The Pharma Innovation Journal 2019; 8(3): 11-18

www.ThePharmaJournal.com

The Pharma Innovation

ISSN (E): 2277- 7695
ISSN (P): 2349-8242
NAAS Rating: 5.03
TPI 2019; 8(3): 11-18

www.thepharmajournal.com
Received: 06-01-2019
Accepted: 10-02-2019

Afseen Bano
Department of Computer Science, Sam Higginbottom University of Agriculture Technology and Sciences, Allahabad, Uttar Pradesh, India

Prateek Singh
Assistant Professor, Department Of Computer Science, Sam Higginbottom University of Agriculture Technology and Sciences, Allahabad, Uttar Pradesh, India

Correspondence
Afseen Bano
Assistant Professor, Department Of Computer Science, Sam Higginbottom University of Agriculture Technology and Sciences, Allahabad, Uttar Pradesh, India

Image encryption using block based transformation algorithm

Afseen Bano and Prateek Singh

Abstract
Digital images are widely communicated over the Internet. The security of digital images is an essential and challenging task on shared communication channel. Various techniques are used to secure the digital image, such as encryption, steganography and watermarking. These are the methods for the security of digital images to achieve security goals, i.e. confidentiality, integrity and availability. Individually, these procedures are not quite sufficient for the security of digital images. This research presents a novel approach of encrypting the images. It comprises of three key components. The original image has been encrypted using large secret key by rotating pixel bits to right through XOR operation. For steganography, encrypted image has been altered by least significant bits (LSBs) of the cover image and obtained stego image, then stego image has been watermarked in the time domain and frequency domain to ensure the ownership. The proposed approach is efficient, simpler and secured; it provides significant security against threats and attacks. The results have been evaluated in terms of PSNR and MSE and comparative analysis with other popular existing methods has been performed.

Keywords: PSNR, MSE, encrypting & decrypting image

1. Introduction
A number of digital services are available now a days for the consumers to use. An important concern is that they require reliable security during the storage and transmission of digital images. Owing to the rapid growth of the internet in the digital world today, the security of digital images becomes most important and hence is acquiring much attention. The omnipresence of multimedia technology in our society (Rew S, 1998) has promoted digital images to play a more significant role than the traditional texts, which demand serious protection of users' privacy for all applications. Encryption and steganography are the two noteworthy techniques of digital images protection and security which are very important and should be used to frustrate opponent attacks from unauthorized access.

Digital images can be possibly exchanged over various types of networks. And in most of the cases it is often true that a large part of this information is either confidential or private. Encryption is the preferred technique for protecting the transmitted data. There are various encryption systems to encrypt and decrypt image data, however, it can be argued that there is no single encryption algorithm which satisfies the different image types single handedly. In general, most of the available encryption algorithms are used for text data. However, due to large data size and various real time constrains, algorithms that are good for textual data may not necessarily be suitable for multimedia data.

Prior to the modern age the Cryptography was known as encryption, the conversion of information from a readable state to unreadable state. The creator of an encrypted message share the decoding technique only to the intended user needed to recover the original information, thereby prevent unwanted persons to decode information.

Digital images are the most widespread cover files used for SG due to the insensitivity of the human visual system (HVS) (A. Almohammad, 2010) [1]. During the embedding stage, a key is used to insert a message in a cover medium resulting in a stego-object as shown in Figure 2-1. The stego-object is then transmitted along public channels to its destination. When the stego-object is received, the embedded message is extracted from stego-object using the known stego-key.

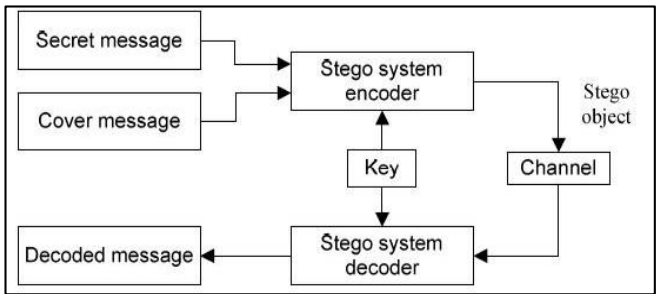


Fig 1.8.1: A general steganographic Model

Steganography has become an interesting and challenging field of research striving to achieve greater immunity of hidden data against signal processing operations on the host cover media; e.g. a good SG technique should offer immunity of hidden data against lossy compression, scaling, interception, modification, or removal etc. and ensure that embedded data remains inviolate and recoverable (F. A. P. Peticolas, 1999) [2]. However, a trade-off between the quantity of hidden data and its degree of immunity to host signal modification is needed in most cases (H. V. Singh, 2006) [3].

