DATA HIDING IN ENCRYPTED IMAGES

Vikas Kumar[1]
Ms Sonu Rana[2]
Global Institute Of Technology and Management Farrukhnagar [1, 2]
Department Of Electronics and Communication Engineering

1. Introduction

Nowadays, information security is becoming more important in data storage and transmission. Information security is needed where company needs to ensures their customers about the security of their information. No one company can afford the loss and negative publicity that could occur because of weak security. It is worth to know that weak security means an organization could be on the loss of money in operations.

1.1 Data Hiding

It was assumed that encryption is the best method to secure data, but researchers have proved the fact that hiding the data is far secured than encrypting the same data. Because encrypted data gives a clear picture to a criminal mind that implementation of certain hacking techniques can break the encryption.

1.3 Uses of Data hiding

1. Data hiding can be a solution which makes it possible to send news and information without being censored and without the fear of the messages being intercepted and traced back to us.

2. It is also possible to simply use data hiding technique to store information on a location. For example, several information sources like our private banking information, some military secrets, can be stored in a cover source. When there is any requirement to unhide the secret information in cover source, it can easily reveal the banking data and it will be impossible to prove the existence of the military secrets inside.

Before the invention of digital means, traditional methods were being used for sending or receiving messages. Before phones, before mail messages were sent on foot. For the messages where privacy was of prime concern, the ways of implementing security were following:

1. Choosing the messenger capable of delivering the message securely.

2. Write the message using such notations that actual meaning of the message was concealed.

3. Hide the message such that even its presence can’t be predicted.

1.4 Advantages & Disadvantages

Advantages:

1. The data hiding and image encryption are done by using same keys i.e. for encryption data hiding.

2. The receiver who has data hiding key can retrieve the data embedded.

1.5 Disadvantages:

1. The secret key used for encryption of compressed image and data hiding is the same. So the user who knows the key used for the encryption can easily access the data embedded and original image.

2. The original can be retrieved from the encrypted image after extracting or removing the data hidden in the image.

3. The content and data hider share the same encryption key for encryption of image and data hiding.

2. Literature Survey

Xizang in [1] proposed a novel reversible data hiding scheme for encrypted image. After encrypting the entire data of an uncompressed image by a stream cipher, the additional data can be embedded into the image by modifying a small proportion of encrypted data. With an encrypted image containing additional data, one may firstly decrypt it using the encryption key, and the decrypted version is similar to the original image.

L.Xuemeiet. al. in [2] proposed The Hilbert transform and the double random phase encoding are utilized in the proposed method. The encrypted image is real-valued without data expanding, which can benefit the digital processing of images by electronic computers where speed of computation is important. The image is processed in the plane which can be regarded as different fractional Fourier domain.

S.Bhowmiket.al.in [3] proposed The Genetic Algorithm (GA), an important method of artificial intelligence has been applied to generate encryption ‘key’, which plays a vital role in any type of encryption. In this work, a hybridized technique called Blowgun is also proposed which is a combination of Blowfish and GA. Blowfish Algorithm is a conventional method of encryption.

Y.Wuet. al. in [4] proposed a wheel-switch chaotic system for image encryption. The used chaotic map is not fixed but changeable via the wheel-switch structure according to the controlling sequence. Further, a substitution and permutation network based image encryption algorithm using the wheel-switch chaotic system is also provided.

ManieKansalet.al. in [5] proposed The Digital image watermarking algorithm based on DWT, DCT and SVD has been proposed in which Arnold transform has been applied to watermark image in order to ensure the watermark robustness. The proposed algorithm is robust to the common image process such as JPEG compression and other attacks like noise and filters.

G.S. Yadavet.al. In [6] proposed a simpler method for data hiding in binary images that reduces the time complexity of the algorithm to O(n) while keeping the distortion low. Use a twofold encryption by inserting the data in the image using block pattern encoding and then using XOR operation to increase the security of the data. The proposed algorithm follows a greedy approach which takes into consideration the local minimum cost of bit replacement leading to a significant difference in the execution time.

G.A.Sathishkumaret.al. in [7] proposed a new image encryption algorithm using random pixel permutation based on chaos logistic maps and prime modulo multiplicative linear congruential generators. The random-like nature of chaos is effectively spread into the encrypted image through permutation and transformation of pixels in the plain image. The pixel transformation results in the encryption scheme being resistive to cryptanalytic attacks. Simulation results show high sensitivity to key, plaintext and cipher text changes.

