Encryption based LSB Steganography Technique for Digital Images and Text Data

Manpreet Kaur, Vinod Kumar Sharma
Computer Science And Engineering, Guru Kashi University, Talwandi Sabo, Punjab

Abstract:
Digital steganography is the art and science of hiding communications; a steganographic system thus embeds secret data in public cover media so as not to arouse an eavesdropper's suspicion. A steganographic system has two main aspects: steganographic capacity and imperceptibility. However, these two characteristics are at odds with each other. Furthermore, it is quite difficult to increase the steganographic capacity and simultaneously maintain the imperceptibility of a steganographic system. Additionally, there are still very limited methods of Steganography to be used with communication protocols, which represent unconventional but promising Steganography mediums. Digital image Steganography, as a method of secret communication, aims to convey a large amount of secret data, relatively to the size of cover image, between communicating parties. Additionally, it aims to avoid the suspicion of non-communicating parties to this kind of communication. Thus, this research addresses and proposes some methods to improve these fundamental aspects of digital image Steganography. Hence, some characteristics and properties of digital images have been employed to increase the steganographic capacity and enhance the stego image quality (imperceptibility). Here, the research aim is identified based on the established definition of the research problem and motivations. Unlike encryption, Steganography hides the very existence of secret information rather than hiding its meaning only. Image based Steganography is the most common system used since digital images are widely used over the Internet and Web. However, the capacity is mostly limited and restricted by the size of cover images. In addition, there is a tradeoff between both steganographic capacity and stego image quality. Therefore, increasing steganographic capacity and enhancing stego image quality are still challenges, and this is exactly our research main aim. To get a high steganographic capacity, novel Steganography methods were proposed. The first method was based on using 8x8 non-overlapping blocks and quantization table for DCT with compression. Second method incorporates the DWT technique, with quality of any stego images as enhanced to get correct hidden image. And last LSB as to store images with Key type security built in.

Keyword
digital images, hidden, Steganography, encryption, steganographic

1. Introduction

Digital Steganography is the art and science of hiding communications; a Steganographic system thus embeds secret data in public cover media so as not to arouse an eavesdropper's suspicion. A Steganographic system has two main aspects: Steganographic capacity and imperceptibility. However, these two characteristics are at odds with each other. Furthermore, it is quite difficult to increase the Steganographic capacity and simultaneously maintain the imperceptibility of a Steganographic system. Additionally, there are still very limited methods of Steganography to be used with communication protocols, which represent unconventional but promising Steganography mediums. Digital image Steganography, as a method of secret communication, aims to convey a large amount of secret data, relatively to the size of cover image, between communicating parties. Additionally, it aims to avoid the suspicion of non-communicating parties to this kind of communication. Thus, this research addresses and proposes some methods to improve these fundamental aspects of digital image Steganography. Hence, some characteristics and properties of digital images have been employed to increase the Steganographic capacity and enhance the stego image quality (imperceptibility).

2. Steganography and Watermarking

Steganography aims to hide the very existence of communication by embedding messages within other cover objects. However, watermarking aims to protect the rights of the owners of digital media such as images, music, video and software. Even if people copy or make minor modification to the watermarked file, the owner can still prove it is his or her file. Thus, both of Steganography and watermarking are forms of data hiding and share some common characteristics. Nevertheless, the goal of Steganography is the embedded message while the goal of watermarking is the cover object itself. Watermarking is a data hiding technique that protects digital documents, files, or images against removal of copyright information. Even if someone knows that a watermark is exist (i.e. visible watermarking) in a given object, it should be impossible to remove the watermark from the watermarked object without causing distortion or destroying the original (watermarked) object. This aspect or feature of watermarking is known as "robustness". According to the