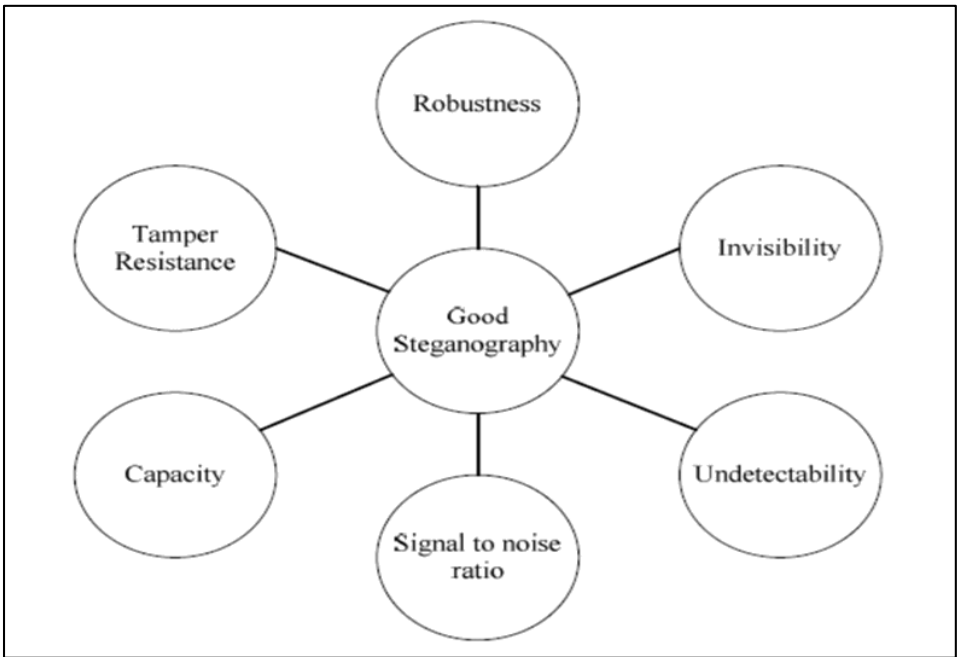


Fig 1.8.1: Properties of a good steganographic technique

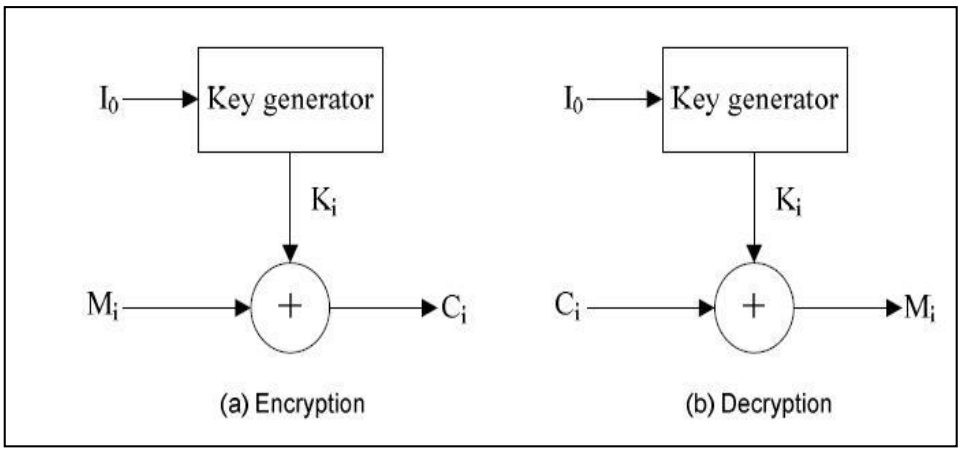


Fig 1.8.5: Block Diagram of Stream Encryption

In a self-synchronous stream cipher, each key character is derived from a fixed number, n, of the preceding cipher text characters, giving rise to the name cipher feedback. In such a system, if a cipher text character is lost during transmission, the error propagates forward for n characters, but the system resynchronizes itself after n correct cipher text characters are received. The block diagram of synchronous stream encryption is as shown in Figure 2.5.

