iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** II **Month of publication:** February 2020

DOI: http://doi.org/10.22214/ijraset.2020.2063

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: 7.177
Volume 8 Issue II Feb 2020- Available at www.ijraset.com

Block based Cipher Key Image Encryption Algorithm combined with Compression using DWT

Sonal Yadav[1], Anamika Tiwari[2]
[1, 2]*Bhabha Institute of Technology, Kanpur, India*

Abstract: ***The internet transfer of pictures has resulted to a safety issue where private images must be protected from unauthorized access. In the increasing technological age, nearly everyone shares their private data with other users, including pictures over the internet, or a database repository that attracts hackers to take advantage of this data. Security supplied pictures such as blue printing of business projects, hidden pictures of the army's concern or the interest of the business using image processing methods have proved useful. In this paper a DWT based compression has been performed along with block transformation based encryption. The aim is to scramble the picture data to a point where the real transmitted picture becomes hard for the intruder.***

Keywords: Watermarking, DWT, haar, coiflet, symlet, wavelets.

I. INTRODUCTION

The Internet has become a requirement today and the data is sent via the internet in the form of emails, pictures and videos. All the data can be sent via e-mail, private blogs, chat apps, and others that are susceptible to multiple assaults with a multitude of electronic media. One of the items that have earned less attention today with the fast growth of Internet use is the unconsciousness of data security and secrecy. Through multiple communication networks, we can send and obtain any data from around the globe. But not many individuals understand that eavesdropping, tapping, hijacking, and many other things are susceptible to the process of sending and receiving emails. Much of that data in particular is confidential and should not be known or intercepted by others. In addition to technology development, cyber crime signs also improved. Several types of data and information assaults exist, such as hackers, crackers, trojans, etc. Today, therefore, many systems have strengthened their attempts to preserve information safety and overcome these assaults. Cryptography is the study of messaging algorithms in encrypted form (not understood) so that only the approved recipients can decrypt and read the message. Cryptography scheme is categorized as a scheme with symmetric key and asymmetric key. Symmetric-key scheme utilizes a single main that both the sender and the receiver have, and asymmetric-key scheme utilizes two distinct keys (a public key and a personal key) where everyone knows the public key and only the approved receiver knows the private key. Every day, the number of attackers and the tools available to them is increasing, making information exchanged over the internet vulnerable to various types of attacks such as brute force attack, chosen plaintext attack, cipher text attack only. This requires the protection of in-transit data from unauthorized consumers. We are interested in securing picture contents from intruders in this project. Researchers have produced numerous contributions to secure pictures from illegitimate users. Our project's motive is to study and work towards a safe and effective system for in-transit pictures.

The section II gives a literature review followed by the proposed implementation framework in Section III. Section IV gives the analysis and result and finally Section V gives the Conclusion.

II. LITERATURE REVIEW

In[1] Al-Husainy addressed a fresh strategy to picture safety by using two simpler and more effective confusion and diffusion techniques, both of which are Boolean operations, the first is XOR operation conducted on pieces of digital image pixels, and the first is to rotate pixel parts circularly. Many times the method is implemented so that the simple picture becomes a cipher picture owing to growing requirements from high-speed networks. Using main room, main sensitivity and statistically, the findings are also analyzed. Due to XOR and circular rotation, this technique is very easy and powerful owing to the large size of the secret key. The model is quite perfect and sufficient for a wide variety of image processing applications.

A novel approach to digital image safety using steganography cryptosystem described by Azam[2], where encryption is based on RTS's gray-scale substitution boxes and stage embedding technique. RTSs are fuzzily and variable size dependent on confidential image pixel size. The source image's spatial and frequency domains are used to create two random masks. The secret picture is integrated in a host picture that uses steganocrypto technologies to create a random mask using two distinct RTSs on the host

©IJRASET: All Rights are Reserved

picture. Host picture is needed to decrypt the secret picture at the receiving end so that the host picture is also broadcast with another RTS and embedded with the secret picture. The author argues that this s-box cryptosystem plus steganocrypto scheme is the state-of - the-art cryptosystem and after little modification can be used for color pictures and data hiding.

