suppressed by effectively eliminating excessive coarse grain information with coefficients generated from the orthogonal transform. When COM compresses the information, the receiver can define the main info of the digital image through the returned coefficient value. The content owner uses the encryption key to produce the original compressed image of the encrypted image. On the Receive Tools page, the data embedded in the created space is taken from the encrypted image, which contains additional information retrieval for easy data hiding.

For LSB programs, even if the embedding only affects the data, deleting the encryption key has an effect similar to the original version. When the encryption and data hiding keys are used to embed additional data successfully retrieved then the digital image that can be effortlessly recovered by the spatial association used in the digital image (Zhaoxia Yin et al 2016).

b. Data Embedding: Some parameters are encoded into a small number of encrypted pixels, which are compressed to make additional data also the original data space is held by the embedded parameters at the occupied position in the data implanting stage. According to the data hiding key, a parameter NP-encrypted pixel for carrying data hiding pseudo-random data hiding is selected. For example, 'NP' is an integer number that is NP = 20. Additional encrypted pixels are separated into their respective group numbers, including pseudo-random permutations and L pixels. The spare technique is identified through the data hiding key.

c. Image Decryption: When the embedded image contains encrypted data, the receiver first creates the encryption key RI, J, K and the image decryption method is unique - or the received data and RI, J, uncertainty the pixel implanted in the pixel block is '0 ' and The pixel belongs to 'S_1', or the implanted bit is '1 ', the pixel goes to 'S_0 ', and the data hiding is arbitrary encryption does not affect the normalized bit pixel. Therefore, it must be the same as the LSB original, which means that the decoded grayscale values of the three LSB decoded pixels are correct.

This means that the decrypted data must be numerous from the initial LSB. Here, double, ' J, K +, BI, J, and K = 1 ', the bit embedded in the pixel chunk is '0 ', the pixel goes to 'S_0', or the embedded pixel with the bit 1 is the S_1. Decrypted LSB D. Data extraction has data hiding, and he can goal to mine implanted information based on data hiding keys. M, S and Np selected scrambled pixels of the original LSB, and the ' (N-NP)*S / L-Np ' extra bits can be mined from the value containing the embedded data encrypted image. The NP is retrieved in its original location LSB, the Np encrypted data of the selected pixel, and their original gray value can be correctly decoded using the encryption key.

d. Data extraction and image recovery: Since information extraction is totally free from media unscrambling, the request for them suggests two diverse commonsense applications.

Case 1: 'Extracting Data from Encrypted Images: To oversee and refresh individual data of pictures which are scrambled for securing customers' protection, a second rate data set administrator may just gain admittance to the information concealing key and need to control information in encoded area.

The request for information extraction before picture decoding ensures the possibility of this work for this situation. At the point when the information base chief gets the information concealing key, he can unscramble the LSB-planes of and extricate the extra information by straightforwardly perusing the decoded variant. While mentioning for refreshing data of encoded pictures, the data set supervisor, at that point, refreshes data through LSB substitution and scrambles refreshed data as indicated by the information concealing key once more. As the entire interaction is altogether worked on scrambled area, it keeps away from the spillage of unique substance (Xinpeng Zhang et al 2016).

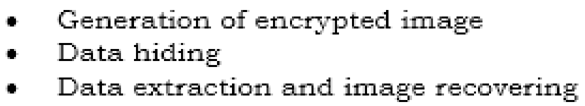
Case 2: 'Extracting Data from Decrypted Images:' In Case 1, both inserting and extraction of the information are controlled in scrambled space. Then again, there is an alternate circumstance that the client needs to unscramble the picture first and concentrates the information from the decoded picture when it is required. The accompanying model is an application for such situation. Expect Alice re-appropriated her pictures to a cloud worker, and the pictures are scrambled to secure their substance. Into the encoded pictures, the cloud worker denotes the pictures by installing some documentation, including the character of the pictures' proprietor, the personality of the cloud worker and time stamps, to deal with the scrambled pictures. Note that the cloud worker has no option to harm the pictures. Presently an approved client, Bob who has been shared the encryption key and the information concealing key, downloaded and decoded the pictures. Weave wanted to get checked decoded pictures, i.e., unscrambled pictures actually including the documentation, which can be utilized to follow the source and history of the information. The request for picture unscrambling previously/without information extraction is totally reasonable for this case (Dr. J. Jagadeesan et al 2014).