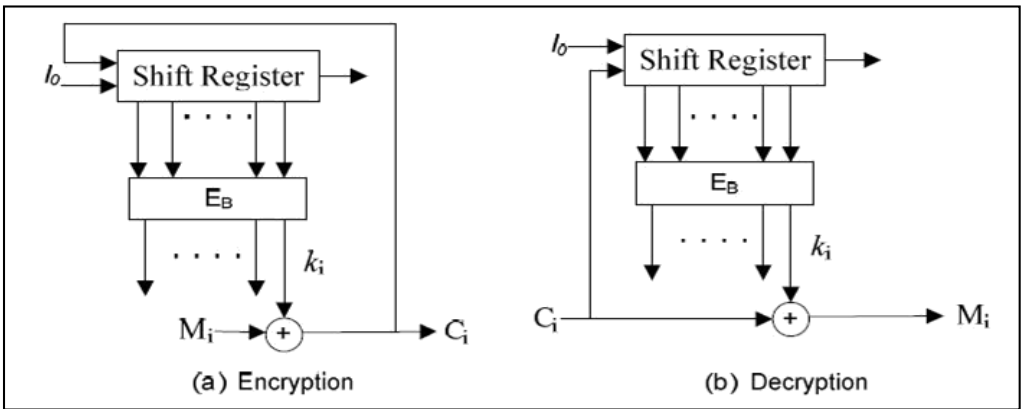


Fig 1.8.5: Block diagram of self-synchronous stream cipher

The pseudo-random numbers can be generated either by using hardware or software. The simplest way of generating the pseudo-random number sequence using hardware is by making use of linear feedback shift registers, which can be used in stream ciphers, and are well suited to low power or high speed requirements. Using software, RC4 is one of the ways of generating the pseudo random number sequence. As with any stream cipher, these can be used for encryption by combining it with the plain text using bit-wise exclusive-or operation. These bits are similar to the Vernam cipher except that generated pseudo random bits, rather than prepared stream, are used.

1.12 Motivation

Image encryption has applications in internet communication, multimedia systems, medical and military imaging systems. Each type of multimedia data has its own characteristics such as high correlation among pixels and high redundancy. Thus, different techniques should be used to protect confidential image data from unauthorized access. The motivation behind this research is the ever-increasing need for harder-to-break encryption and decryption algorithms as the computer and network technologies evolve. It is commonly believed that the block-based encryption and decryption algorithm helps to reduce the relationship among image elements by increasing the entropy value of the encrypted images as well as lowering the correlation. A block cipher is used to encrypt a text to produce a cipher text, which transforms a fixed length of block data size into same length block of cipher text in which a secret key and algorithm are applied to the block of data. Thus, it can be effective in providing a robust encryption and decryption method in case of images.

Materials and Methods

Image encryption scheme have been increasingly studied to meet the demand for real-time secure image transformation over the internet and through wireless network. Many researchers have put their efforts in this area. Numerous algorithm have been proposed and investigated which includes permutation – substitution scheme, which is based on chaotic standard map enhanced blowfish algorithm. A digital image is defined by an array of individual pixels and each pixels has its own value. The array, and thus the set of pixels, is called a bitmaps. If we have an image of 512 pixels* 512 pixels, it means that the data for the image must contain information about 262144 pixels. An image is the two dimensional (2-D) picture that gives appearance to a subject usually a physical object or a person. It is digitally represented by rectangular matrix of dots arranged in row and columns. Each pixel of the images is divided into smaller blocks. If a pixel is divided into two parts one is black and one is white block. If pixel is divided into four equal parts, there are two white and two black blocks. If pixel is divided into 8 equal part, there are four white and four black blocks.

2.1 Matlab

MATLAB stands for Matrix laboratory and is a high-performance language for technical computing. It integrates computation, visualization, and programming in an easy-to-use environment where problems and solutions are expressed in familiar mathematical notation.

2.1.1 Matlab Simulator

The name MATLAB stands for Matrix Laboratory. MATLAB was originally made to provide easy access to matrix software developed by the LINPACK and EISPACK projects. Today, MATLAB engines incorporate the LAPACK and BLAS libraries, embedding the state of the art in software for matrix computation.

2.2 Image Encryption

Image encryption algorithm based on s-boxes substitution and chaos random sequence, image encryption based on ASE encryption algorithm and digital signal processing technology, method for image encryption, digital watermarking technique to resolve the rightful ownership of digital image using block cipher RC6 and secure JPEG2000 encryption techniques based on arithmetic coding.

In this research work image encryption tries to convert an image into coded image that is hard to understand.