Chen and Lai [3] provided an image encryption security system using CA cellular automata by recursively replacing picture pixels. Due to the flexibility of CA, the suggested method conducts confusion diffusion characteristics. The model of encryption generates lossless pictures by replacing pixel values with the same big secret key on both sender and receiver sides. To demonstrate powerful efficiency, the writers used two color and gray-scale pictures in simulation. The proposed CA scheme utilizes two-dimensional hybrid cellular automatons from Neumann for a key stream of random sequence and recursive replacement. They also addressed the advantages of the suggested scheme as the keys; secret, type selection, CA, and iteration keys are of variable lengths, the second advantage is that they cover replacement and cropping attacks due to 2-D CA size with regard to image size, and the third advantage is their economy in computational use of funds for encryption and decryption, since they use only easy logical and integral And better than RC-4, AES, and 3-DES, the current system.

Pushpad et al.[4] evaluated various picture safety algorithms based on random number generation for encryption / decryption pictures, watermarking, reversible integer wavelet transformation, random matrix, histogram, compression, pixel shuffling, reversible watermarking and steganography, frequency and time domain digital watermarking. But they suggested a mixed picture encryption operation with reversible watermarking. First, the picture is encrypted and then the watermark is integrated in order to improve effectiveness and confidentiality. In order to increase capacity, the watermark is embedded in the frequency domain although it may be embedded in time and frequency domains.

Verma and Jain[5] defined a less complicated algorithm for encrypting pictures using Dual Tree Complex Wavelet Transform which divides the picture into components of approximation and detail. Using the pixel chaotic shuffle method, the first one is encrypted and the other one is shielded using Arnold Transform. According to the claim of the authors, the image is highly secured even if the first image is removed without extracting the algorithm, then the image can not be complete. The simulation results also showed that, while having entropy differences and mean errors, the decrypted image at the receiving end is completely the same as the original. Wang et al.[6] proposed that DWT, discrete wavelet transforms for encryption along with multi-chaos as they are relevant in network body region. According to the proposed algorithm, the two-dimensional discrete wavelet transformation is used for decomposed image spatial reconstruction and multi-chaos matrices are then used for space encryption. The algorithm against attacks is outstanding. The advantages of the suggested algorithm are; it hides the image size to enhance safety, has important room that makes the intruders uncomfortable. Random keys are produced using chaotic techniques. Pixel values and places are used to encrypt.

Garg and Kamalinder[7] provided a steganographic and encryption-based picture security system using AES; a hybrid strategy particularly for cloud computing as internet storage is emerging for users with little accountability and ease because computer hardware is not managed. The cover image is used for steganography based on color illumination-based estimation (CIBE), and bits of encrypted images are changed to hide each pixel of the cover image with the least significant bits of LSBs. A bit of initial picture distinction does not influence its quality and it appears to be the initial picture.

In[8], by following three guidelines, Sedighi and Fridrich focused on four embedding algorithms used in steganography to embed source picture with cover picture. The writers claim the rules have a powerful effect in steganography and provide scientists with knowledge of saturated pixels, although they are uncommon, but their effect on steganalysis is not insignificant. There are three rules discussed in this paper; initially changes are allowed then dynamically corrected, the change in boundary values is allowed as a single sided and the last one is that there is no change in boundary values at all. The authors discovered that rule three was the best after experiments.

Badshah et al.[9] provided a lossless compression watermarking method to secure delicate pictures such as ultrasound, X-ray, CT scan, ECG, MRI pictures because physicians have to make a choice for therapy based on these medical records. If altered owing to noisy channel or intruder, this LZW method recovers distortion in pictures. In their research, the authors have shown that the watermark bits are reduced to reduce the total image size and are based on secret key and ROI (region of interest) to secure the medical image in tele-radiology. The authors also notified that if the watermark bits are too much reduced i.e. 0 and 1 then the quality of the image will also be degraded, thus minimizing watermark bits at optimum limits. At the receiving end, the watermark's secret keys are compared to ensure ROI, it is authentic and the image is used for medical analysis otherwise lossless image is recovered and location of temperature is required.