3. Problem Definition

In above literature survey, it has been seen data hiding in image data is one of the major research issue. In recent, many algorithms have been proposed. Most of algorithms are too complex to implement, in which complex transformation techniques are used. As mentioned DCT is one of easy transformation to use, which is commonly used for image compression. When data is hiding in an image, there may be some changes in the pixel values. Small changes in an image can be neglected, but if the difference is large in the values will not accepted and degrade the quality of image. The main motive is to develop an alternative algorithm for reversible data hiding in encrypted image using DCT transform and reduce the noise and improves the quality of image. The quality of image can be improved by maximizing the Peak Signal to Noise ratio and minimizing the Mean Square Error and Bit Error Rate. Smaller the extraction error rate there should be greater the quality of image.

4. Objective of Dissertation

The main objective of this scheme is to recover the data embedded in the image. The data of original image are entirely encrypted by using Discrete Cosine transform by finding the noisy pixels or higher frequencies and then applying closest match approach. This work proposes a novel reversible data hiding scheme for encrypted image, which is made up of image encryption, data embedding and data-extraction/image-recovery phases. The data of original cover are entirely encrypted, and the additional message is embedded by modifying a part of encrypted data. At receiver side, with the aid of spatial correlation in natural image, the embedded data are successfully extracted while the original image is perfectly recovered. With an encrypted image containing embedded data, a receiver may firstly decrypt it using the encryption key, and the decrypted version is similar to the original image. According to the data-hiding key, with the aid of spatial correlation in natural image, the embedded data can be correctly extracted while the original image can be perfectly recovered. For ensuring the correct data-extraction and the perfect image recovery, we may introduce error correction mechanism before data hiding to protect the additional data with a cost of payload reduction.

Overview of the objectives is as follows:

1. To generate key for hiding data.
2. To develop reversible data hiding algorithm using DCT.
3. To improve the quality of image.
4. To evaluate the percentage of quality decreased with hiding given number of data.

5. Proposed Method

This technique is based on encryption as well as decryption. Encryption is the process of encoding messages (or information) shown in such a way that eavesdroppers or hackers cannot read it, but that authorized parties can. In an encryption scheme, the message or information (referred to as plaintext) is encrypted using an encryption algorithm, turning it into an unreadable cipher text. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Any adversary that can see the cipher text should not be able to determine anything about the original message.

5.1 Results and Discussion

This work proposes a novel reversible data hiding scheme for encrypted image, which is made up of image encryption, data embedding and data-extraction/image-recovery phases. The data of original cover are entirely encrypted, and the additional message is embedded by modifying a part of encrypted data. At receiver side, with the aid of spatial correlation in natural image, the embedded data are successfully extracted while the original image is perfectly recovered. Here four gray level images of size 512×512, including Lena, Baboon, Sailboat, and Splash are taken as the test images, as shown in Fig. 4.1.This technique is based on two methods: Encryption and Decryption. The experimental results are compared with [36] shown in figure below.

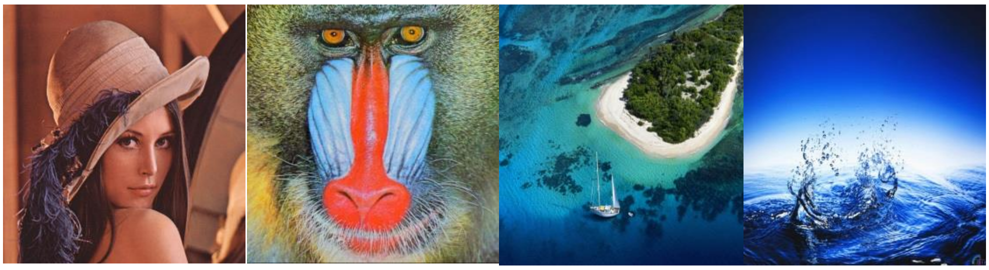
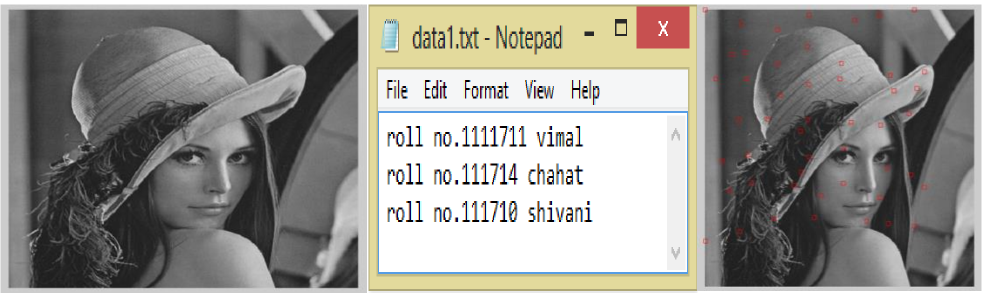