2.2.1 Encryption Block diagram

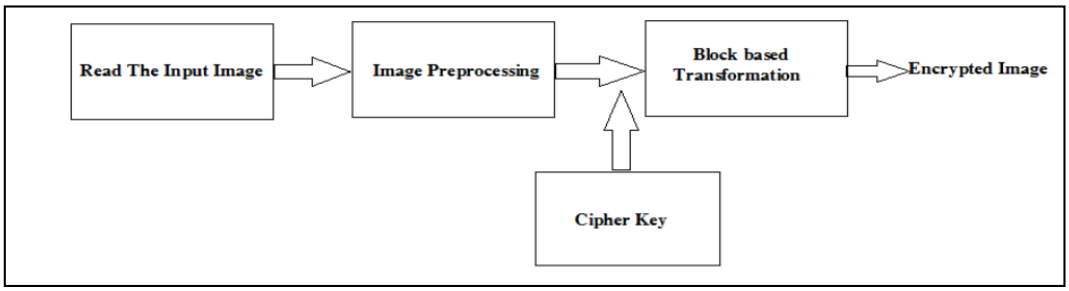
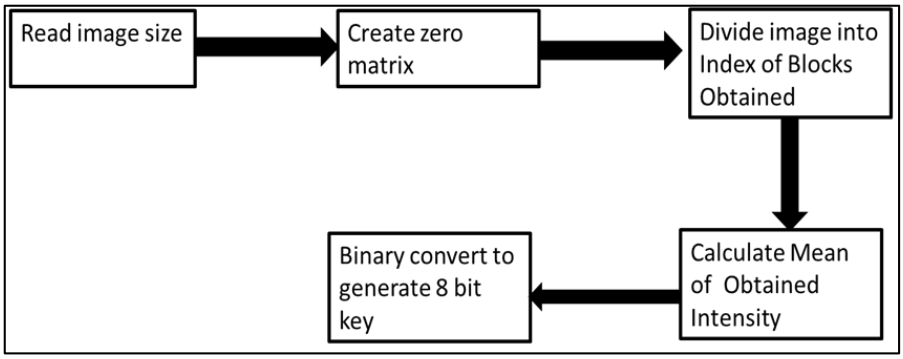


Fig 2.2.1: Encryption Block Diagram

2.2.2 Proposed encryption algorithm



Algorithm block diagram

2.2 Block Transformation

The block based transform is described by the block diagram shown in figure 3.2. As shown in the block diagram, the input image and cipher key generated is combined using the XOR operation, which finally results into the encrypted image.