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 8 Issue II Feb 2020- Available at www.ijraset.com

III.METHODOLOGY

The proposed method uses has been shown block diagram shows the process flow for the encryption algorithm. The input image is read into the system which can be of any format or type e.g. colored or grayscale or .png, .jpg, tiff. etc. The image is them preprocessed to convert it into a format acceptable by the system. The cipher key is generated using the key generation algorithm and then the input image and the key is given as input to the image encryption algorithm which uses block based transformation to convert the input image into a scrambled, non-meaningful form. This is the encrypted image and it can only be useful after decryption using the same key algorithm. The encrypted image is then compressed using DWT technique to obtain compressed encrypted image.

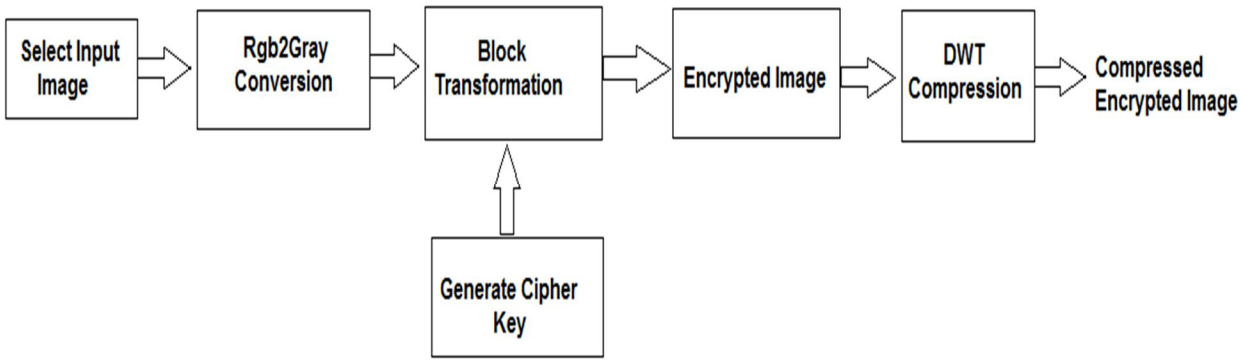


Figure 1: Block diagram of Encryption

The following is the key generation algorithm

1) Read the image size
2) Generate a zeros row vector having same number of rows as rows multiplied by columns of original image.
3) for ind = 2 : n

```
   x_N = 1 - 2* bin_x_N_Minus_1 * bin_x_N_Minus_1;
    if (x_N > 0.0)
      bin_x(ind-1) = 1;
   end
    bin_x_N_Minus_1 =  x_N;
```

4) t = uint8(0);

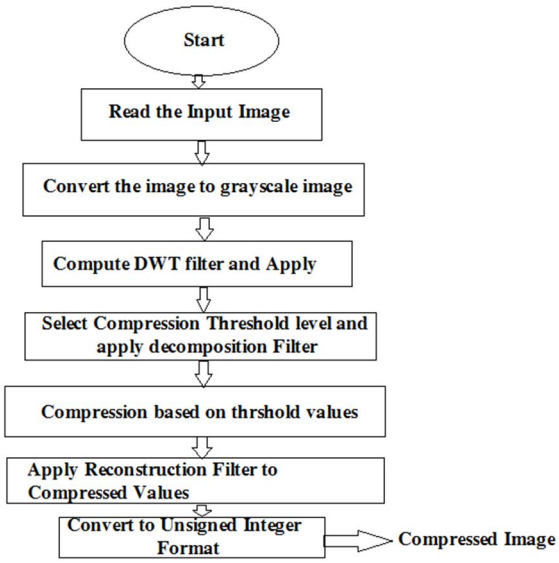
```
key = zeros(n/8,1,'uint8');
for ind1 = 1 : n/8
      for ind2 = 1 : 8
   key(ind1) = key(ind1) + bin_x(ind2*ind1)* 2 ^ (ind2-1);
end
end
```

The above algorithm generates the cipher key for each input image depending on the size of the input image.

