iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** VIII **Month of publication:** August 2017

DOI: http://doi.org/10.22214/ijraset.2017.8019

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue VIII, August 2017- Available at www.ijraset.com

Improved Approach to Encrypt Medical Data

Jasmine Kaur[1], Dr. Gagandeep[2]
[1,2] *Department of Computer Science Punjabi University Patiala,Punjab*

Abstract. In this paper, an improved steganography technique has been proposed based on embedding in middle pixels of a 3*3 window in which corner pixels are used to detect edges in an image so that only those can be chosen which has varying intensity i.e. edges in them. In the initial step the ROI object is detected. To select the ROI, rectangular box is used on which the salient object is located by applying active contour segmentation. Two matrices are made from sanitized area pixels each containing LSB and MSB bits. Pseudo random no generation algorithm is used for MSB bits encryption. Non overlapping square blocks are used to convert the whole image and edge block are calculated by taking four corner pixels of a 3*3 block. To embed the encrypted MSB bits into block one bit LSB steganography is used. ROI object is blacked out after embedding stego image. The reverse of embedding process is extraction. By taking edge blocks encrypted MSB bits are extracted from the stego image during extraction to the extracted bits decryption algorithm is applied and in the original location the resulted image bits are stored. Experimental results show that there is 20% increase in embedding capacity from the existed system and system is able to hide only useful information of a medical image. As MSB bits are chosen for embedding, system has even higher embedding capacity in which remaining LSB bits can be useful for data hidden

Keywords: Edge detection, Active contours, Encryption, Steganography, LSB

I. INTRODUCTION

These days, a recent cybercrime is the capture of medical data. If medical data is captured or altered, it may cause a violation of patient's rights and changes in medical treatment Hence, all patient records, especially medical images, must be kept confidential [1]. An electronic health record (EHR) is a systematic collection of electronic health information about a patient or population. It may include clinical examinations, patient demographics, diagnosis annotations, prescriptions, medications, past medical history, histological and other findings, vital signs, immunizations, laboratory data, and radiology reports. It is gathered for patient care, clinical research, epidemiological studies, or insurance companies. It is shared by means of information systems and local or wide networks. The process of medical image information accounts for at least 90% of all the medical information in a hospital system [2, 3]. Medical images (X-ray, CT (computed tomography), MR (magnetic resonance) imaging, ultrasound, etc...) are handled, stored, printed, and transmitted using the Digital Imaging and Communications in Medicine standard. Hence, patient information must be secured within the network to prevent tampering, illegal copying, and patient privacy leaks, and to ensure copyright protection, and other information security issues [3]. Medical information (MI) security protects the rights of patients and ensures the responsibilities of the health professionals. Health information systems must possess three mandatory characteristics: confidentiality, reliability, and availability [4]. Security tools such as firewalls, virtual private networks (VPNs), and cryptography techniques (symmetric, asymmetric, or hashing encryption) are used to secure medical data. However, firewalls are easily bypassed by hackers. Encryption does not guarantee the confidentiality or secrecy of data; moreover, it increases computational costs. In addition, the file headers of medical data can be captured in the plaintext format [4]. Alternatively, steganography techniques can be used to increase the security of medical data.

II. PARAMETERS OF AN EFFICIENT HIDING SYSTEM

There are three most important parameters for an information hiding system, known as capacity, imperceptibility and robust-ness. Robustness refers to protection against any manipulation or attack sought out by the hackers or the eavesdropper in the transmitted information. Imperceptibility refers to the fact that the original cover image and the hidden information are in distinguishable. Capacity refers to the amount of data or in case of image the size of image that can be hidden the cover image. The information hiding schemes are principally classified into Steganography and Watermarking [5], depending on the application. The term Steganography is derived from the Greek word, steganos meaning "covered" and graphy meaning "writing" hence called covered writing. In Steganography systems, our main aim is to provide more capacity, security and maintain the quality of the cover image in which the payload has been introduced. It usually deals with trans-mission of such hidden data along the communication network such that the hidden messages appear to be undetectable to the eaves dropper who will be putting all his efforts to get through it.