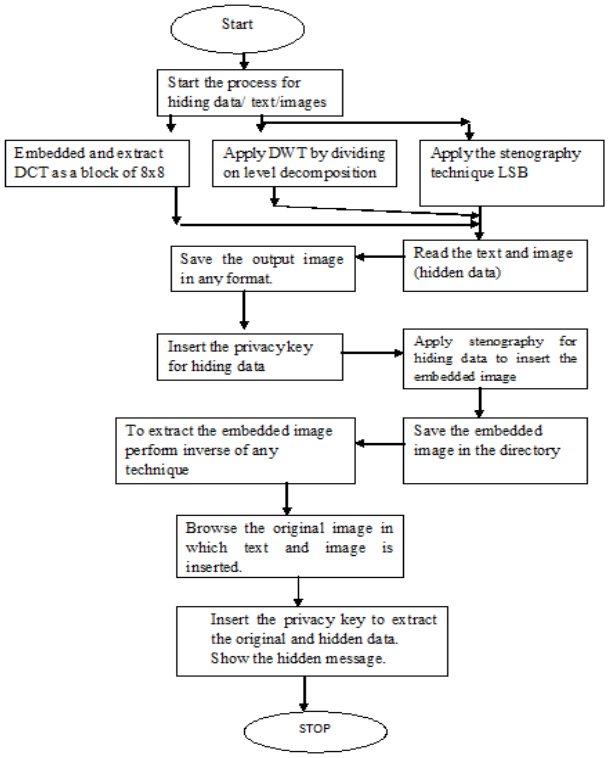
Manuscript received September 5, 2016
Manuscript revised September 20, 2016

kind of embedded information, two techniques of document marking can be distinguished: watermarking and fingerprinting. Watermarking is the process of embedding a specific copyright mark into digital documents in the same way. On the other hand, in order to detect any break of licensing agreement, a serial number is embedded in every copy of this digital document. This process is known as “fingerprinting”. Even if these markings are detected, it should be practically impossible to remove them.

3. Literature Survey

Rasha Adel Ibrahim et al. 2015, here working on Fractal compression is done on various fractions of images, relying on the fact that parts of an image often resemble other parts of the same image. It takes long encoding time and affects the image quality. Here an improved model integrating quantized quad trees and entropy coding used for fractal image compression which results in improving the recovered image’s quality and compression ratio significantly on different types of images and encoding time. Here there decreasing in images sizes making less encoding time, but decrease image quality [17]. Vinayak S. Dhole et al. 2015, here studies of different existing methods are discussed. A new method of watermarking named self-embedding fragile watermark technique is worked out. Embedding is done in two phases one with own image and another with watermark image. Combinations of above two images are to be used for generation of final watermark image. Self-embedding fragile watermark technique is useful for image recovery with higher recovery in tamper region which gives more accurate recover image in comparison with other existing methods [20]. C.P.Sumathi et al. 2013, in this author attempted to analyze the various techniques used in Steganography and to identify areas in which this technique can be applied, so that the human race can be benefited at large [7]. Gurpreet Kaur 2013, here a technique of data hiding, which provide security of data with least significant bits (LSB) is worked out [8]. Mrs. Kavitha 2012, here a brief idea about the image steganography that make use of Least Significant Bit (LSB) algorithm for hidding the data into image is implemented is faster and reliable and compression ratio is moderate compared to other algorithm. The approach provides higher security and can protect the message from stego attacks. The image resolution doesn't change much and is negligible when we embed the message into the image and the image is protected with the personal password. So, it is not possible to damage the data by unauthorized personnel [12]. Adnan Gutub, Mahmoud Ankeer et al. 2010, Image based steganography uses the images as the cover media. LSB is a commonly used technique in this filed. Several scenarios of utilizing least significant bits within images are available. We merge between the ideas from the random pixel manipulation methods and the stegokey ones to propose our work, which uses the least two significant bits of one of the channels to indicate existence of data in the other two channels. This work showed attractive results especially in the capacity of the data-bits to be hidden with relation to the RGB image Pixels [2]. A. Daneshkhah 2010, proposed the two bits of message is embedded in a pixel in a way that not only the Least Significant Bit (LSB) of picture element is allowed to change but also the second bit plane and fourth bit plane are allowed to be manipulated, but the point is in each embedding process only one alternation in one bit plane is allowed to happen. It is compared by the method LSB-Matching, the results shows this method has an acceptable capacity of embedding data and hardly is detectable for Steganalysis algorithm [3]. Q. Huang 2010, proposed the problem in LSB Matching Revisited (LSBMR) algorithm to make regions selection on images to find suitable area. By counting on each pixel we can decide if it should be protected. It can improve the visual imperceptibility and detectability of the LSB matching method. By adjusting the parameters of neighbour pixels, the max embedding capacity can be increased as needed [16]. Sujay Narayana and Gaurav Prasad 2010, the science of securing a data by encryption is Cryptography whereas the method of hiding secret messages in other messages is Steganography, so that the secret’s very existence is concealed. The term ‘Steganography’ describes the method of hiding cognitive content in another medium to avoid detection by the intruders. This paper introduces two new methods wherein cryptography and steganography are combined to encrypt the data as well as to hide the encrypted data in another medium so the fact that a message being sent is concealed. One of the methods shows how to secure the image by converting it into cipher text by S-DES algorithm using a secret key and conceal this text in another image by Steganographic method. Another method shows a new way of hiding an image in another image by encrypting the image directly by S-DES algorithm using a key image and the data obtained is concealed in another image. The proposed method prevents the possibilities of stego analysis also [18].