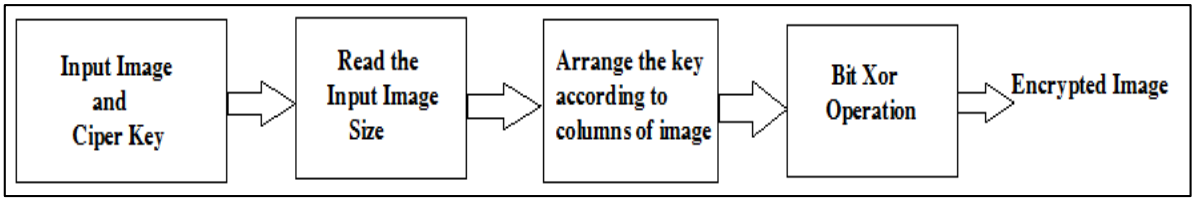


Fig 2.3: Block transformation

3.3.2 Bit Xor Example

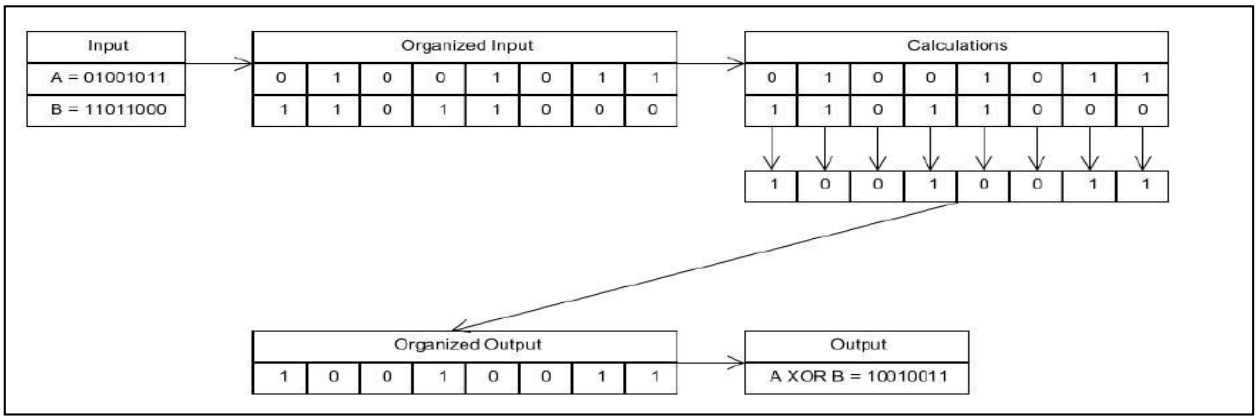


Fig 2.3.1: Bit XOR Example

2.4 Proposed Decryption Technique

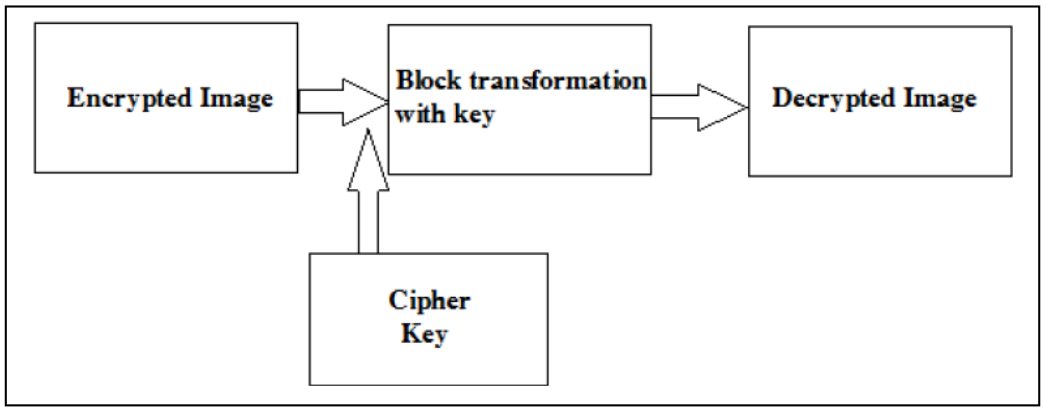


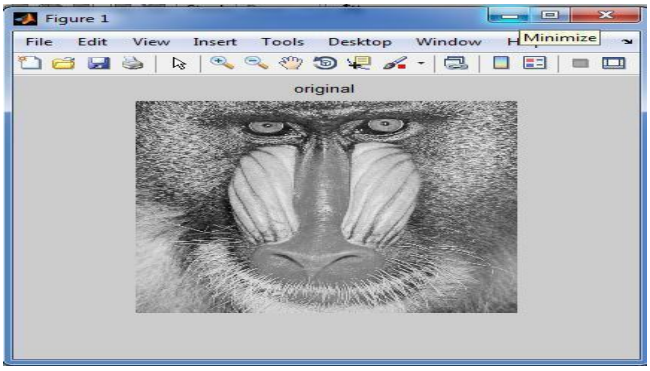
Fig 2.6: Decryption process

Result and Analysis

The algorithm described in the above chapter has been implemented in MATLAB software version MATLAB7.10, R2010a. The below section gives a description of the MATLAB software.

3.7 Implementation 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.



Case 1: Baoon.png

Figure 3.2: Input Image (Baboon)

The figure 4.1 shows the baboon image. It is a grayscale image with 256x256 pixels. The below figure 4.3 and 4.4 correspondingly show the results after encryption and decryption.

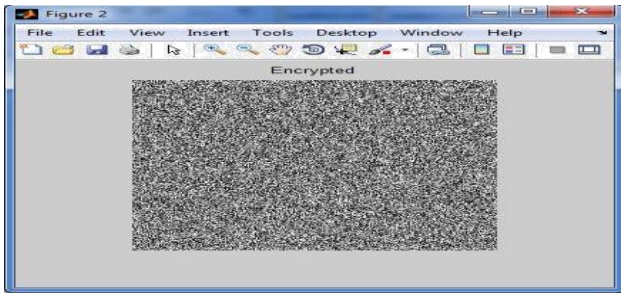


Fig 4.3: Encrypted Image (baboon)

As is visible from figure 4.3 the encrypted image is srambled and it is impossible to retreive the actual image hidden inside it, without the cipher key. So while transmision on the network if an attacker or hacker tries to hack the image, he would not be able to retreive the actual image.

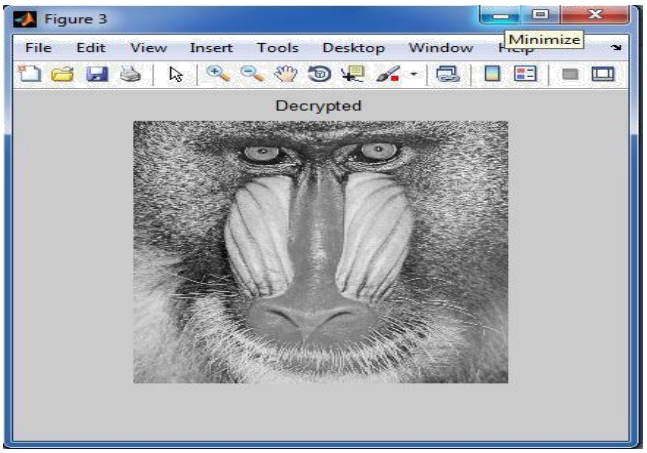


Fig 3.4: Decrypted Image (baboon)

Case 2: Lena.png

The second image is that of Lena which is a 256x256 pixel size colored image. The results obtained after encryption and decryption are as shown below:

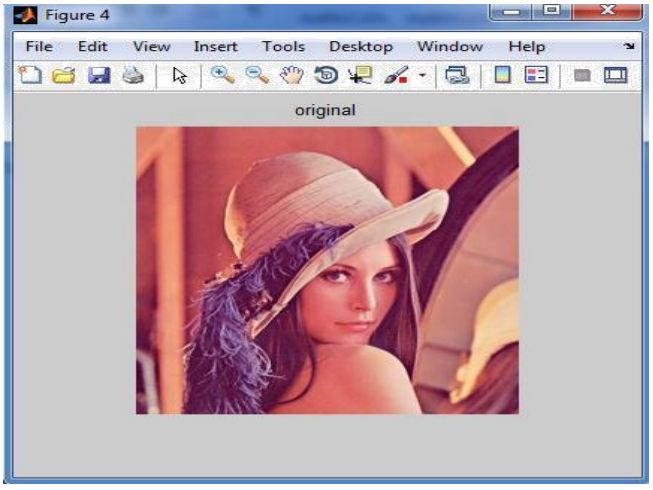


Fig 3.5: Input Image (Lena)

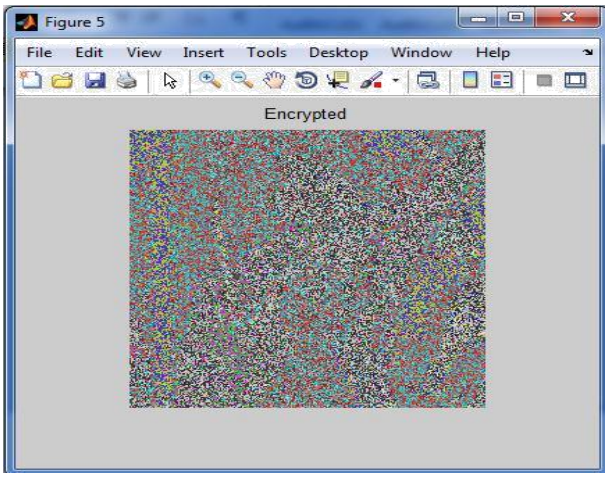


Fig 4.6: Encrypted Image (Lena)

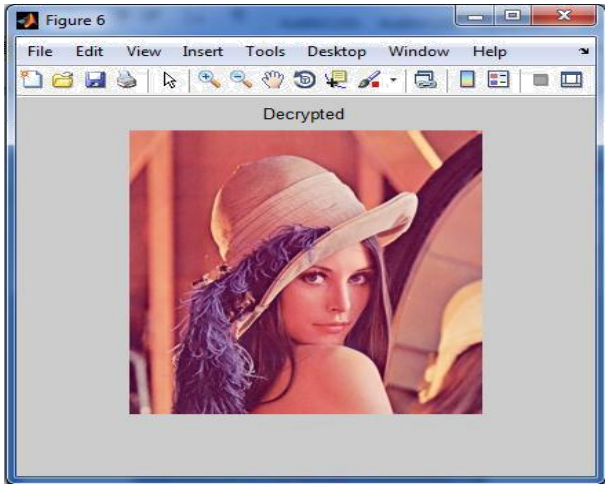


Fig 4.7: Decrypted Image (Lena)

Thus the proposed method in this research work shows good results for both colored and grayscale images.

3. 8 Performance Evaluation

The performance metrics such as MSE, PSNR are tested on various images are mean square arror and PSNR (Peak signal to Noise ratio)

MSE: Mean square error

MSE is the difference between the original image and the encrypted image. This difference must be very high for a better performance.

MSE = (1/MN)*(original image-encrypted image)

The MSE is a measure of the quality of an estimator – it is always non – negative, and values closer to zero are better. The MSE is the variance of the estimator like the variance, MSE has the same units of measurement as the square of the quality being estimated.

PSNR: Peak Signal to Noise Ratio

PSNR is the ratio of peak signal power to noise power. It is measured for image quality. For a good encrypted image the value of PSNR must be low.

PSNR=10log10 (I2max /MSE) Db

Where, Imax is the maximum intensity of image

PSNR is most easily defined via the mean squared error (MSE). Given a noise – free mxn monochrome image I and its noisy approximation K, MSE is defined as; the PSNR (indB) is defined as; Here, MAX, is the maximum possible pixel value of the image.

Performance metrics with capacity and various images are analyzed in the following table. Performance Analysis-Mean Square Error (MSE) and Peak signal to noise ratio (PSNR) is depicted in Table 4.1 and Table 4.2 shows the overall time taken by the proposed method to encrypt as well as to decrypt the image.