The wavelet expansion coefficients represent a local component thereby making it easier to interpret. Wavelets are adjustable and hence can be designed to suit the individual applications. Its generation and calculation of DWT is well suited to the digital computer. They are only multiplications and additions in the calculations of wavelets, which are basic to a digital computer. The DWT compression and reconstruction step is performed on the encrypted image. The block diagram for the same is shown in figure 2.

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 8 Issue II Feb 2020- Available at www.ijraset.com



Figiure 2: DWT Compression Algorithm

The block diagram in figure 3 shows the decryption procedure. The encrypted image is input to the block transformation along with the cipher key. The bit-XOR operation is applied again on the encrypted image and the result is decrypted image, which is similar to the original input image.

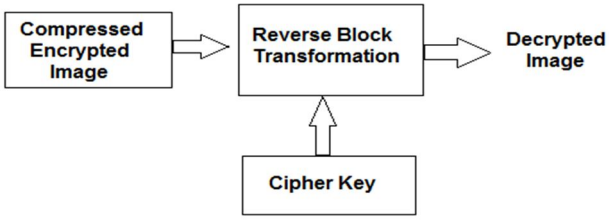


Figure 3: Decryption Process

IV. EXPERIMENTAL RESULTS

Extensive experiments have been performed on a number of images to analyse the working of the algorithm. Several standard test images such as boat, baboon, Lena, peppers, couple, cameramen etc are referred to in the present paper for watermark embedding and watermark detection. The technique is not limited to the use these cover images but we have used them as they are standard images widely used by other researchers working on watermarking. They all are images with size 256x256.

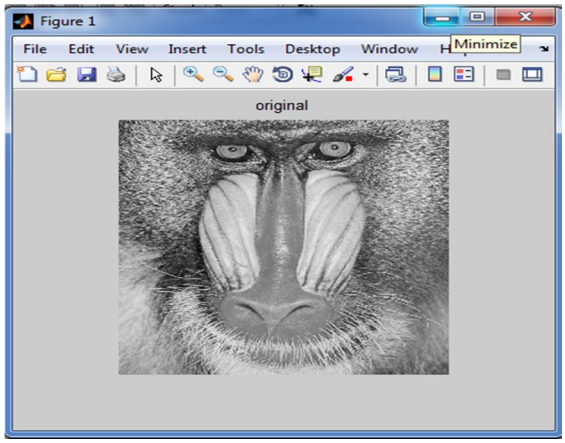


Figure 4: Original Image(Baboon)

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 8 Issue II Feb 2020- Available at www.ijraset.com