III. RELATED WORK

A. *G.L. Smitha et. al. [6]* reviewing the two Steganography algorithms - Least Significant Bit and (LSBMR)- based approach. They considers digital images as covers and verifies an adaptive and secure data hiding scheme in the spatial domain. Existing image steganographic methods lack in the complexity, which can be utilized by the radical to decode the images and neutralize the operations. Several methods have been proposed in order to combat this. Perhaps the most efficient method is Least-Significant-bit Matched Revisited (LSBMR)- based approach. It is a famous type of steganographic methods in the spatial domain.

B. *K. Joshi et. al. [7]* presented a three bit XOR steganography system for concealing messages into gray Images is projected. In this method, last three bits of pixel value offer 100 percentage of message addition. This new technique uses the XOR operation between the message and original image. If the intruder extracts the last three bits, he would not be able to find the meaning of the message as the message is in decoded form.

C. *N. Patel et. al. [8]* proposed a technique for the space domain image steganography. Here, modification of least significant bit (LSB) of picture element of carrier image (CI) is done by the most significant bit (MSB) of secret image (SI). Here, along with information hiding, security is provided by the dynamic key cryptography. The dynamic feature of key is enabled by rotating the key and each rotation of key produces new key. In this technique, pixel selection of carrier image and secret image is done on the basis of pseudo random number (PRN) which provide double layer security against the stegano analytic attack.

D. *H.N. N. Simha et. al. [9]* Proposed a frequency domain Image Steganography using DWT and Modified LSB technique . The proposed approach uses DWT to convert spatial domain information to frequency domain information. The LL band is used for further Image Steganographic process. The image is decoded using inverse LSB. Since the LL band is used for encoding and decoding purpose, memory requirement of the design is less for hardware implementation. Also this will increase the operating frequency of the architecture.

E. *S. N. Gowda [10]* proposed an algorithm which is a modulation of the standard Least Significant Bit Algorithm (LSB). In the proposed algorithm the information to be hidden is considered to be text. This text is taken and first encrypted using the Data Encryption. Standard Algorithm (DES) with the help of a key. This key to encrypt the data is then encrypted using the RSA algorithm.

F. *A. Arora et. al. [11]* gives an overview of LSB technique of steganography and further they proposed and implemented a unique algorithm to base steganography which is an enhanced and improved technique better in all aspects. The paper further compares their proposed enhanced technique with the existing LSB technique on various parameters.

G. *S. N Gowda et. al. [12]* Developed an approach to help increase the security of the algorithm. For the proposed approach they consider the entire data to form one big block of information. The first step is to encrypt this information. This is done using the famous Advanced Encryption Standard (AES) algorithm. The key to encrypt this information is then hidden using the RSA algorithm. This adds an extra layer of security to the algorithm. Next the encrypted block of data is broken down to 'n' blocks, where 'n' is chosen by the user. 'n+1' images are then chosen at random and each block is hidden using LSB with an image.

H. *B. Debnath et. al. [13]* Introduces a novel architecture for image steganography using reversible logic based on quantum dot cellular automata (QCA). Feynman gate is used to achieve the reversible encoder and decoder for image steganography. A Nano communication circuit for image steganography is shown using proposed encoder/decoder circuit. The proposed QCA circuits have lower quantum cost than traditional designs.

I. *A. U. Islam et. al. [14]* proposed a novel image steganography technique based on most significant bits (MSB) of image pixels. Bit No. 5 is used to store the secret bits based on the difference of bit No. 5 and 6 of cover image. If the difference of bit No. 5 and 6 is different from secret data bit then the value of bit No. 5 is changed. Usually, the hackers focus on LSB bits for secret data extraction but the proposed technique utilizes the MSB bits that make it more secure from unauthorized access

.