4. Methodology



5. Results

The work Data hiding using color palette in stenography shows different results that are shown below. The figure 1.1 shows the starting of the work, with three buttons. On clicking first button DCT technique working as stenography with watermarking will be running. On clicking Second button DWT technique will be run. On clicking third button LSB technique will work. Below figure shows the starting window.

Figure 1.1: Starting Window for Steganography with three different buttons

5.1 Results Using Lsb Technique

Figure 1.2, shows the window in which insert and extract button is provided for selecting options as insert button to add original image and the image or text to be marked for embedding and second button extract get out back original and hidden data. Third button compatibility information shows the ASCII code on clicking on it.

Figure 1.2: Window for inserting and extracting images using LSB technique.

Figure 1.3 and 1.4, shows the adding information of source image and hidden image or text selection information.

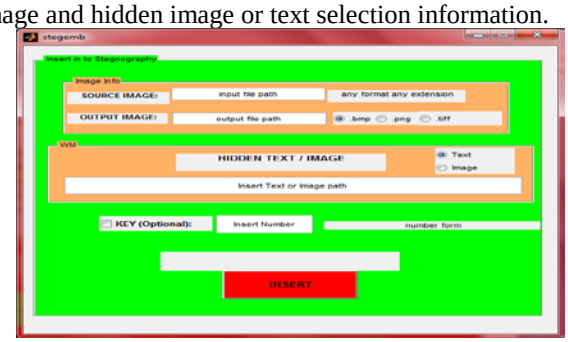


Figure 1.3: Window for inserting of source file and text or image as hiding using LSB.

Figure 1.4 shows, how to select the source file and add text with security key as hiding into image itself. In this window a text box is shown with source file to be select as original file as to be inserted as cover image. Then output file text with edited text is shown in window which indicates that what image name is to save in database after adding text to cover image and security key. Three extensions are shown as to save output image with radio button as .bmp, .png, .tiff. After this window is shown with to radio button for selection of text or image to be used as hidden data under cover image. Path is to be provided of hidden image or write text on it. Then security key is to e provided and remember that key as needed for extraction process. At last click on insert button for embedding process.

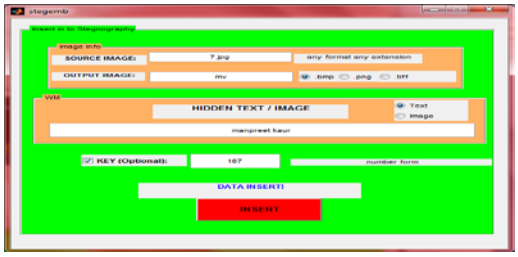


Figure 1.4: Window after insertion of source file and text as hiding using LSB.

Below figure 1.5 shows the window in which after insertion of source file and hidden text with security key shows the original and hidden image as named mentioned in output text box.

Figure 1.5: Window after insertion Showing Original and Hidden image.

In figure 1.6, Extraction process is explained in which a file saved is used as source file for extracting the hidden image and security key is to be provided. At last click on extract button for getting back original and hidden text or image.

Figure 1.6: Window for extracting source file and hidden text using LSB.

Figure 1.7 to 1.9, shows above insertion and extraction process for hiding image respectively.