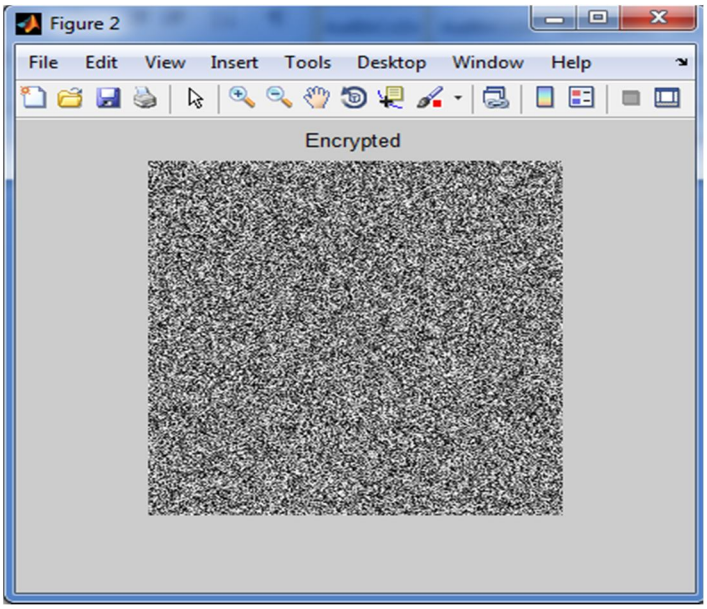


Figure 6: Encrypted Image

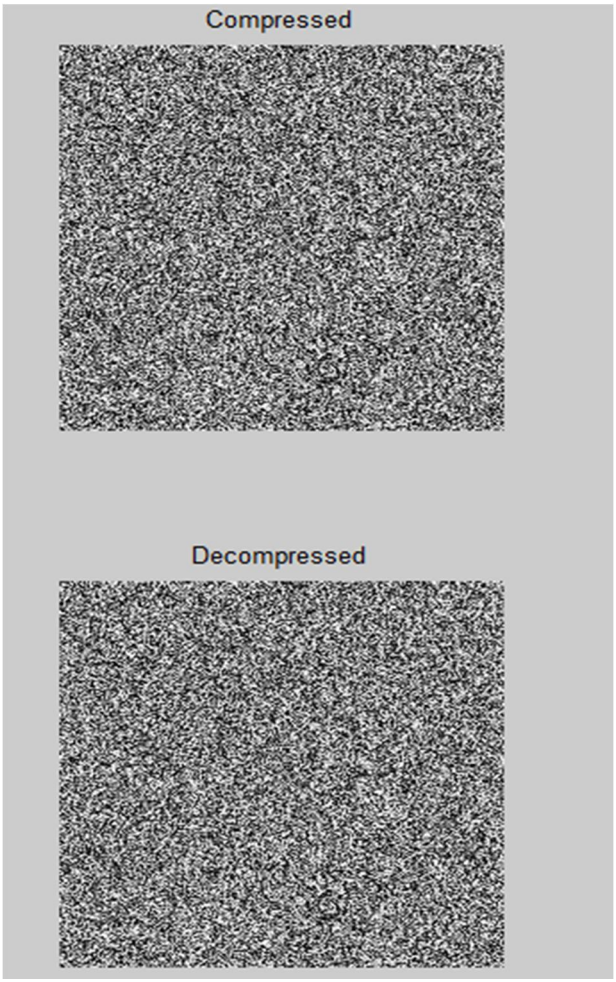


Figure 5: Compressed and Decompressed Image

©IJRASET: All Rights are Reserved

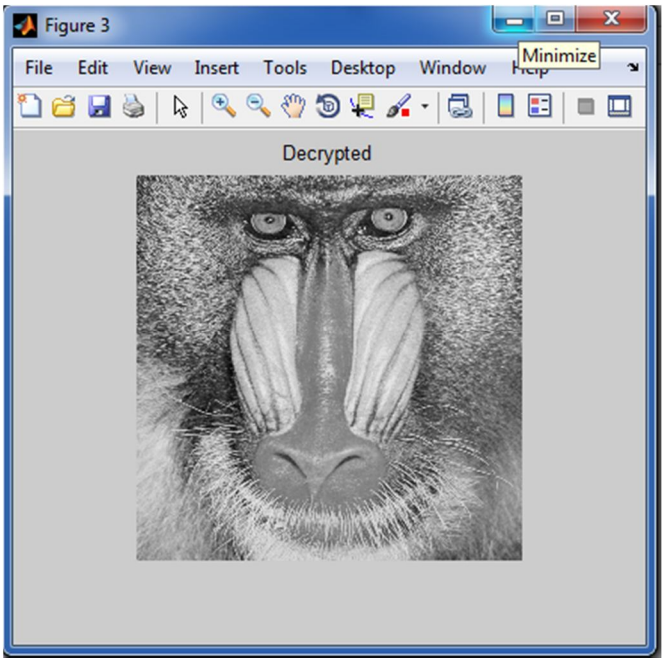


Figure 8: Decrypted Image

TABLE I: Comparison of MSE and PSNR values with other methods

Image	MSE[1]	PSNR[1]	MSE[2]	PSNR[2]	MSE[3]	PSNR[3]	MSE[4]	PSNR[4]
Baboon	13.2019	36.9244	13.5778	36.8365	17.9092	35.7074	15.8750	36.1576
Lena	11.6322	37.4742	12.1568	37.3653	16.9806	35.8653	13.9654	36.7142
Barbara	12.1947	37.2691	18.9032	35.3995	23.8694	34.3864	19.8309	35.1914
Boat	11.8868	37.3801	13.5760	36.8370	17.2098	35.8070	14.6013	36.5209
Peppers	10.8651	37.7705	12.0979	37.4139	16.2685	36.0513	13.0296	37.0155

The above table shows comparison of MSE and PSNR values obtained on standard test images of 256x256 pixels grayscale images with previous algorithms. As can be observed the proposed methods achieves better results as compared to previous algorithms.

A. Proposed Algorithm
B. Hybrid DCT-DWT encryption-decryption technique.
C. DCT based encryption-decryption technique.