IV. PROPOSED WORK

The hiding area size is based on user selection. In such area the size of bits is larger than the normal text message size that is hidden inside an image with steganography.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue VIII, August 2017- Available at www.ijraset.com

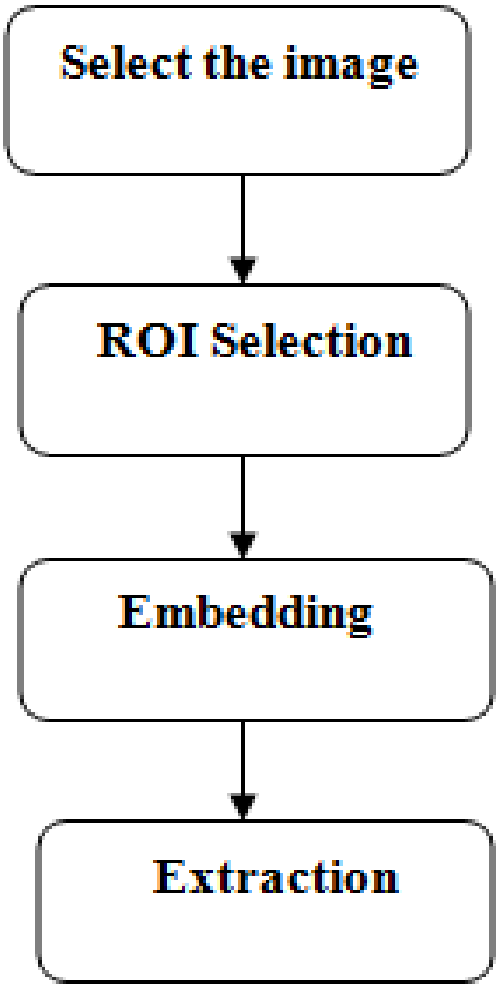


Fig. 1. Proposed Model

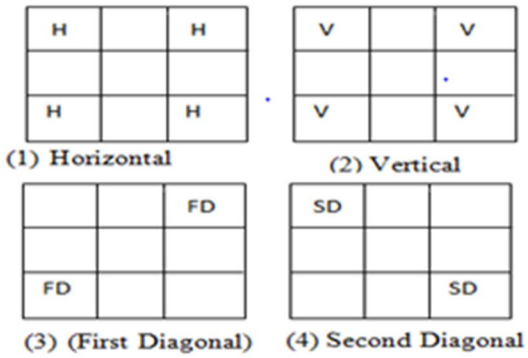
The probability of detection is increased with larger payloads. A method is implemented to maintain 100 percentage quality restored by decreasing the size of payloads. The four most significant bits (MSB's) are extracted from the ROI area. Inside the selected area, the most of the image informative information is presented by most significant bits (MSB). The least significant bits are not image informative, so there is possibility to leave behind the least significant bits. The quality of ROI is not lost after the extraction process as the most significant bitsvare simply reapplied to the ROI.

A. Stepwise Description of Process

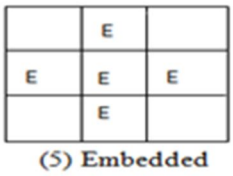
1) ROI selection and encryption. In this step, the image to be embedded is selected and a region is cropped around the region of interest. Further object is localized using active contours which will be used for further processing. MSB bits from this region are encrypted.

2) Embedding. To embed the encrypted MSB bits into blocks which have highest entropy first one bit steganography is used. In the sharp contrast area (edges) as compared to uniform area of image the human visual system is less sensitive. The edge (sharp) regions of the cover image are discovered such that the two edge images generated using the original cover image and the stego image are identical. This will enable the correct extraction of the concealed message from the stego image

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue VIII, August 2017- Available at www.ijraset.com



. (a)



(b)

Fig. 2. (a) 3 × 3 block edges and (b) Selected pixels for embedding 3 × 3 block.

Algorithm for embedding has been written as under.

Step 1. Divide the image C into non-overlapping blocks of the size n × n.

Step 2. Compute the absolute mean difference between the left and right columns of the block (magnitude of vertical edge). Repeat same for horizontal, first diagonal and second diagonal edges. Figure 2(a) shows the specific pixels used to calculate the edges for the 3 × 3 block.