PROPOSED METHODOLOGY

The problem of data hiding is about how efficient the data hidden in the image could be retrieved in efficient manner. There are many algorithms has been used in earlier days and the methods has used various measures and strategies to encode the data into the image. The block based methods has use, each block to encode the data and in some of the methods, other forms of approaches has been used. The problem of block based approach is to decide, how many blocks are necessary to encode the data and how much amount could be encoded in the image. To overcome the existing problems, here proposed the Multi-Level Continuous Reversible Character Encoding Scheme, Random Block Selection Technique and Random Substitution Box Generation Method. These methods stores different information regarding the encoding scheme in the first block. The diagonal element includes the information about the coding scheme. Then the method identifies the minimum value from the first block and selects the number of blocks based on the power function. According to the result of a power function, some blocks will be chosen according to the length of a message to be encoded. The message will be encrypted in the diagonal elements and will be decoded in the same procedure at the receiving side. The simulation work does with the MATLAB 2018a environment.

a. Multi-Level Reversible Character Encoding (MLRCE) Scheme: The block based Multi-level Reversible Character Encoding Scheme computes the size of data to be hidden and compute the number of blocks necessary to hide the data. Based on the size and number of blocks the method assigns the level of coding should be used. The method encodes the size of data to be hidden in the first row of the block and the second layer is used to specify the number of blocks and then the third layer is used to specify the number of layers to be used. The entire process has been split into number of stages namely, Metadata Coding, Multi-Level Reversible Character Encoding, Multi-Level Decoding and Remainder-Averaging scheme. In this stage, the method reads each bit of input information and number of bits to be encoded and the number of layer prescribed. For each layer or row of the block, the method computes the averaging scheme. The averaging scheme returns the row and the method replaces the block with the averaging result produced. This will be iterated for each of the bit of the information and if the number of layer is higher than one, then the method uses the second and third layer, which is continued till the number of bits to be encoded is finished.

b. Random Block Selection (RBS) Technique: The primary thought of this strategy is first to appraise a bit of the pixels in a unique picture using the rest pixels and get the assessment mistakes. At that point we encode the assessment bogus and the rest pixels independently utilizing the Random Block Selection calculation. The information hider then inserts the mystery information into the encoded assessment mistakes utilizing the information concealing key and scrambles the picture utilizing the sharing key. At the collector side, the mystery information and the first picture can be removed and recuperated independently by utilizing diverse security keys. The arbitrary square determination is made out of three stages:



- Generation of encrypted image
- Data hiding
- Data extraction and image recovering

These 3 stages are cultivated by the substance proprietor, data hider and collector, individually. In the third stage, two cases are actualized which is information extraction when picture recuperating for meet various applications.

C. Random Substitution Box Creation (RSBC) Method: The previous method looks for the data at each block even if there is no data hidden in the block. To overcome this issue in this work, to proposed the Random Substitution Box Creation (RSBC) method. The proposed RSBC method can be further embedded the data directly into the secret image without need any preprocessing action on the original image. The method selects the pixels of the RSBC as a group to encrypt, and the data is hidden to search for the absolute difference between the groups.

EXPERIMENTAL RESULTS AND DISCUSSION

There are a few techniques to quantify the exhibition of the proposed method. Numerous medial scan images every one of size 256x256 pixels have been picked as cover picture for information implanting. The adequacy of the inserting cycle has been broke down based on PSNR and MSE on the two advanced medical images. The execution time has additionally been registered, that is the measure of time it takes to handle the picture for the MATLAB programming. The condition for figuring the Mean Square Error (MSE) and Peak Signal to clamor proportion (PSNR) (R. Senthilnathan et al 2018)are given as follows:

$$PSNR = 10\log_{10}(255 \times 255 \div MSE)\text{dB}$$

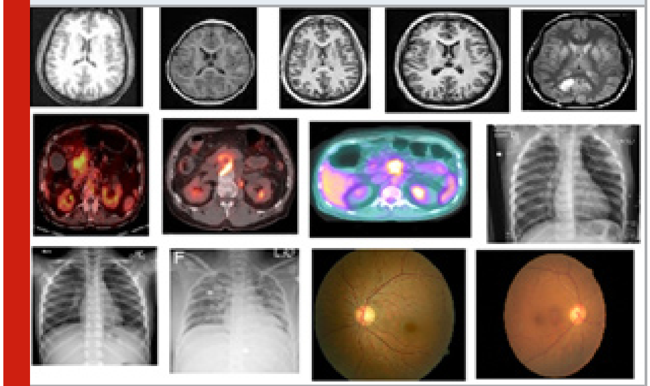
$$\text{MSE}=\frac{1}{PQ}\sum_{i=1}^{P}\sum_{i=0}^{q}(x_{i,j}-y_{i,j})^2$$

The MATLAB code has been implemented with various medical scan images show in below Fig.2.