D. DWT based encryption-decryption technique.

V. CONCLUSION

The primary goal of this research work was to study the various data hiding techniques and to implement an algorithm using block based cipher key image encryption algorithm combined with compression using DWT. The goal has been successfully achieved as is visible from the obtained results over a number of input images of various kinds.

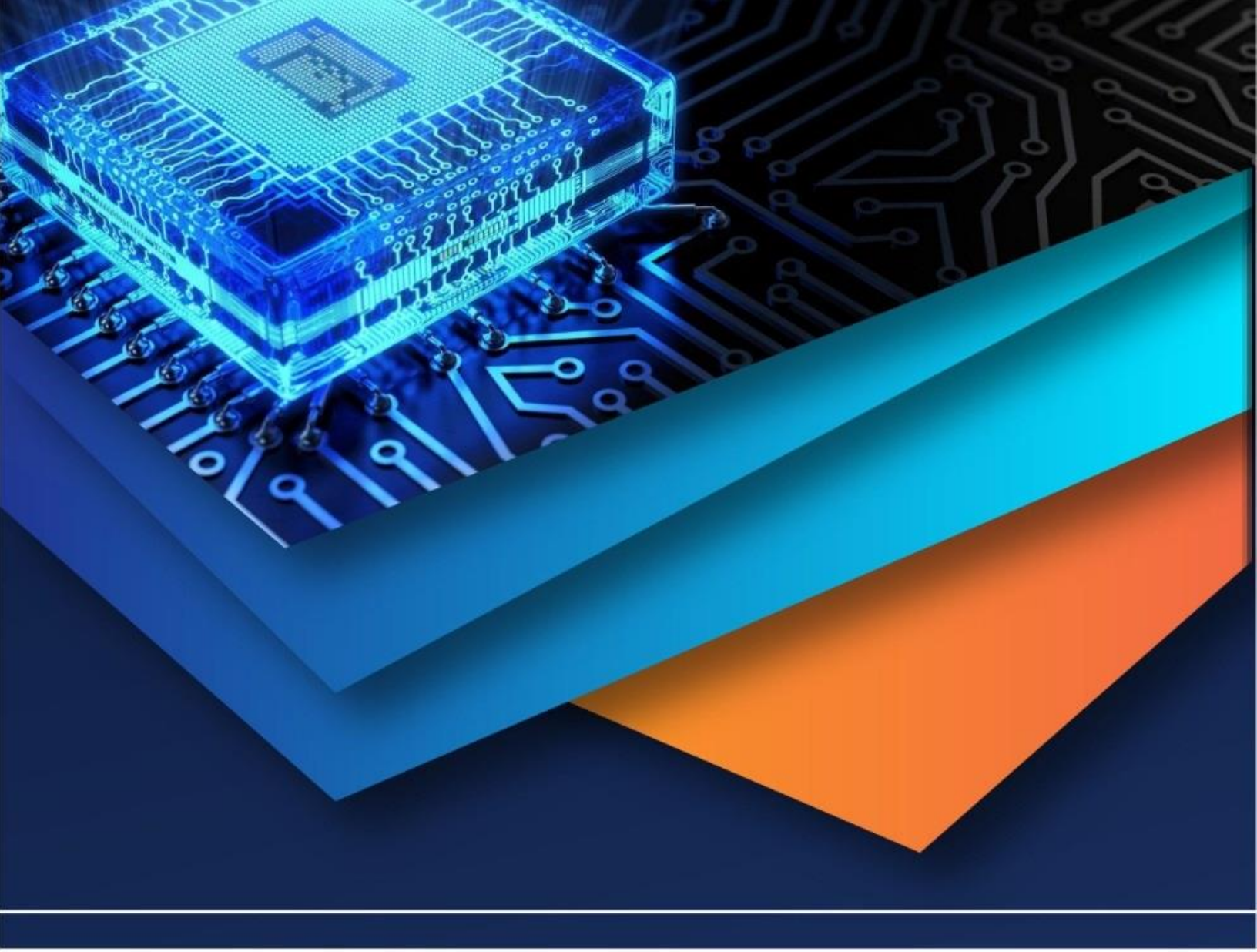
A number of data hiding techniques and their different types and methods have been studied in detail and relevant findings have been mentioned in the report. The performance parameters in terms of MSE and PSNR values have been evaluated for all the images. A high signal to noise ration demarcates feeble loss to the image quality, which is a characteristic of all the test images in this research work. All the simulation, calculation and programming used in this research work has been done using the MATLAB software and Image Processing Toolbox which provides a number of functions for quick implementation of various kinds of operations.