Step 3. Find the maximum of the four values and assign it to e. If e > Th, then the block is considered to be an edge block, otherwise it is not an edge block. Construct E that contains the calculated e value of each of the edge blocks, and 0 for non-edge blocks. A binary edge image can also be constructed, which contains 1 for edge blocks and 0 for non-edge blocks. For the edge blocks, embed in the shaded 5 pixels as shown in Figure 2(b).

Step 4. In order to evaluate the obtained binary edge image of the proposed algorithm, we considered the gray image shown in used different values of threshold in constructing binary edge images using a block size of 3 × 3 block in the cover image to have the same edge strength as its counter part in the stego image.

Step5. The embedding process is performed on the detected edge locations using the proposed XOR coding. This method partitions the index table into groups of four pixels and encodes three message bits into the pixels of each group. The XOR operation ensures that the secret message is concealed into the cover with minimum number of pixel changes. Thus, the three secret bits m1,m2, and m3 are embedded in the four LSBs p1, p2, p3, p4 and p5 (one bit for each edge pixel) according to the following procedure:

Perform the following three XOR operations

$$k1 = p1 \oplus p2$$
$$k2 = p3 \oplus p4$$
$$k3 = p1 \oplus p3$$

To embed the secret bits m1,m2, m3 and m4, the three calculated bits k1, k2 and k3 are compared with the secret message bits m1,m2, m3. The result of this comparison, which can take one of eight possibilities, determines which of the four bits p1, p2, p3, and p4 have to be modified, as shown in Table 4.1 and p5 is embedded with same message bit m4.

TABLE I. Embedding Conditions

Condition			Action
m1=k1	m2=k2	m3=k3	No Change Required
m1= k1	m2= k2	m3≠ k3	Complement p3 and p4
m1= k1	m2≠ k2	m3= k3	Complement p4
m1= k1	m2≠ k2	m3≠ k3	Complement p3
m1≠ k1	m2= k2	m3= k3	Complement p2
m1≠ k1	m2= k2	m3≠ k3	Complement p1
m1≠ k1	m2≠ k2	m3= k3	Complement p2 and p4
m1≠ k1	m2≠ k2	m3≠ k3	Complement p1 and p4

c) Extraction. Proposed system is reversible. stego image can be converted back into original image. During extraction encrypted MSB bits are extracted from the sanitized image by taking maximum entropy block first. Decryption algorithm is applied to the extracted bits and resulted image bits are stored to the original location. The extraction process is easier and faster than the embedding process. It starts by retrieving the threshold value. The edge blocks of the stego image are then identified using the retrieved threshold, which will return the same edge image as the one obtained using the cover image. This will be followed by dividing the LSBs of the edge pixels into groups of four. Finally, for each of the four stego edge bits q1, q2, q3, and q4 the XOR operations listed below are used to retrieve three message bits m1, m2, m3 and m4 is received form the fifth embedding location.

$$m1 = q1 \oplus q2$$

$$m2 = q3 \oplus q4$$

$$m3 = q1 \oplus q3$$

V. RESULTS

Rectangular box is used to select ROI. ROI pixels are separated into two matrices each containing LSB and MSB bits. MSB bits are encrypted using pseudo random no generation algorithm. In the proposed system only MSB bits are hidden within the image because it decreases the payload size and decreases the probability of detection.

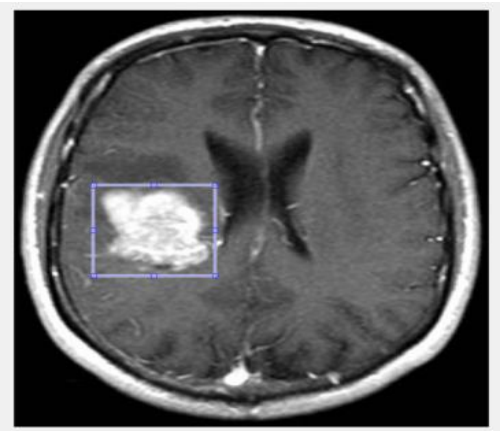


Fig. 3 shows the rectangle for selecting the sanitized area.