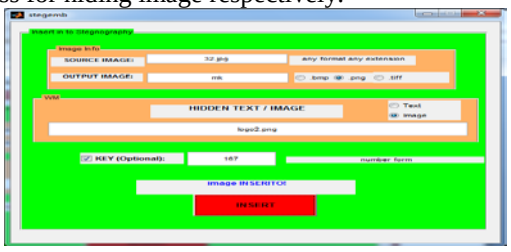


Figure 1.7: Window after insertion of source file and Image as hiding using LSB.

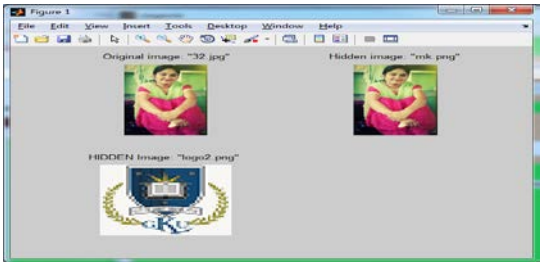


Figure 1.8: Window after insertion Showing Original, hidden image and covered image.

Above figure 1.8, shows the images after insertion as original means source image, hidden image as logo which is selected to be hide as image and last as output image saved with named as mention which is to be extracted after sending via internet for security with key.

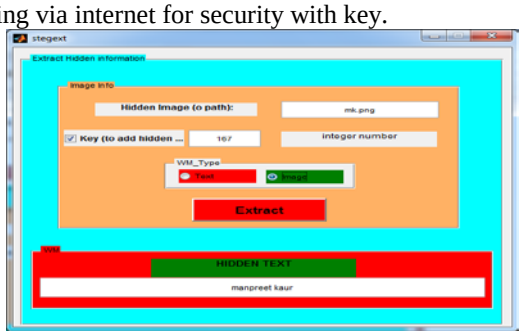


Figure 1.9: Window for extracting source file and hidden Image using LSB

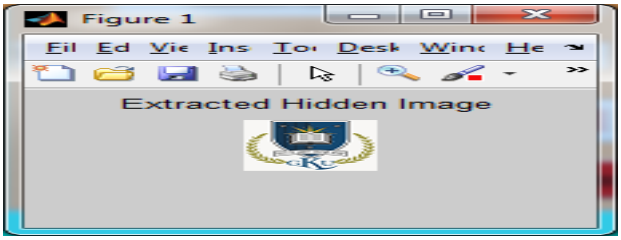


Figure 1.10: Window after extracting showing hidden image

Figure 1.10, shows the logo which has been used for hidden message with source file as covered image after applying security key is extracted.

5.2 Results Using Embedded And Extracting (Dwt) Technique

The data hiding as image using color palette in embedded and extracting shows us different results as described below. The figure 1.1 shows the starting of the work, where we have to choose the operations DWT button firstly, for embedded and extracting the hidden image or text into original image and vice versa, the results of embedded image is shown in figure 1.11 to 1.17, figure

1.11 shows the original image, 1.12 shows us the hidden image which is to be embedded and figure 1.13 shows the actually embedded image with hidden data to the original image. Figure 1.14 shows the extracted image showing hidden image. 1.15 shows the original and text as hiding under it is worked in window. Figure 1.16, shows the actually embedded image with hidden text as covered image. Figure 1.17 shows the extracted text.

Figure 1.11: Original Image for embedding using DWT technique

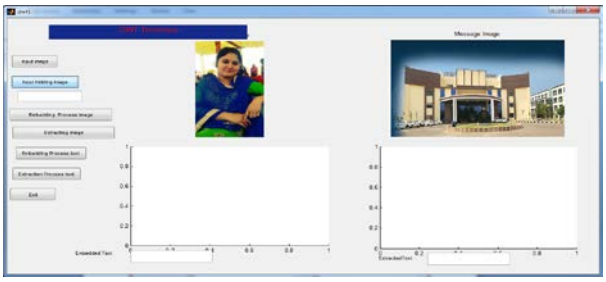


Figure 1.12: Hidden Image to be embedded in Original Image using DWT

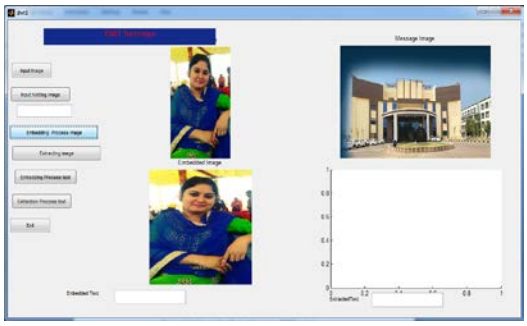


Figure 1.13: Image after Embedding using DWT technique.