©IJRASET: All Rights are Reserved

REFERENCES

[1] M. A. F. Al-Husainy, "A novel encryption method for image security", International Journal of Security and Its Applications, Vol. 6, No. 1, pp. 1-8, 2012.
[2] N. A. Azam, "A Novel Fuzzy Encryption Technique Based on Multiple Right Translated AES Gray S-Boxes and Phase Embedding", Security and Communication Networks, Vol. 2017, pp. 1-9, 2017.
[3] R. J. Chen, and J. L. Lai. "Image security system using recursive cellular automata substitution", Pattern Recognition, vol. 40, pp. 1621-1631, 2007
[4] A. Pushpad, A. A. Potnis, and A. K. Tripathi, "A Review on Current Reversible Image Security Schemes", Imperial Journal of Interdisciplinary Research, Vol. 2, Issue. 11, pp. 953-955, 2016.
[5] A. Verma, and A. Jain, "Pixel chaotic shuffling and Arnold map based Image Security Using Complex Wavelet Transform", Journal of Network Communications and Emerging Technologies, Vol. 6, Issue 5, pp. 8-11, 2016.
[6] W. Wang, H. Tan, Y. Pang, Z. Li, P. Ran, and J. Wu, "A novel encryption algorithm based on DWT and multichaos mapping" journal of sensors, Vol. 2016, pp. 1-7, 2016.
[7] N. Garg, and K. Kaur, "Hybrid information security model for cloud storage systems using hybrid data security scheme", International Research Journal of Engineering and Technology, Vol. 3, Issue 4, pp. 2194-2196, 2016.
[8] V. Sedighi, and J. Fridrich, "Effect of saturated pixels on security of steganographic schemes for digital images", IEEE International Conference on Image Processing (ICIP), Phoenix, Arizona, USA, September 2016.
[9] G. Badshah, S. C. Liew, J. M. Zain, and M. Ali, "Watermark compression in medical image watermarking using Lempel-Ziv-Welch (LZW) lossless compression technique", Journal of Digital Imaging, Vol. 29 No..2 pp. 216-225, 2016.

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)