In Object detection phase, tumor etc. has been figured out and cropping has been done around the tumor only hence results in least area needed for embedding.

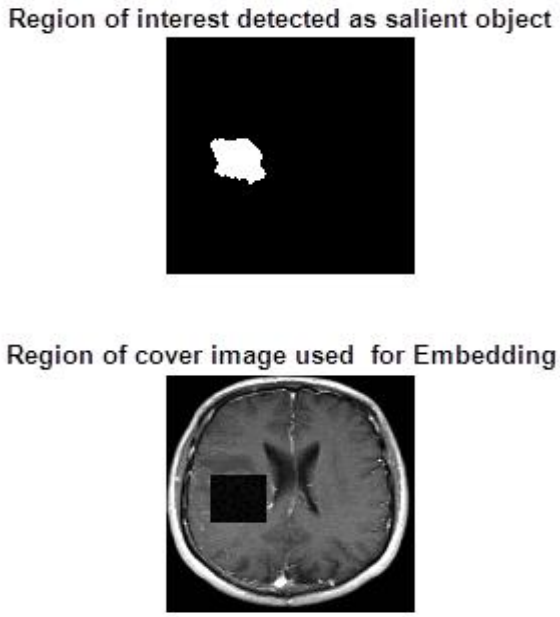


Fig. 4. (a) detected tumor object (b) Image used for embedding

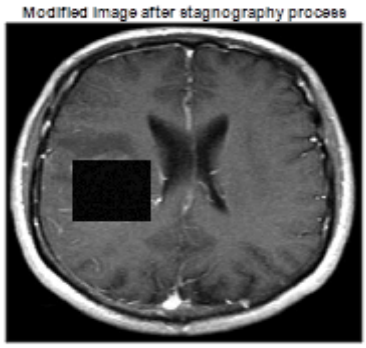


Fig. 5. Modified image after steganography embedding process

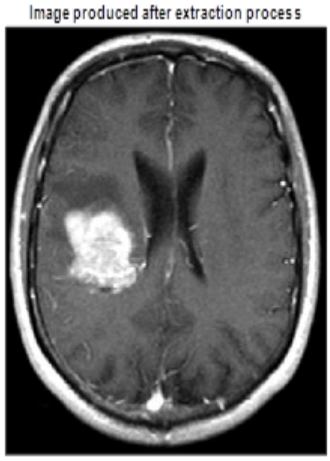


Fig. 6. Image produced after extraction process

A. Performance Efficiency

1) Mean Square Error (MSE): The MSE signifies the cumulative squared error between the input and the output image. It is calculated by the following equation (1).

$$MSE = \frac{\sum_{M,N}[I1(m,n) - I2(m,n)]^2}{M * N} \quad (1)$$

Where N and M are the number of columns and rows in the input images, respectively and I1 (m, n) is the input image, I2 (m, n) is the sanitized image.

2) Peak Signal-to-Noise Ratio (PSNR): Signal–to-noise ratio (SNR) is a mathematical measure of image quality. PSNR is defined by the following equation (2)

$$PSNR = 10\log_{10}\left[\frac{R^2}{MSE}\right] \quad (2)$$

Where R represents maximum fluctuation or value in the image, its value is 255 for 8 bit unsigned number.