Fig. 4.1 Four test images (a) Lena (b) Baboon (c) Sailboat (d) Splash

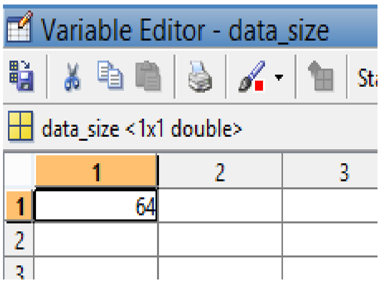
To demonstrate the performance of the proposed method, let take Lena image as an example. In encryption, first of all the image is loaded in the mat lab shown in fig.4.2(a) and then reading data which is to be hide in the image which is shown in fig. 4.2(b). Fig.4.2(c) shows the encrypted Lena image with data hidden in it.



roll no.1111711 vimal
roll no.111714 chahat
roll no.111710 shivani

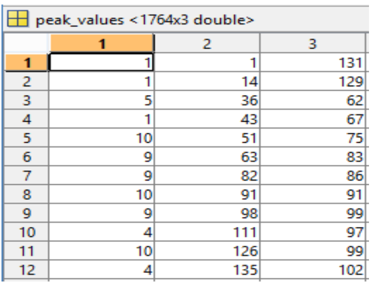
Fig.4.2 (a) Lena image (b) Data (c) Encrypted image with hidden data

Size of data is then calculated shown in Fig. 4.3(a) and then finding noisy pixels by applying DCT shown in Fig. 4.3(b) after thatpsnr is calculated for different blocks for Lena image shown in Table.4.1 to check the quality of image at different block sizes. Then by saving key and encrypted image, decryption process is done.



data_size <1x1 double>

	1	2	3
1	64		
2			
3			



peak_values <1764x3 double>

	1	2	3
1	1	1	131
2	1	14	129
3	5	36	62
4	1	43	67
5	10	51	75
6	9	63	83
7	9	82	86
8	10	91	91
9	9	98	99
10	4	111	97
11	10	126	99
12	4	135	102

Fig. 4.3 (a) Calculating data size (b) Finding noisy pixels

Table 4.1 Block size v/s PSNR and BER for Lena image

Block Size	Peak signal to noise ratio	Bit error rate
12	97.5450	0
22	82.1459	0
32	74.2273	0
42	69.1523	0
52	62.2005	0
62	55.0961	0
64	54.2725	8.5938

In Decryption process, first of all the saved encrypted image is loaded and then saved key. After that, calculation of Bit Error Rate is done. The calculated BER is shown in Table 4.1.The graph of PSNR of Lena image is shown in Fig 4.4 (a) which shows that as the block size increases the PSNR decreases and BER are shown in and Fig 4.4(b)

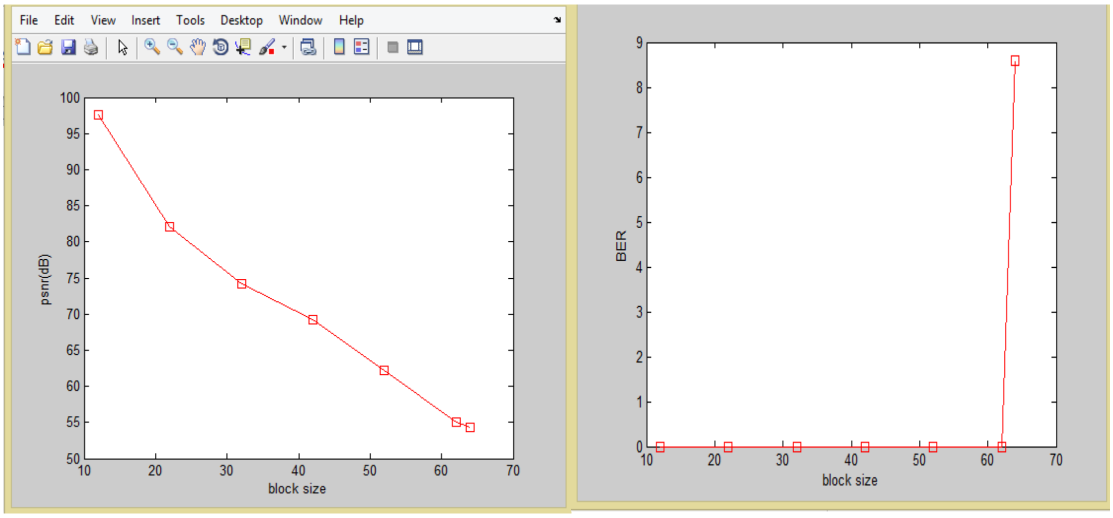


Fig. 4.4(a) Block size v/s PSNR (b) Block size v/s BER of Lena image for different blocks