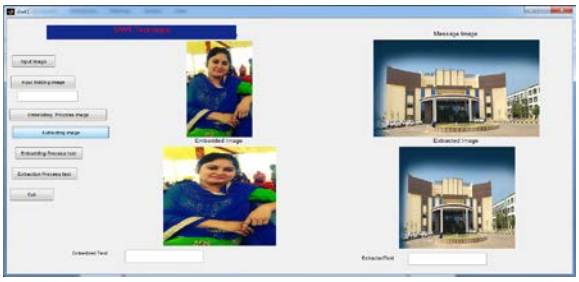


Figure 1.14: Image after Extracting hidden image using DWT technique.

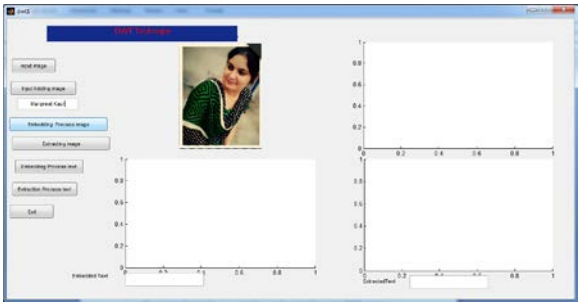


Figure 1.15: Original Image and hiding text for embedding using DWT technique

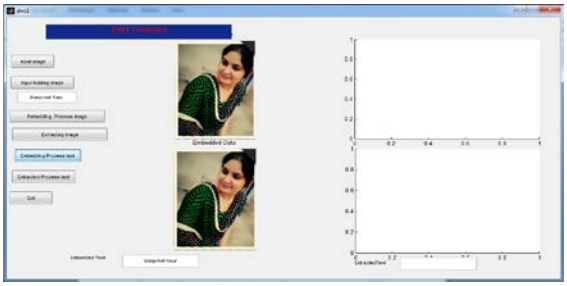


Figure 1.16: Shown embedded text with original Image as cover image using DWT

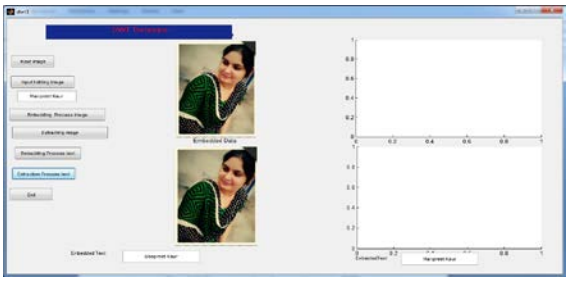


Figure 1.17: Shown extracted text from cover image using DWT

5.3 Results Using Dct Technique

The data hiding as image using color palette in DCT techniques shows us different results as described below. The figure 1.1 shows the starting of the work, where we

have to choose the operations as DCT clicking on button. A new window open in which we will select some button to load the input image, hiding image/text, embedding process for embedding message and last button extraction process for Extracting message again back which was embedded in inputted image as with figure 1.18 to 1.24.

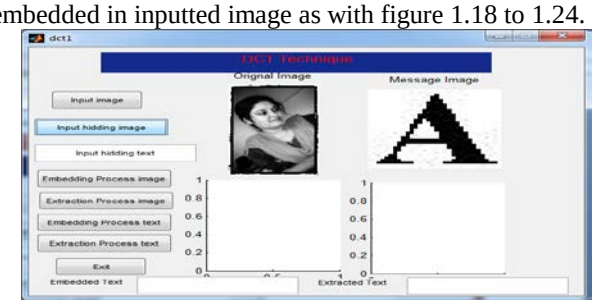


Figure 1.18: DCT technique for Original and hidden image

Figure 1.18, shows the original image as inputted image after clicking on input button on which we have to embed the message or image. İt also shows the message imagewhich is to be embedded.