The values of MSE and PSNR are shown in the Table1 and Table2.

The performance of the proposed algorithm has been evaluated using the various algorithms are shown in the table

Figure 2: Input medical images



The above Table clearly shows that proposed algorithm has a maximum PSNR in the medical images. The highest PSNR achieved from proposed RDH technique has been compared with various algorithms in order to evaluate the performance at the different medical scan images. The comparative analysis is shown in following fig 3

Comparative Analysis of the PSNR value for the Proposed RSBC Algorithm with the other existing algorithms using medical datasets.

Table 1. PSNR Comparison for different algorithms

S.NO	MLRCE	RBS	RSBC
IM1	20.29	23.06	28.75
IM2	20.02	22.69	35.86
IM3	21.05	23.59	37.35
IM4	20.23	23.26	36.00
IM5	10.13	12.61	14.00
IM6	11.70	13.79	15.52
IM7	11.03	14.21	17.52
IM8	11.68	13.76	18.03
IM9	11.04	12.80	16.28
IM10	11.16	13.07	17.09

Figure 3: Comparative Analysis of the PSNR value

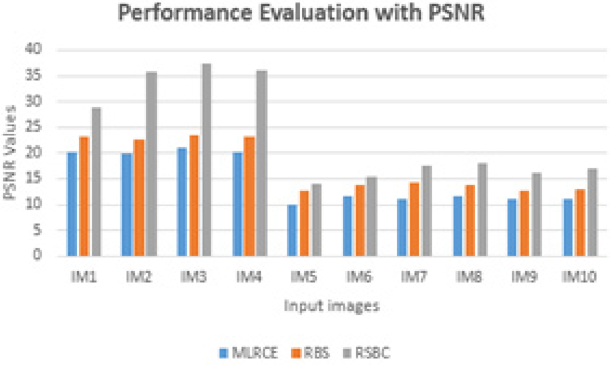


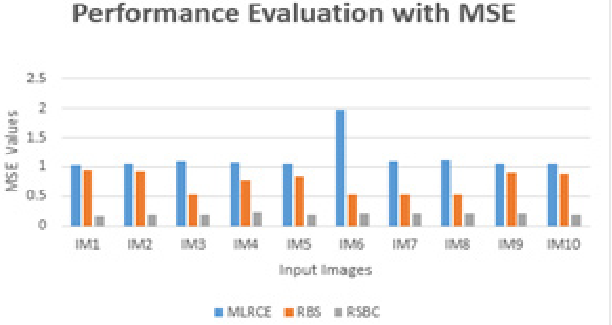
Table 2. MSE Comparison for different Algorithms

S.NO	MLRCE	RBS	RSBC
IM1	1.04	0.95	0.17
IM2	1.05	0.93	0.19
IM3	1.10	0.52	0.19
IM4	1.07	0.78	0.23
IM5	1.06	0.85	0.19
IM6	1.98	0.53	0.21
IM7	1.10	0.53	0.21
IM8	1.11	0.53	0.22
IM9	1.06	0.90	0.21
IM10	1.06	0.88	0.20

Table 2 clearly shows that RSBC algorithm has a minimum MSE in the medical images in order to evaluate the performance. The comparative analysis is shown in following fig 4

The above figure clearly shows that RSBC algorithm has minimum MSE values when compared with other steganography algorithms.

Figure 4: Comparative Analysis of the PSNR value



CONCLUSION

Currently, the essential for transmitting medical scan images is rising promptly also progressive medical information system is varying the method that medical scan images are accessed, stored and circulated. A big quantity of patients' personal data is comprised in medical scan images. Thus, the secrecy defense of medical scan images has come to be a significant subject. Steganography which is an art as well as a science of invisible transmission arrived as a protector by providing utmost security through various techniques. Most of obtainable image steganography systems might extinguish the inter block data also hence the security presentation is not fulfilled so far. This research paper mostly focuses on numerous related works also methodology of data hiding as well as extraction among them. A novel medical scan image steganography system is intended depends on conserving the enslavements of inter block data in medical images. Comparative analysis demonstrate that the RSBC system can successfully process the data-hiding method, and obtain better performance when compared with MLRCE and RBS methods.