Now the same procedure of encryption and decryption is done for Baboon image. After applying the method of encryption and decryption, the calculated PSNR and BER is shown in Table 4.2.which shows that as the block size increases, PSNR decreases.

Table 4.2 Block size v/s PSNR and BER for Baboon image

Block Size	Peak signal to noise ratio	Bit error rate
12	88.0026	0

22	76.2632	0
32	63.5264	0
42	59.0672	0
52	52.4640	0
62	47.9335	0
64	50.0535	7.3750

The graph of PSNR and BER of baboon image is shown in Fig.4.5(a) and Fig.4.5(b). Similarly the same procedure of encryption and decryption is done for Sailboat image. After applying the method of encryption and decryption, the calculated PSNR and BER is shown in Table 4.3.The graph of PSNR and BER is shown in Fig. 4.6(a) and Fig. 4.6(b).

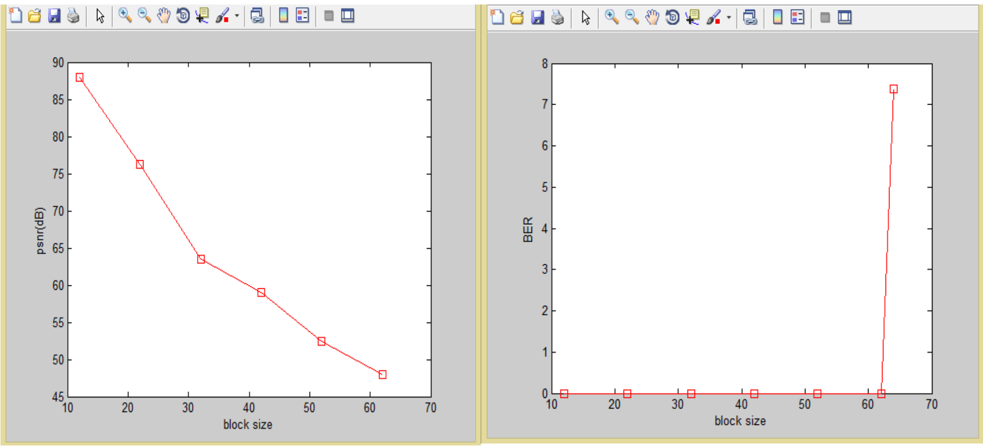


Fig. 4.5(a) Block size v/s PSNR (b) Block size v/s BER of Baboon image for different blocks

Table 4.3 Block size v/s PSNR and BER for Sailboat image

Block Size	Peak signal to noise ratio	Bit error rate
16	102.3162	0
22	90.5553	0
32	78.8527	0
42	72.1794	0
52	62.7873	0
62	55.0150	0
64	53.0458	7.3750

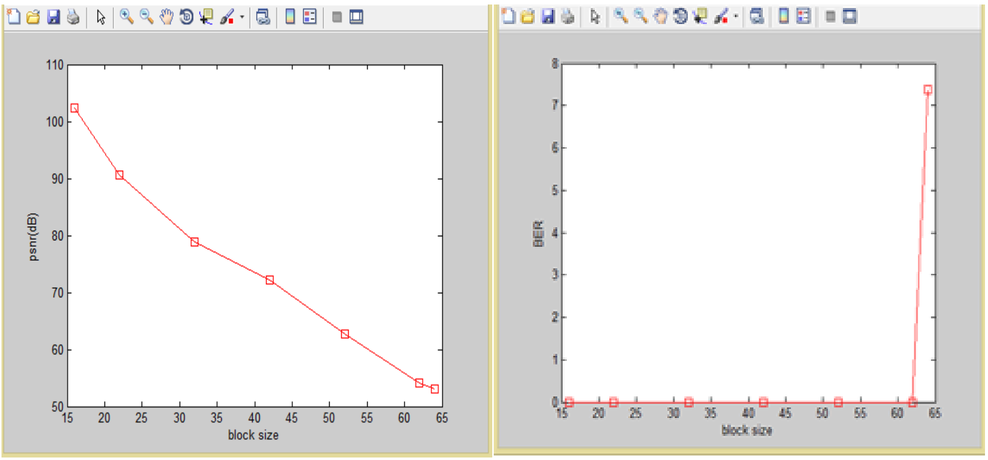


Fig. 4.6(a) Block size v/s PSNR (b) Block size v/s BER of Sailboat image for different blocks