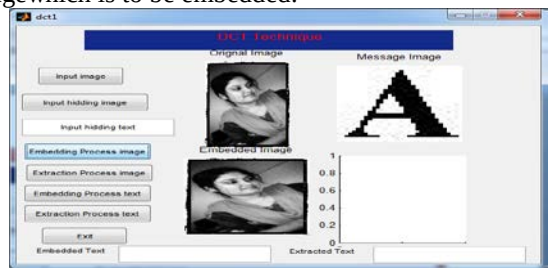


Figure 1.19: window for selecting original image using DCT Technique

Above figure 1.19, shows the embedded image as covered image after selecting embed msg or image with original image.

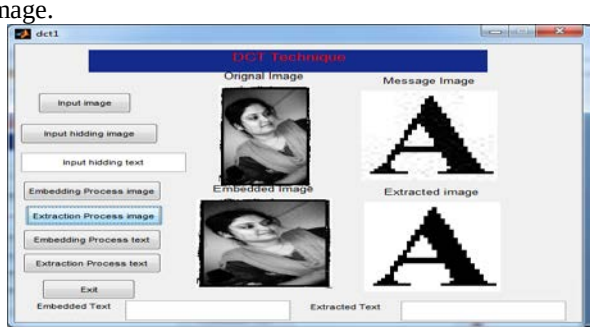


Figure 1.20: Shows the extracted hidden image using DCT.

Above figure 1.20, shows the extracted image as image which is used for hiding after clicking on Extraction process button.

Now same process is worked out for text hidding. Select the embedded message/text with original image by clicking on load image button and writing hidden text in the text box.

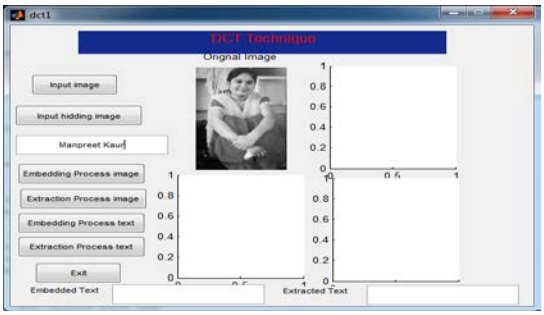


Figure 1.21: Window showing hidding msg/text and Original Image

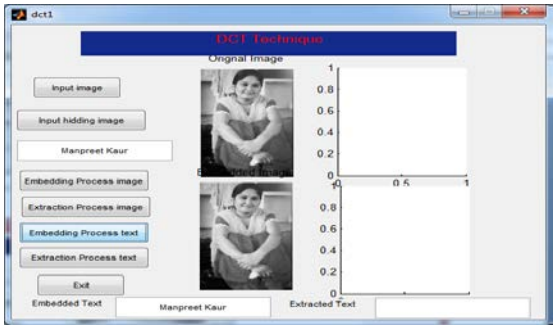


Figure 1.22: Embedding Window with DCT

Above figure 1.22 shows the window after embedding process as embedded or covered image showing hidden msg/text as embedded under original image. Below figure 1.23, shows the embeddded message/text with original image after processing extracting text process.

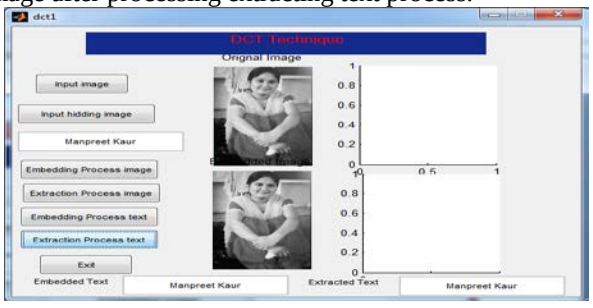


Figure 5.23: Extracted hidden text/msg using DCT technique

Above, we have discuss three different techniques having different methods to encode and decode image with text or images.

6. Discussion

Here, calculation of PSNR and MSE value are used as parameter for embedded image with msg as encoded for

stegnography with DCT, DWT and LSB technique. As requirement is what are the difference lies between all these techniques as while encoding and decoding the message such as image or text.

Above, we have discuss three different techniques having different methods to encode and decode image with message or images for stegnography.