Table 3.1 Comparison of MSE and PSNR values with different algorithm

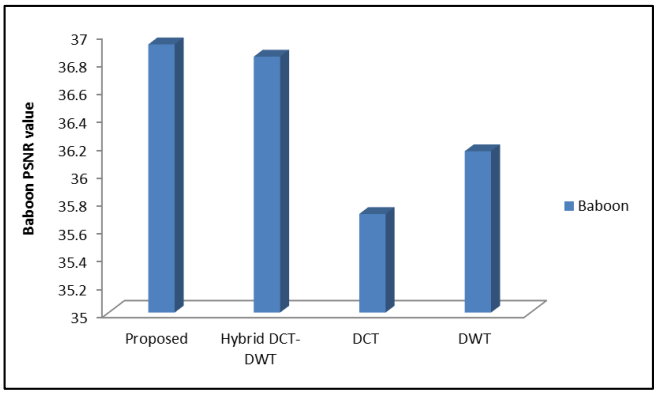
Peak signal to noise ratio (PSNR) and mean square error (MSE) are used to comparing the squared error between the original image and the reconstructed image there is am inverse relationship between PSNR and MSE so a higher PSNR value indicates the higher quality of the image (better). It is easy to evaluate and calculate the value for all the images.

Table 3.1: Comparison of MSE and PSNR values with different algorithms

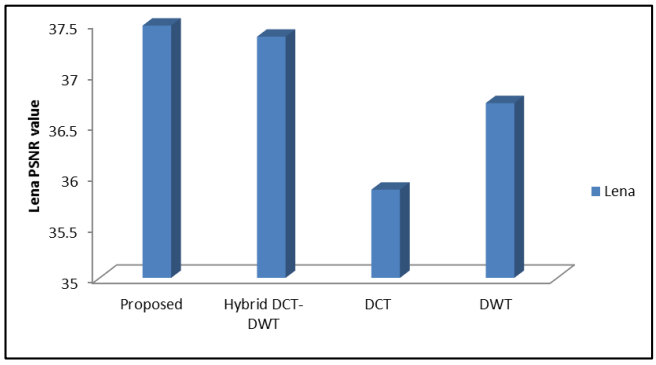
Image	MSE[1]	PSNR[1]	MSE[2]	PSNR[2]	MSE[3]	PSNR[3]	MSE[4]	PSNR[4]
Baboon	13.2019	36.9244	13.5778	36.8365	17.9092	35.7074	15.8750	36.1576
Lena	11.6322	37.4742	12.1568	37.3653	16.9806	35.8653	13.9654	36.7142
Barbara	12.1947	37.2691	18.9032	35.3995	23.8694	34.3864	19.8309	35.1914
Boat	11.8868	37.3801	13.5760	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

PSNR: Peak signal to noise ratio and **MSE:** mean square error

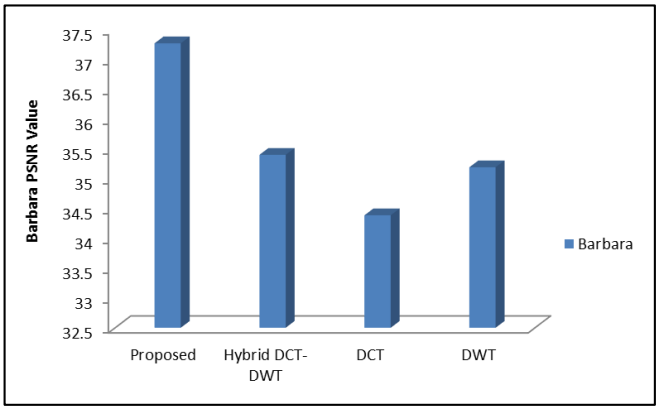
Comparison PSNR values for Different Methods