For the image, such as sailboat, the error rate at block size 16×16 is 0 and PSNR is 102.3162 dB.for the sailboat image at block size 64×64 the error rate changes from 0 to 7.3750% and PSNR is 53.0150 dB which shows that as the block size increases, error rate also increases shown in fig. 4.6(b) and psnr decreases which is shown in fig.6 (a) and the error rate is same from block size 16×16 to 63×63 i.e 0%.

Table 4.4 Block size v/s PSNR and BER for Splash image

Block Size	Peak signal to noise ratio	Bit error rate
16	93.8652	0
22	73.0528	0
32	63.5976	0
42	61.2799	0
52	53.6401	0
62	48.0655	0
64	47.3918	7.3750

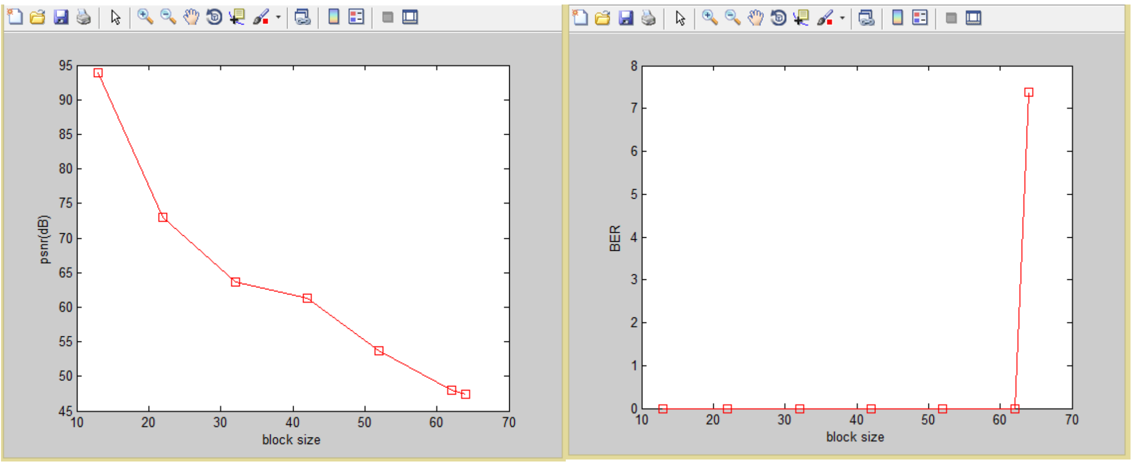


Fig. 4.7(a) Block size v/s PSNR (b) Block size v/s BER of Splash image for different blocks

Similarly the same procedure of encryption and decryption is done for Splash image. After applying the method of encryption and decryption, the calculated PSNR and BER is shown in Table 4.4.

For the image, such as splash, the error rate at block size 13×13 is 0 and PSNR is 93.8652 dB.For the sailboat image at block size 65×65 the error rate changes from 0 to 7.3750% and PSNR is 47.4383 dB which shows that as the block size increases, error rate also increases shown in fig. 4.7(b) and psnr decreases which is shown in fig. 4.7(a) and the error rate is same from block size 13×13 to 64×64 i.e. 0%.

Fig. 4.8 plots the block size versus extraction error rate of the proposed method and [36]. The error rates are calculated by dividing the number of total blocks by the number of incorrectly recovered blocks.