REFERENCES

Thinn A.A., Thwin M.M.S. (2019) Modification of AES Algorithm by Using Second Key and Modified SubBytes Operation for Text Encryption. In: Alfred R., Lim Y., Ibrahim A., Anthony P. (eds) Computational Science and Technology. Lecture Notes in Electrical Engineering, vol 481. Springer, Singapore

Parameshachari, B.D., Panduranga, H.T. and liberata Ullo, S., 2020, September. Analysis and Computation of Encryption Technique to Enhance Security of Medical Images. In IOP Conference Series: Materials Science and Engineering (Vol. 925, No. 1, p. 012028). IOP Publishing.

Prabu, S., Balamurugan, V. and Vengatesan, K., 2019. Design of cognitive image filters for suppression of noise level in medical images. Measurement, 141, pp.296-301.

Norouzi B et al (2014) A simple, sensitive and secure image encryption algorithm based on hyperchaotic system with only one round difusion process. Multimed Tools Appl 71(3):1469–1497

Prabu, S., Lakshmanan, M. and Mohammed, V.N., 2019. A multimodal authentication for biometric recognition system using intelligent hybrid fusion techniques. Journal of medical systems, 43(8), pp.1-9.

Kumari M, Gupta S, Sardana P (2017) A survey of image encryption algorithms. 3D Res 8(4):37

Zahmoul R, Ejbali R, Zaied M (2017) Image encryption based on new Beta chaotic maps. Opt Lasers Eng 1(96):39–49

Liu Hongjun, Wang Xingyuan (2011) Color image encryption using spatial bit-level permutation and high-dimension chaotic system. Opt Commun 284(16-17):3895–3903

Guan Zhi-Hong, Huang Fangjun, Guan Wenjie (2005) Chaos-based image encryption algorithm. Phys Lett A 346(1-3):153–157

Ye G, Wong KW (2012) An efficient chaotic image encryption algorithm based on a generalized Arnold map. Nonlinear Dyn 69(4):2079–2087

Patro K, Banerjee A, Acharya B (2017) A simple, secure and time efcient multi-way rotational permutation and difusion based image encryption by using multiple 1-D chaotic maps. In: International Conference on Next Generation Computing Technologies. Springer, Singapore, pp 396–418

Patro K, Acharya B (2018) Secure multi–level permutation operation based multiple color image encryption. J Inf Secur Appl 40:111–133

Hailan Pan, Lei Yongmei, Jian Chen (2018) Research on digital image encryption algorithm based on double logistic chaotic map. EURASIP J Image Video Process 2018(1):142

Sravanthi D et al (2019) A secure chaotic image encryption based on bit-plane operation. Soft computing in data analytics. Springer, Singapore, pp 717–726

Partheeban P, Kavitha V (2018) Dynamic key dependent AES S-box generation with optimized quality analysis. Cluster Comput. https://doi.org/10.1007/s10586-018-2386-6

Ashraf Odeh, Shadi R.Masadeh, Ahmed Azzazi, "A performance evaluation of common encryption techniques with secure watermark system(SWS)", International Journal of Network Security & Its Applications(IJNSA), vol. 7, No. 3, pp. 31-38, 2015.

R. Senthilnathan1, A. Marimuthu "Non-linear Based Hybrid Denoising filter for Alzheimer's disease Magnetic

Resonance Imaging“ International Journal of Computer Sciences and Engineering, Vol.-6, Issue-11, Nov 2018 E-ISSN: 2347-2693

Zhaoxia Yin, Andrew Abel, Xinpeng Zhan, Bin Luo “Reversible Data Hiding In Encrypted Image Based On Block Histogram Shifting“ Acoustics, Speech and Signal Processing (ICASSP), 2016 IEEE International Conference on, DOI: 10.1109/ICASSP.2016.7472053, Pages:2129-2133

Xinpeng Zhang, Jing Long, Zichi Wang, and Hang Cheng ”Lossless and Reversible Data Hiding in Encrypted Images with Public Key Cryptography” IEEE Transactions on Circuits and Systems for Video Technology, DOI:10.1109/TCSVT.2015.2433194, Volume: 26, Issue: 9, Sept. 2016, Pages:1622-1631

Dr. J. Jagadeesan, Mr. Balika J. Chelliah, Nikhila Nyapathy, Neha Tiwari ”Reversible Data Hiding In Encrypted Images Using AES Data Encryption Technique” International Journal of Emerging Research in Management &Technology, ISSN: 2278-9359 (Volume-3, Issue-4) April 2014.