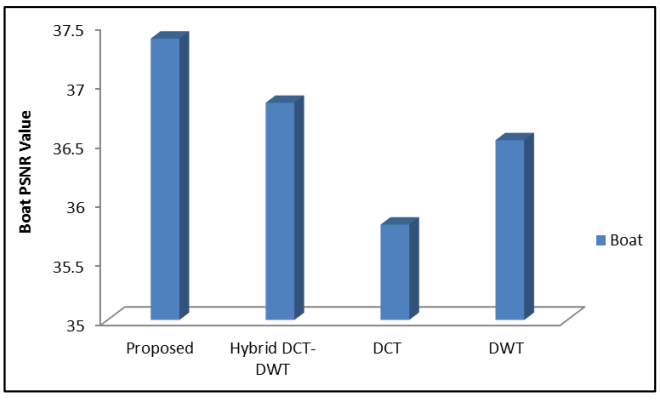
Baboon



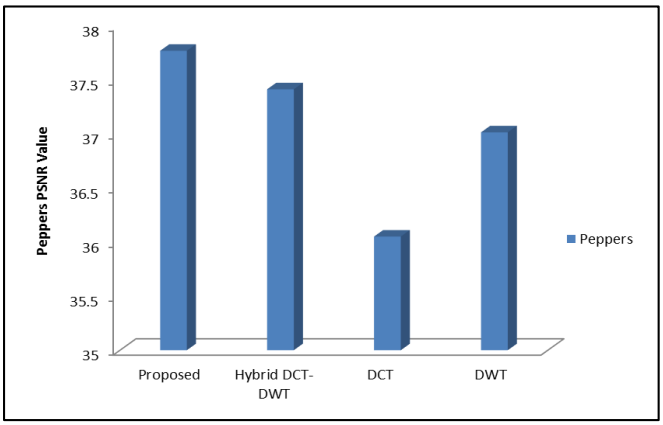
Lena



Babara



Boat



Peppers

Fig 3.8: Comparison PSNR values for Different Methods

3.9 Analysis

The implementation results were obtained on two images one baboon and another lena which are grayscale and colored image respectively. The algorithm shows acceptable levels of perceptibility and image quality also remains good after decryption.

The graph above shows a comparison of Peak Signal to Noise Ratio of the different methods and compared with the proposed method for different images. As can be observed from the graph the proposed method shows better PSNR values as compared to Discrete Wavelet Transform, Discrete Cosine Transform and Hybrid of both DCT and DWT. The higher PSNR values ensure that the proposed method means the image quality of the encrypted image is better as compared to the previous papers. The higher PSNR values indicate higher quality of encrypted image whereas the lower PSNR values indcate lower quality. The Mean Square Error needs to be lesser for better quality of images.

4.1. Conclusion

This research work was to study the various data hiding techniques and to implement an algorithm using block based cipher key image encryption algorithm. The algorithm has been successfully applied to and tested for the image encryption although the algorithm presented in this thesis has focused on image encryption. It can be seen from the result that the proposed system offers a higher complex city. 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. The perceptibility and image quality after decryption for both colored and grayscale images was found to be excellent and no trails of image modification is evidently visible. The MSE and PSNR have been evaluated which give an mathematical analysis of the research work.

This research present a novel approach of encrypting the image. It comprises of three key components the original image has been encrypted using large secret key by rotating pixel bits to right through XOR operation, for steganography, encrypted image has been altered by last significant bits (LSBs) of cover image and obtained stego image than stego image has been water mark in the time domain frequency

domain to ensure the ownership.

5.3 Future work

Future work in this direction could be exploiting other ways to improve the utilization of public images for secure communication. The encryption and decryption technique proposed can be used as a robust data hiding technique, if the number of bits to decrypt the message is further reduced. Moreover, if both data encryption and steganography are used together, the data security can be highly improved. Future work also includes implementing the proposed stream encryption algorithms in hardware to test its speed.

6. References

1. Almohammad, Ghinea G. Image steganography and chrominance components, Proc. IEEE Int. Conf. on Computer and Information Technology, Bradford, UK, 2010, 996-1001.
2. Peticolas AP, Anderson RJ, Kuhn MG. Information Hiding: A Survey, Proc. IEEE, 1999; 87(7):1062-1078.
3. Singh HV, Singh AK, Balasubramanian SK, Mohan A. Minimizing Security Threats in Multimedia Systems, Second Int. Conf. Distributed Frameworks for Multimedia Applications, Penang, Malaysia, 2006, 1-5.
4. Rueppel A. Analysis and Design of Stream Ciphers, Springer-Verlag, Berlin, 1986.
5. Abhinav Srivastava. A survey report on Different Techniques of Image Encryption. International Journal of Emerging Technology and Advanced Engineering. 2012; 2(6).
6. Ahmed Bashir Abugharsa, Abd Samad Bin Hasan Basari, Hamida Almangush. A New Image Encryption Approach using Block-Based on Shifted Algorithm. International Journal of Computer Science and Network Security. 2011; 11(12).
7. Ankit Gupta, Namita Tiwari, Meenu Chawla, Madhu Shandilya. An Image Encryption using Block based Transformation and Bit Rotation Technique. International Journal of Computer Applications (0975-8887), 2014.
8. Ankita Gaur, Maneesha Gupta. Review: Image Encryption Using Chaos Based algorithms. Journal of Engineering Research and Applications www.ijera.com ISSN: 2248-9622, 2014; 4(3):904-907.
9. Artz. Digital steganography: Hiding data within data, IEEE Internet Computing. 2001; 5(3):75-80.
10. Behnia A, Akhshani H, Mahmodi, Akhavan A. A novel algorithm for image encryption based on mixture of chaotic maps, Chaos, Solitons & Fractals. 2008; 35:408-419.