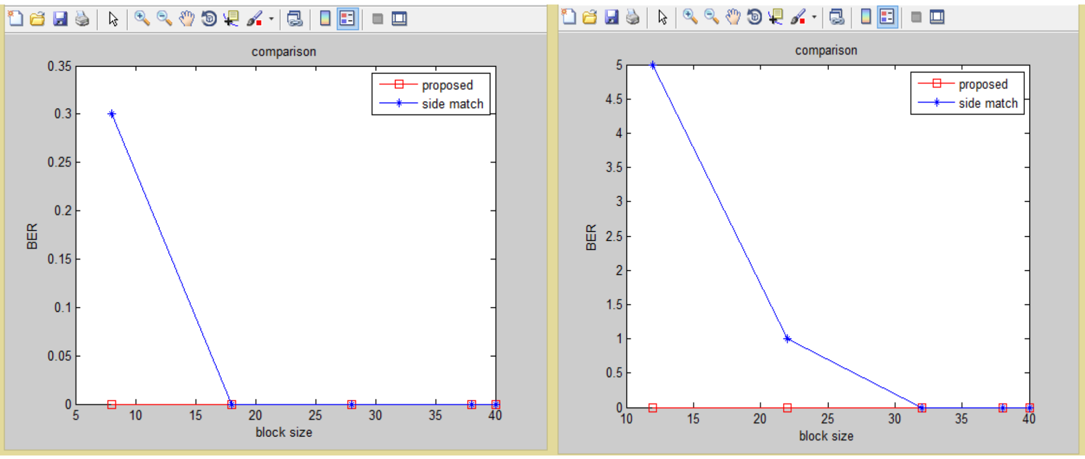


Fig. 4.8 Error rate comparison. (a) Lena (b) Baboon

Fig.4.8 reveals that the proposed method offers lower error rates than that of [36]. For example, for the Lena image at block size8×8, the error rate of the proposed method is 0%whereas the error rate of [36] is 0.34 %, which is less than that of [36] and at block size 12×12 the error rate is 0% and PSNR is 97.5450dB.For Lena image at block size 64×64 the error rate changes from 0 to 8.5938% as shown in fig. 4.4(b) and psnr is 54.2725 dB which shows that as the block size increases, error rate also increases, and psnr decreases as shown in fig. 4 (a)

For the image, such as Baboon, the error rate at block size 12×12 is 0 and psnr is 88.0026 dB.For the Baboon image at block size 64×64 the error rate changes from 0 to 7.3750% and PSNR is 50.0535 dB which shows that as the block size increases, error rate also increases shown in fig. 4.5(b) and PSNR decreases which is shown in fig.4.5 (a)

5.3 Result phase -2

By using this method of hiding data in encrypted image using DCT, a large amount data can also be hide in the image. For example, for Baboon image if 2333 byte of data is embedded in it (shown in Fig. 4.9) then the PSNR comes to be 74.8811 dB and BER is 0% as shown in Fig. 4.10(a) and Fig. 4.10(b)

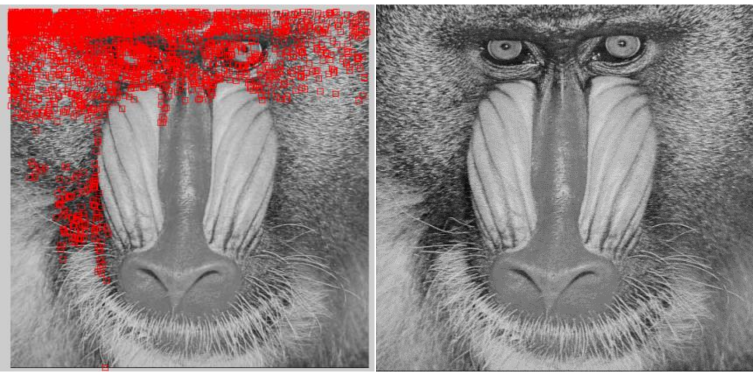
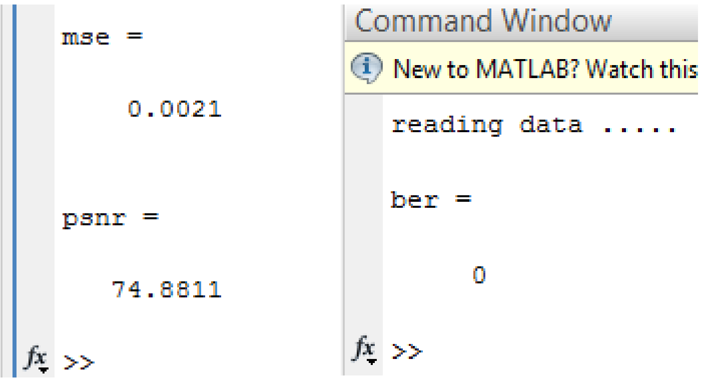


Fig. 4.9 (a) Baboon image while hiding data (b) Encrypted image



```
mse =

    0.0021


psnr =

   74.8811

>>
```

Command Window

New to MATLAB? Watch this

```
reading data .....

ber =

     0

>>
```

Fig. 4.10 (a) PSNR (b) BER of Baboon image

For example, for water splash image(with less details) if 2333 byte of data is embedded in it(shown in Fig. 4.11(a)) then the PSNR comes to be 74.8811 dB and BER is 0% as shown in Fig. 4.12(a) and Fig. 4.12(b). Encrypted image is blurry where the hide is embedded shown in Fig. 4.11(b).