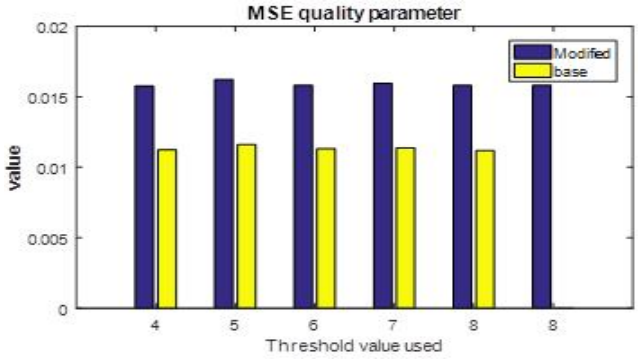


Fig. 7. MSE Index at different thresholds for image one

TABLE II. Result Table for Proposed method

T	Elapsed time (embedding)	Elapsed time (extraction)	MSE	PSNR
Proposed				
4	0.6574	0.4533	0.07488	59.3869
5	0.7473	0.4634	0.07521	59.3678
6	0.7441	0.4767	0.07554	59.3485
7	0.7017	0.4804	0.07505	59.3767
8	0.7180	0.4714	0.07521	59.3676
9	0.7145	0.4745	0.07551	59.3505
Base				
4	1.1565	0.4802	0.05365	60.8345
5	1.1655	0.4652	0.05380	60.8224
6	1.1229	0.4604	0.05399	60.8072
7	NA			
8	NA			
9	NA			

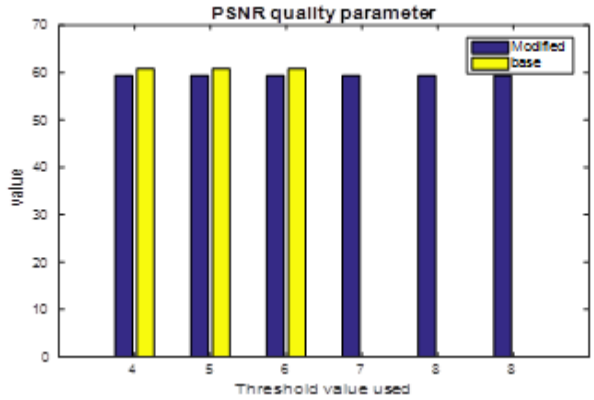


Fig.8. PSNR Index at different thresholds for image one

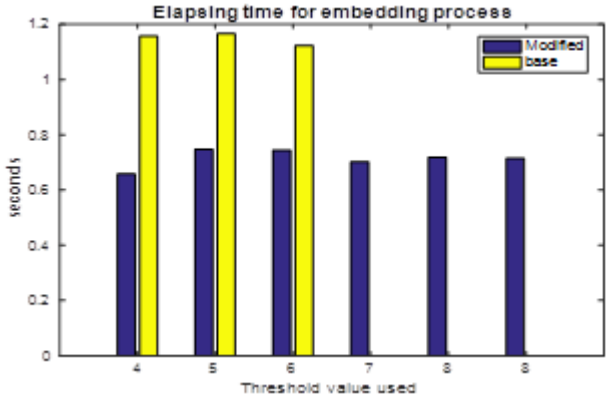


Fig. 9. Elapsing time for embedding process

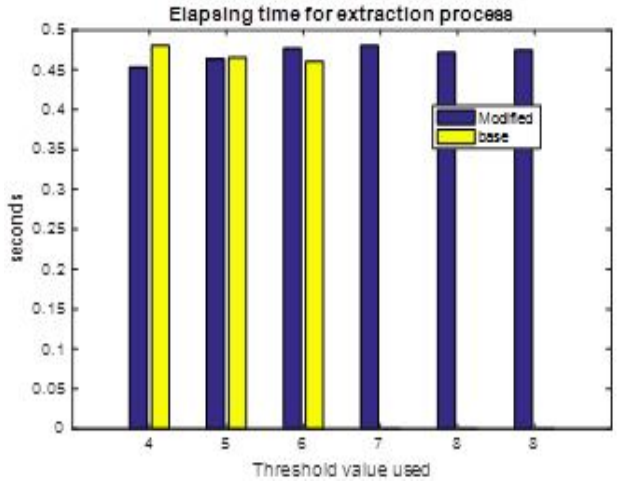


Fig. 10. Elapsing time for extraction process

Figures above shows that proposed algorithm has less elapsing time in both embedding and extraction phases. Graphs an table also shows that existed method fails when threshold is increased whereas proposed system can embed more pixels hence can be chosen for large object sizes.