Table 1.1: Comparison of techniques by parmeters as PSNR and MSE

Cover Image	Hidden Image	DCT		DWT		LSB	
		PSNR	MSE	PSNR	MSE	PSNR	MSE
		1.3251	4.792	2.8433	2.472	4.7363	2.193
		3.0280	3.238	2.8293	3.529	5.4195	1.875
		2.2945	3.833	2.8492	2.153	5.4988	1.834

As discussed psnr and mse are two parameter used for comparing three techniques. PSNR should be high and MSE should be Low for best result. From above table 1.1 it is concluded that LSB is best technique as compared through both parameters. From below figure of graphs 1.24 and 1.25, describes about three techniques results. From these results conclusion is that LSB have compatively best results as output and can work on any type of images. DWT can also work with any type of images but its parameters are less better than LSB. DCT technique works best with black and white images only.

7. Conclusion

Steganography is a really interesting subject and outside of the mainstream cryptography and system administration that most of us deal with day after day. Steganography can be used for hidden communication. We have explored the limits of Steganography theory and practice. We printed out the enhancement of the image Steganography system using LSB approach to provide a means of secure communication. A stego-key has been applied to the system during embedment of the message into the cover image. This Steganography application software provided for the purpose to how to use any type of image formats to hiding any type of files inside there. The master work of this application is in supporting any type of pictures without need to convert to bitmap, and lower limitation on file size to hide, because of using maximum memory space in pictures to hide the file.

Since ancient times, man has found a desire in the ability to communicate covertly. The recent explosion of research in watermarking to protect intellectual property is evidence that Steganography is not just limited to military or espionage applications. Steganography, like cryptography, will play an increasing role in the future of secure communication in the “digital world”. The proposed scheme used in this work is encrypts the secret information before embedding it in the image. Certainly the time complexity of the overall process increases but at the same time the security achieved at this cost is well worth it. In this invisible watermarking is used with Steganographic techniques. We have explained the basic mechanism of our proposed model and it is an alternative approach of Steganographic. It is not pure Steganographic technique but the effect is same with some additional advantage. First advantage is the data file and reference image is going through the open channel separately. The basic result is interception of any one cannot provide desired objective. Second advantage is that any amount of data can be transmitted using the method because it is not depending on the size of image. Final advantage, the said method is not affecting the image. There is no change of quality and color change of reference image. It is most vital achievement of method.

The algorithm time complexity is simple and always proportional to O(n). The performance of hiding algorithm is totally depending on the length of text to hide and size of image. Similarly unhidden algorithm is reverse process of previous one and complexity character is same.

8. Future Scope

This Dissertation is developed for hiding information in any image file. The scope of the work that is implemented of Steganography tools for hiding information includes any type of information file and image files and the path where the user wants to save image and extruded file. In cryptography, information can be accessed by any unauthorized person. The secret information can be loss the data and leakage the information. We solve this problem of loss data by the Steganography. In the Steganography do not access the information by the unauthorized. The security is available for every information and personal data with the help of Steganography.

At end, this can be said that the aforesaid method may be improved, instead of text small image may be hiding, invisible watermarking may be used or much improvement in this field may be incorporated in future. Lastly it is expected by the authors that any kind of future endeavors in this field will definitely route it a path to design a secure system using the proposed algorithm for both Internet and Mobile Communication Technology.

REFERENCES

[1] Abdullah Bamatraf, Rosziati Ibrahim and Mohd. NajibMohd. Salleh, “A New Digital Watermarking Algorithm Using Combination of Least Significant Bit (LSB) and Inverse Bit”, JOURNAL OF COMPUTING, VOLUME 3, ISSUE 4, APRIL 2011, ISSN 2151-9617.

[2] Adel Almohammad and Gheorghita Ghinea, "Image Steganography and Chrominance Components", 10th IEEE International Conference on Computer and Information Technology, 2010.

[3] Ali Daneshkhah, Hassan Aghaeinia and Seyed Hamed Seyedi, "A More Secure Steganography Method in Spatial Domain", Second International Conference on Intelligent Systems, Modelling and Simulation, 2011.

[4] Ankita Sharma, Sarika khandelwal, “A Brief Introduction to Digital Watermarking”, (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (3) , 2015, 2399-2401.

[5] Arup Kumar Bhattacharjee, Tanumon Bej, Saheb Agarwal, “Comparison Study of Lossless Data Compression Algorithms for Text Data”, IOSR Journal of Computer Engineering (IOSR-JCE),e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 11, Issue 6 (May. - Jun. 2013), PP 15-19.