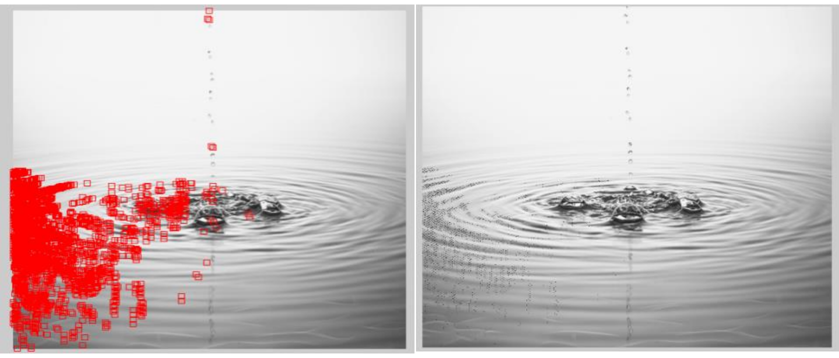
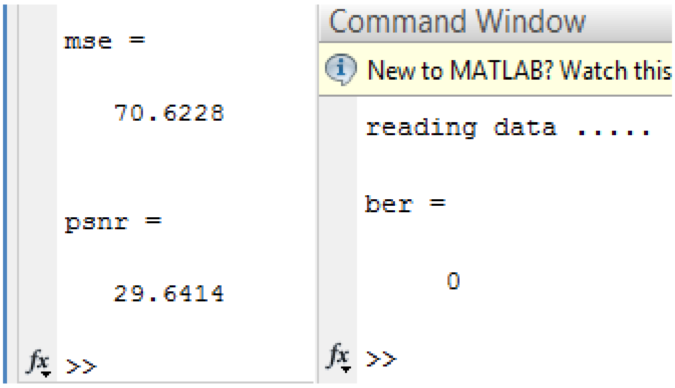


Fig. 4.11 (a) Water Splash image whilehiding data (b) Encrypted image



```
mse =

   70.6228


psnr =

   29.6414

fx >>
```

```
reading data .....

ber =

     0

fx >>
```

Fig. 4.12 (a) PSNR (b) BER of Baboon image

From the above two results, it is observed that image with more details has psnr much better than images with less details (i.e if there is a plain image ,then the PSNR is very low as compare to detailed one).

6. Discussion

To enhance the quality of image after hiding some amount of data in it, here is to hide data in images using reversible data hiding algorithm with the use of DCT to match the closest data hiding pixel for every symbol to be hide. There are two methods: Closest element approach and random sequence approach. But here with the help of closest element approach the closest data hiding is to be match. Basically the purpose of this method is to find out the noisy pixels and then hiding the data in it. This can be done in encryption process and then generating the key for decryption. PSNR and MSE is then calculated to check the changes in quality of image. Then by saving the key and the encrypted image, the decryption process is done. Then calculation of bit error rate is done to check the changes in extracted data. In this work, a novel reversible data hiding scheme for encrypted image using DCT is proposed, which consists of image encryption, data embedding and data extraction/ image-recovery phases. The data of original image are entirely encrypted by using DCT. Additional data is embedded into the encrypted image by modifying a part of encrypted data. With an encrypted image containing embedded data, a receiver may firstly decrypt it using the encryption key, and the decrypted version is similar to the original image.

7. Conclusion and Future Scope

Finally, this paper ends presenting the summary of the main conclusion drawn and future scope. This method proposes data extraction and image recovery strategies based on Hong’s work. Different algorithms are used to hide the data in the image. The presented research work is about to find out the pixels in the image to which the data is to be hide. In this proposed work the two files are used for this method one is image file and another one is text file.

In the near future, the most important use of data hiding techniques will probably be lying in the field of digital watermarking. Content providers are eager to protect their copyrighted works against illegal distribution and digital watermarks provide a way of tracking the owners of these materials. Data hiding might also become limited under laws, since governments already claimed that criminals use these techniques to communicate.