VI. CONCLUSIONS

It has been found that proposed method increases in 20% of embedding capacity as there are five pixels are used for embedding as compared to four pixels. The active contour based segmentation results in reduction of ROI boundary hence less no. of pixels are

need for embedding as whole ROI can be selected with marginal extra pixels for hide. The security has been improved as MSB bits are embedded after encryption process in which a pseudo random generator has been used which produces random bits of same size as secret message bits by taking a seed point from a user defined key. Further XOR operation is implemented using these random bits and the secret message results in a encrypted secure message. The technique adopted for data hiding is also fully reversible in nature as edge parameter has been used for selecting the pixels which can be modified. As existed edge detectors i.e. Canny, Soble does not results in same edge pixels when provided on original and modified image, there can be a loss of data when secret message is extracted. For this we have used corner pixels of a 3*3 window for detecting edges and remaining five pixels has been used for data embedding. It results in no modifications in corner pixels and edge detection remains same on both original and modified image.

REFERENCES

[1] G. Coatrieux, H. Maitre, B. Sankur, Y. Rolland, R Collorec ”Relevance of watermarking in medical imaging” in: Proceedings of the 2000 IEEE EMBS International Conference on Information Technology Applications In Biomedicine. 2000, pp. 250-255.

[2] Muhammad Sajjad; Khan Muhammad;Sung Wook Baik; Seungmin Rho; Zahoor Jan; Sang-Soo Yeo;Irfan Mehmood," Mobile-cloud assisted framework for selective encryption of medical images with steganography for resource-constrained devices." published in Multimedia Tools and Applications (2016), pp 1–18

[3] L-Q. Kuang. Y. Zhang. X. Han “Watermarking image authentication in hospital information system” in: Proceedings of International Conference on Information Engineering and Computer Science. 2009.1C1ECS 2009, pp. 1-4.

[4] H. Nyeem. W. Wageeh Boles. C. Colin Boyd” A review of medical image watermarking requirements for teleradiology ” J. Digit. Imaging 26 (2013) 326-343.

[5] N. Bi, Q. Sun, D. Huang, Z. Yang, J. Huang, Robust image watermaking basedon multiband wavelets and empirical mode decomposition, IEEE Trans. ImageProcess. (2007), August.

[6] G. L. Smitha and E. Baburaj, "A survey on image steganography based on Least Significant bit Matched Revisited (LSBMR) algorithm," 2016 International Conference on Emerging Technological Trends (ICETT), Kollam, 2016, pp. 1-6.

[7] K. Joshi and R. Yadav, "New approach toward data hiding using XOR for image steganography” 2016 Ninth International Conference on Contemporary Computing (IC3*)*, Noida, 2016, pp. 1-6

[8] N. Patel and S. Meena, "LSB based image steganography using dynamic key cryptography,*"* 2016 International Conference on Emerging Trends in Communication Technologies (ETCT), Dehradun, 2016, pp. 1-5.

[9] H. N. N. Simha, P. M. Prakash, S. S. Kashyap and S. Sarkar, "FPGA implementation of image steganography using Haar DWT and modified LSB techniques," 2016 IEEE International Conference on Advances in Computer Applications *(ICACA)*, Coimbatore, 2016, pp. 26-31.