[6] Chin-Chen Chang et al.,“A steganographic method based upon JPEG and quantization table modification”, Information Sciences 141 (2002) 123–138, Elsevier.

[7] C.P.Sumathi, T.Santanam and G.Umamaheswari, “A Study of Various Steganographic Techniques Used for Information Hiding”, International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.6, December 2013.

[8] Gurpreet Kaur, Kamaljeet Kaur, “Image Watermarking Using LSB (Least Significant Bit)”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 4, April 2013, ISSN: 2277 128X.

[9] Hardikkumar V. Desai, “Steganography, Cryptography, Watermarking: A Comparative Study”, Journal of Global Research in Computer Science, Volume 3, No. 12, December 2012, ISSN No: 2229-371X.

[10] Haroon Altarawneh, Mohammad Altarawneh, “Data Compression Techniques on Text Files: A Comparison Study”, International Journal of Computer Applications (0975 – 8887), Volume 26– No.5, July 2011.

[11] Jay Prakash Pandey, Gajendra Singh, “Digital Color Image Watermarking using DWT-SVD Techniques in YUV and RGB Color Spaces”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 1, January 2015, ISSN: 2277 128X.

[12] Mrs. Kavitha, Kavita Kadam, Ashwini Koshti, Priya Dunghav, “Steganography Using Least Signicant Bit Algorithm”, International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com, Vol. 2, Issue 3, May-Jun 2012, pp. 338-341.

[13] Nirbhay Kashyap, Dr. Shailendra Narayan Singh, “Review of Image Compression and Comparison of its Algorithms”, International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 2, Issue 12, December 2013, ISSN 2319 – 4847.

[14] Pooja Singh, “LOSSLESS DATA COMPRESSION TECHNIQUES AND COMPARISON BETWEEN THE ALGORITHMS”, International Research Journal of Engineering and Technology (IRJET), Volume: 02 Issue: 02 | May-2015, e-ISSN: 2395-0056, p-ISSN: 2395-0072.

[15] Puneet Kr Sharma and Rajni, “ANALYSIS OF IMAGE WATERMARKING USING LEAST SIGNIFICANT BIT ALGORITHM”, International Journal of Information Sciences and Techniques (IJIST) Vol.2, No.4, July 2012

[16] Qinhua Huang and Weimin Ouyang, "Protect Fragile Regions in Steganography LSB Embedding", 3rd International Symposium on Knowledge Acquisition and Modelling, 2010.

[17] Rasha Adel Ibrahim, et al., “An enhanced fractal image compression integrating Quantized quadtrees and entropy coding”, 2015 11th International Conference on Innovations in Information Technology (IIT), 978-1-4673-8511-4/15 $31.00 ©2015 IEEE.

[18] Sujay Narayana and Gaurav Prasad, "TWO NEW APPROACHES FOR SECURED IMAGE STEGANOGRAPHY USING CRYPTOGRAPHIC TECHNIQUES AND TYPE CONVERSIONS", in Signal & Image Processing: An International Journal (SIPIJ) Vol.1, No.2, December 2010.

[19] Tanmay Bhattacharya, Nilanjan Dey, S. R. Bhadra Chaudhuri, “A session based multiple image hiding technique using DWT and DCT”, International Journal of Computer Applications (0975 – 8887), Volume 38– No.5, January 2012.

[20] Vinayak S. Dhole, Nitin N Patil, “Self Embedding Fragile Watermarking for Image Tampering Detection and Image Recovery using Self Recovery Blocks”, 2015 International Conference on Computing Communication Control and Automation, 978-1-4799-6892-3/15 $31.00 © 2015 IEEE.

[21] Zhou Fu-an, “A Robust Watermarking Scheme Based on Least Significant Bit and Discrete Cosine Transform”, International Journal of Security and Its Applications, Vol. 9, No. 4 (2015), pp. 175-184.

[22] Zhu Yuefeng, LinLi, “Digital Image Watermarking Algorithms Based On Dual Transform Domain And Self-Recovery”, International Journal On Smart Sensing And Intelligent Systems Vol. 8, No. 1, March 2015.