The possible use of data hiding technique is as following:

1. Hiding data on the network in case of a breach.

2. Peer-to-peer private communications.

3. Posting secret communications on the Web to avoid transmission.

4. Embedding corrective audio or image data in case corrosion occurs from a poor connection or transmission.

REFERENCES

[1] X. Zhang; "Reversible Data Hiding in Encrypted Image "Signal Processing Letters, vol.18,no.4,pp.255-258,April 2011.

[2]L. Xuemei, T. Xinhai and D. Lin; "A Novel Scheme on Reality Preserving Image Encryption",Third International Conference on measuring Technology and Mechatronic Automation(ICMTMA) ,vol.1,pp.218-221,6-7 Jan.2011.

[3] S. Bhowmik and S.Acharyya "Image Cryptography: The Genetic Algorithm Approach",Computer Science and Automation Engineering (CSAE),vol.1.,pp.223-227,10-11 June 2011.

[4] Y.Wu, J.P. Noonan and S.Agaian ,"A Wheel-Switch Chaotic System for Image Encryption",System Science and Engineering(ICSSE),vol.44,pp.23-27,8-10 June 2011.

[5] M. Kansal, G. Singh and B V Kranthi "DWT, DCT and SVD based Digital Image Watermarking",Computer Sciences(ICCS),vol.2,pp.77-81,14-15 September 2012.

[6] G.S.Yadav and A.Ojha, "A Fast and Efficient Data Hiding Scheme in Binary Images",Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2012 Eighth International Conference on, vol., no., pp.79-84, 18-20 July 2012.

[7] G.A.Sathishkumar, S.Ramachandran andK.B.Bagan " Image Encryption Using Random Pixel Permutation by Chaotic Mapping" , Computers & Informatics (ISCI), 2012 IEEE Symposium on , vol., no., pp.ix-xxii, 18-20 March 2012.

[8] M.I. Khan, V. Jeoti and A.S. Malik, M. F.Khan "A Joint Watermarking and Encryption scheme for DCT Based Codecs" , Communications (APCC), 2011 17th Asia-Pacific Conference , vol., no., pp.816-820, 2-5 Oct. 2011.

[9] A. B. Mahmood and R. D. Dony "Segmentation Based Encryption Method for Medical Images", Internet Technology and Secured Transactions (ICITST), 2011 International Conference for , vol., no., pp.596-601, 11-14 Dec. 2011.

[10] P.Telagarapu, B.Biswal and V.S.Guntuku "Security of Image in Multimedia Applications", Energy, Automation, and Signal (ICEAS), 2011 International Conference on, vol., no., pp.1-5, 28-30 Dec. 2011.

[11] X. Zhang "Separable Reversible Data Hiding in Encrypted Image" ,Information Forensics and Security, IEEE Transactions on , vol.7, no.2, pp.826-832, April 2012.

[12] J. Tian "Reversible Data embedding using difference expansion," IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890-896, Aug. 2003.

[13] Z. Ni, Y.Q. Shi, N. Ansari, and W. Su," Reversible data hiding", IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354-362, 2006.

[14] X. Li, B. Yang and T.Zeng, "Efficient Reversible Watermarking Based on Adaptive Prediction-Error Expansion and Pixel Selection," Image Processing, IEEE Transactions on , vol.20, no.12, pp.3524,3533, Dec. 2011.

[15] M.U.Celik, G. Sharma, and A.M. Tekalp and E. Saber, "Lossless generalized-LSB data embedding," Image Processing, IEEE Transactions on , vol.14, no.2,pp.253,266, Feb. 2005.

[16]W. Hong,T-S.Chen,C-W.Shiu andY-P. Chang " A high capacity reversible data hiding scheme using orthogonal projection and prediction error modification,"Signal Processing, vol.90, no.11, pp.2911-2922, Dec. 2010.

[17] C. –C. Chang, C.C. Lin and Y.H. Chen, "Reversible data-embedding scheme using differences between original and predicted pixel values," Information Security, IET , vol.2, no.2, pp.35,46, June 2008.

[18] S. Lian, Z. Liu, Z. Ren and H. Wang, "Commutative Encryption and Watermarking in Video Compression," Circuits and Systems for Video Technology, IEEE Transactions on , vol.17, no.6, pp.774,778, June 2007.

[19]B. V. Dasarathy, Editorial: An overview of information fusion in the domain of watermarking and document security, Information Fusion, v.14 n.2, p.123-126, April, 2013.

[20] D.Kundur and K. Karthik, "Video fingerprinting and encryption principles for digital rights management," Proceedings of the IEEE , vol.92, no.6, pp.918,932, June 2004.