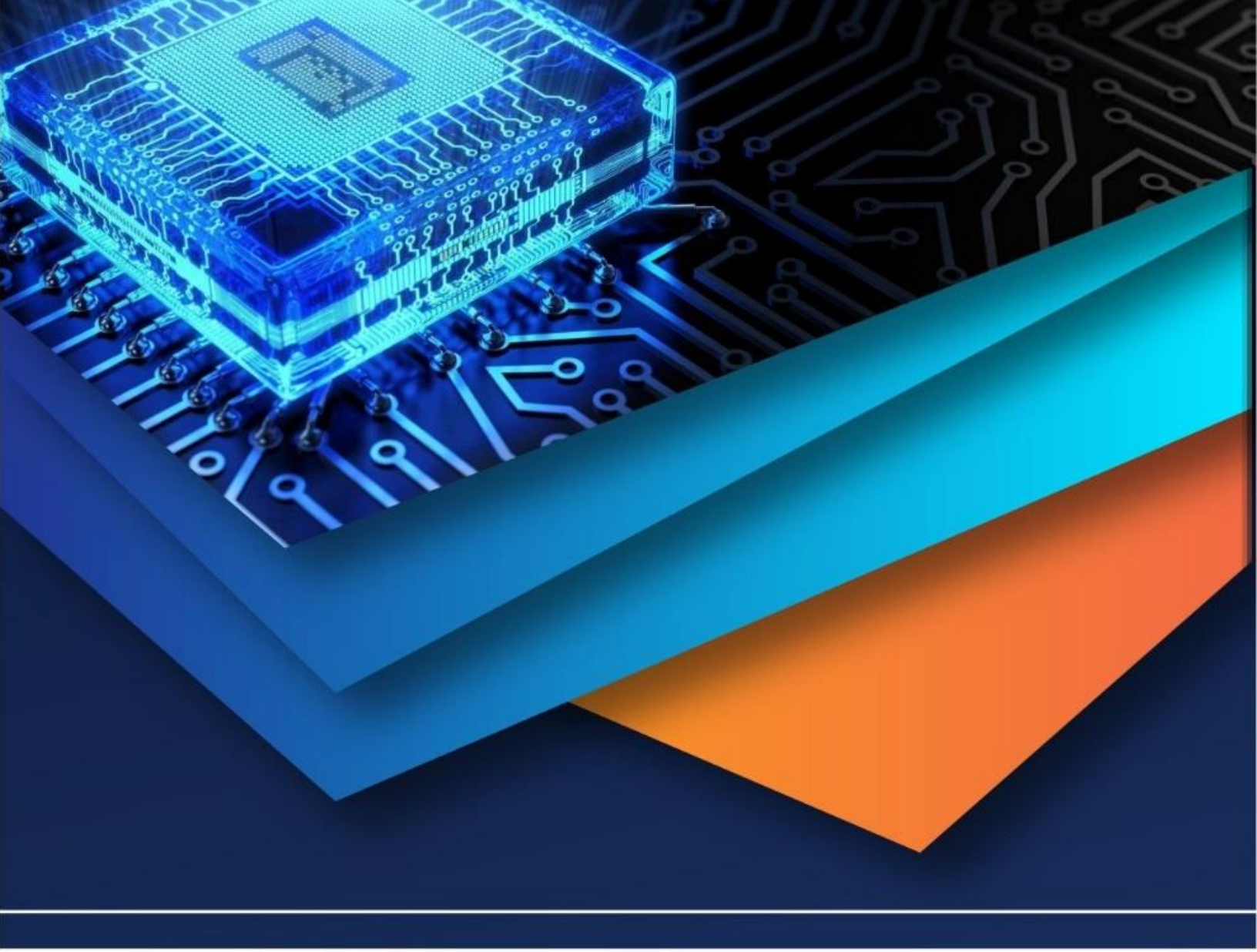
[10] S. N. Gowda, "Dual layered secure algorithm for image steganography,*"* 2016 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), Bangalore, 2016, pp. 22-24.

[11] A. Arora, M. P. Singh, P. Thakral and N. Jarwal, "Image steganography using enhanced LSB substitution technique,*"* 2016 Fourth International Conference on Parallel, Distributed and Grid Computing (PDGC), Waknaghat, 2016, pp. 386-389.

[12] S. N. Gowda, "Advanced dual layered encryption for block based approach to image steganography,*"* 2016 International Conference on Computing, Analytics and Security Trends (CAST), Pune, 2016, pp. 250-254.

[13] B. Debnath, J. C. Das and D. De, "Reversible logic-based image steganography using quantum dot cellular automata for secure nanocommunication,*" in* IET Circuits, Devices & Systems, vol. 11, no. 1, pp. 58-67, 1 2017.

[14] A. U. Islam *et al.*, "An improved image steganography technique based on MSB using bit differencing,*"* 2016 Sixth International Conference on Innovative Computing Technology (INTECH), Dublin, 2016, pp. 265-269



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY