

Steganography: A Comparative Survey Conducted on Digital Images

¹Miftah Ul Uroos, ²Sukhvinder Kaur, ³Muheet Ahmed Butt

Student, Department of Electronics and Communication Engineering, Swami Devi Dyal Institute of Engineering and Technology, Haryana, India

HOD & Assistant Professor, Department of Electronics of Communication Engineering, Swami Devi Dyal Institute of Engineering and Technology, Haryana, India

Scientist "D" PG Department of Computer Sciences, University of Kashmir, Srinagar, J&K, India

Corresponding Author: Miftah Ul Uroos,

Abstract: *Steganography refers to the data hiding. The main purpose of image steganography is to hide the data behind images. It means that it encodes the text in the form of image. The steganography is done when the communication takes place between sender and receiver. It is used to send the sensitive information with high security [15]. Nowadays in data transfer over the network, the security is the main issue concerned with this. Before the growth of the steganography, security of the data was the main concern of research for the researchers around the globe. The steganography method mostly depends on robustness, capacity, undetectability, invisibility of cover image and secret image. More the protection is done on these attributes more clarity is seen in the results. The number of techniques was developed in order to secure transmission. Steganography use algorithms for concealing the data. There are different types of steganography [13]. The steganography can be carried on data pertaining to image, audio and video formats. The proposed research focuses mainly on various steganography techniques such as LSB, DCT and DWT and algorithms associated with them. The research also provides a comparative analysis pertaining to PSNR and MSE after these techniques are applied on various digital images.*

Keywords: *Secret data, Encryption, Watermarking, LSB, DCT, DWT.*

Date of Submission: 04-10-2018

Date of acceptance: 19-10-2018

I. INTRODUCTION

Data sharing is increasing as thousands of messages and data is being transmitted on internet everyday from one place to another. Hence the protection of data is prime concern of the sender. The need is that correct data should be sent but in a secret way that only the legal receiver should be able to understand the message. At first, technique of cryptography was invented to transmit secret messages over places. In cryptography the message was encoded in another message in a covered way such that only the sender and receiver knew the way to decrypt it. A cryptographic key was used to decode the message that was known only by the authorized persons. The limitation of cryptography was that illegitimate person came to know that the message had a hidden text in it and so the probability of message being decoded by illegitimate person increased. To overcome this limitation the method of steganography was introduced [17]. The technique of steganography is better than cryptography as in it the data is hidden in image. The image is then sent over internet. It had advantage over cryptography as now the illegitimate person does not come to know whether data is hidden in the image or not. The data could only be decrypted from image by the authorized person as he knows the phenomenon to decode it and had the authorized key with him that was required to decode the data. The security and the reliability of data transmission also improved with invention of steganography as now the other person could not alter the sent data.

From the ancient times, steganography is used to hide the confidential data. The information to be sent was hidden on the back of wax, writing tables, stomach of rabbits or on the scalp of the slaves. The word steganography belongs to Greek language. In Greek the steganography stands for "covered writing". First of all steganography was used in Greece. They use to enter the message on a wooden tablet and then apply wax on it to hide the written data.

In this modern time, where technology is developing at fast speed and each day new developments are made, security is of highest priority. The data needs to be kept secure and safe so that it could be accessed only by the authorized workers and any unauthorized user cannot have any access of that data. But now a day, for unauthorized access of data, latest hacking methods are used. So, to keep the data confidential, sender uses

different methods. Digital watermarking is a special case of information hiding. In digital watermarking process the message is embedded into digital multimedia content (image, video, audio) and the message (the watermark) can later be extracted or detected for a various purposes such as copy prevention and control. While steganography hides as much data as possible into a cover signal, watermarking tries to emphasize the robustness against rotation, cropping, and translation of the embedded information at the expense of hiding capacity. Due to the inherent properties of steganography and watermarking, they have different applications. Steganography is used for instance covert communication applications, where the transmission of a large amount of information is needed. Watermarking is more appropriate for ownership authentication, content authentication and copy control, where the robustness is more important than capacity. In contrast to steganography and watermarking, steganalysis is the process of extracting the hidden message. The message is hidden using steganography or watermarking. Steganalysis is analogous to cryptanalysis applied to cryptography.

Steganography is one of the technique in which the data is hidden in the cover object with the use of secret key. The extractor should have secret key to extract the data. The secret key is designed in such a manner that it can't be find out by an unauthorized user. This is shown in the below figure 1.

In steganography systems following terms are used [18]:

- Cover Media: The cover media is the medium in which information is embedded in order to hide the secret data.
- Stego: The media through which the data is hidden.
- Secret data: The data to be hidden or extract.
- Steganalysis: The method by which secret data is to be extracted.

In image steganography, images are used as cover object.

The block diagram of basic steganography is shown below:

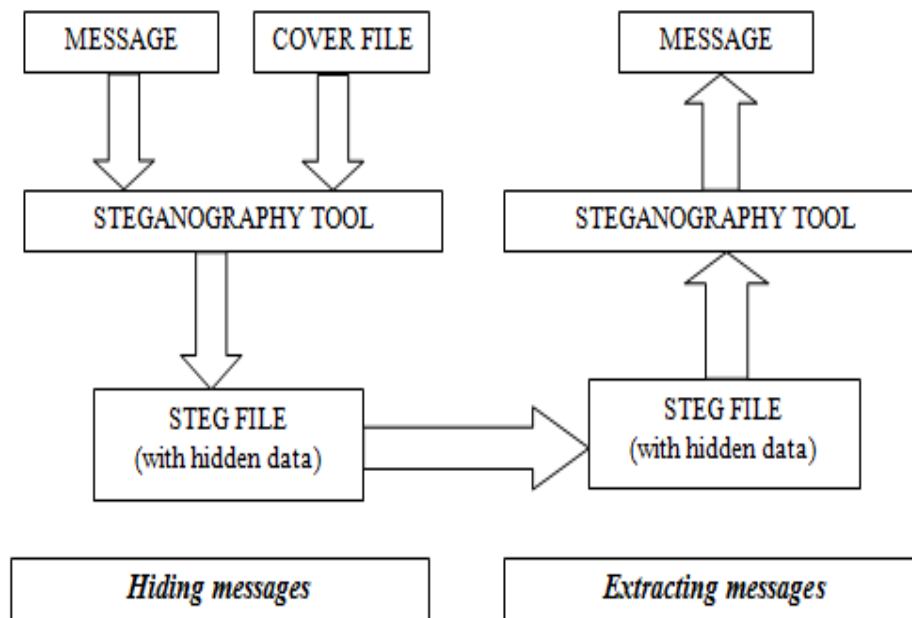


Figure 1: Block diagram of basic steganography.

II. VARIOUS STEGANOGRAPHY TECHNIQUES USED:

The techniques used in this paper are:

- LSB Technique.
- Discrete Cosine Transform (DCT) Technique.
- Discrete Wavelet Transform (DWT) Technique.

2.1 LSB technique: LSB stands for Least Significant Bit. This is a technique for image steganography which works on the Least Significant Bit value of the pixels. First the cover image is decomposed into bit planes and then LSB of bit planes is substituted with secret data. This is shown in below figure 2.1. This substitution concept includes embedding at the minimum weighting bit so that the value of original pixel is not affected [18]. This technique does not lead to any kind of distortion in the image while embedding data behind it. The value of

least significant bit varies but this change is invisible to human eye. The LSB have many advantages such as the image does not depreciated or distorted and by using LSB one can encrypt large amount of data behind an image. LSB transfers the data to the receivers end with security without allowing the illegitimate person to access the encrypted data. LSB is the popular and oldest method for hiding the message in a digital image. In LSB method we hide the message in the least significant bits (LSB's) of pixel values of an image. This is done in the binary form. It also poses some lacks and also it is less robust in nature, sometimes changes in image can lead to the data lost, hidden data can be revealed easily i.e. less secure. The problem with this technique is that it is very susceptible to attacks.

a) Advantages of LSB

- Less suspicious to human eyes.
- Simple to implement and many techniques uses this method.
- High perceptual transparency.
- 100% chances of insertion.

b) Disadvantages of LSB

- Three weakness- Robustness, Tamper and Resistance.
- Sensitive to filtering.
- The secret message is destroyed by Scaling, Rotation, Cropping, adding extra noise.

The figure below shows the block diagram of LSB Technique:

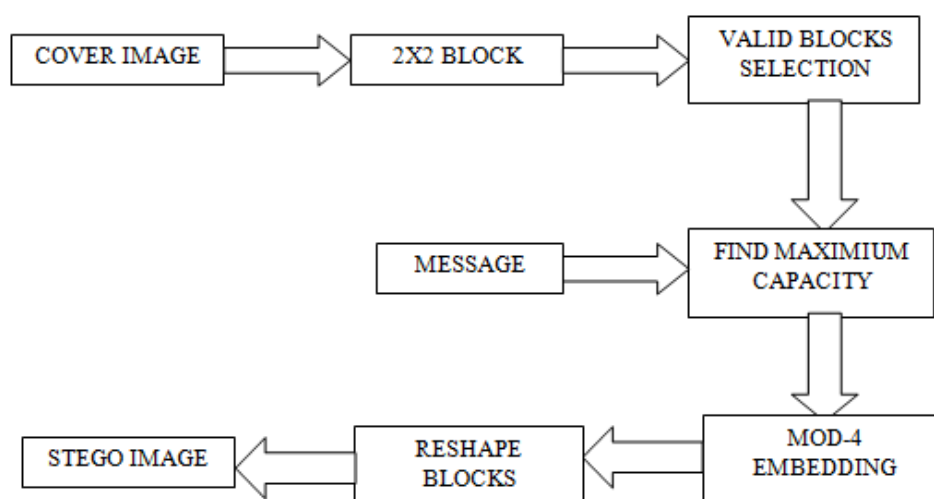


Figure 2.1: Block diagram of LSB Technique

PROPOSED ALGORITHM FOR LSB TECHNIQUE

Embedding Process

Input:

An $m \times n$ carrier image and a secret message/image.

Output: an $m \times n$ stego-image.

Algorithm: Steps-

Step1. Read the original image and the image which is to be hidden in the original image

Step2. Shift the image to hide in the cover image by X bits.

Step3. And the original image or cover image with 240 which is 11110000 so four LSB's set to 0. Because of this only four LSB's considered further.

Step4. The shifted hidden image and the result of step 3 are bitored. This makes changes only in the X LSB bits so that the image is hidden in the original image.

In MATLAB we convert it to uint8 format. This image can be called as the stego-image.

Extraction process

Input: An $m \times n$ carrier image and an $m \times n$ stego-image.

Output: a secret message/image.

Algorithm: Steps-

Step1: The stego-image is bit shifted by 4 bits since it was shifted by 4 bits to insert it into the original image.

Step2: The image is the ANDED with 255 i.e., 11111111, which gives the original image. It is ANDED with 255 because initially all the LSB's were made 0. Now it is recovered back.

Step3: To get it to uint8 format, we convert it back to uint8 which is the extracted image.

2.2 DCT and DWT Techniques: These techniques come under the frequency domain steganography. In frequency domain steganography, secret data is hidden in significant areas of covered image, which makes data invigorated to attacks such as compression, cropping or image processing methods than LSB approach. This provides an improved security level to steganography technique and leads to the development of algorithms. The various transforms include DCT, DWT and DFT. For a typical image, most of the visually significant data about the image is concentrated in just a few coefficients of the DCT. This is the property of DCT for a typical image. Due to this reason, the DCT is often used in image compression applications. DWT is the multiresolution analysis that enables us to detect image patterns that are invisible in the raw data. Wavelet Transform (WT) converts spatial domain information to the frequency domain information. Wavelets are used in image because wavelets separately partition the high frequency and low frequency information pixel by pixel. This method mainly addresses the capacity and robustness of the data hiding system.

The figure below shows the block diagram of DCT Technique:

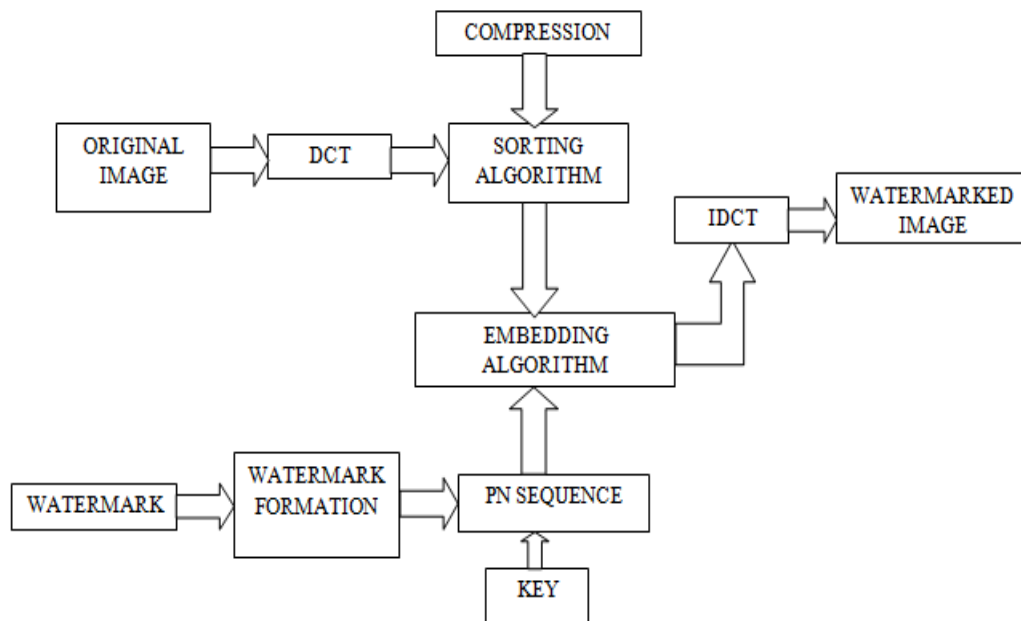


Figure 2.2.1: Block diagram of DCT Technique

Figure 2.2.1 depicts the steganography technique using Discrete Cosine Transform. In this DCT is applied to original image and then watermark is embedded in the image using various algorithms. In order to get back the image in spatial domain, we perform IDCT.

PROPOSED ALGORITHM FOR DCT TECHNIQUE

Embedding Procedure

Input:

An $m \times n$ carrier image and a secret message/image.

Output: an $m \times n$ stego-image.

Algorithm: Steps-

- Step1. Set minimum coefficient difference.
- Step2. Set the size of the block in cover to be used for each bit in watermark.
- Step3. Read in the cover object.
- Step4. Determine the size of cover object.
- Step5. Determine the maximum message size based on cover object, and block size.
- Step6. Read in the message image.
- Step7. Reshape the message to a vector.

- Step8. Check that the message is not too large for cover, if length of message is greater than maximum message size error message is displayed.
- Step9. Pad the message out to the maximum message size with ones.
- Step10. Generate shell of watermark image.
- Step11. Process the image in blocks. Encode such that $(5,2) > (4,3)$ when $message(x)=0$; and that $(5,2) < (4,3)$ when $message(x)=1$.
- Step12. In loop
 Transform block using DCT.
 If message bit is 0 then $(5,2) > (4,3)$
 If message bit is 1 then $(5,2) < (4,3)$
 If the above cases are not satisfied then we need to exchange them.
 Now we adjust the two values such that their difference $>$ coefficient difference set in step 1.
 Transform block back into spatial domain using IDCT2.
 Move on to next block, at end of row move to next row.
- Step13. Convert to 8 bit integer using uint8 and write the watermark image out to a file.
- Step14. Display processing time.
- Step15. Calculate PSNR and display it.
- Step16. Display the watermarked image.

Secret Image Recovery Mechanism

Input:

An $m \times n$ carrier image and an $m \times n$ stego-image.

Output: a secret message/image.

Algorithm: Steps-

- Step1. Clear all.
- Step2. Save start time.
- Step3. Set the size of the block in cover to be used for each bit in watermark.
- Step4. Read in the watermarked object.
- Step5. Determine the size of watermarked image.
- Step6. Determine maximum message size based on cover object, and block size.
- Step7. Read in the original watermark.
- Step8. Determine the size of the original watermark.
- Step9. In loop process the image in blocks.
 Transform block using DCT
 If $dctblock(5,2) > dctblock(4,3)$ then $message(x) = 0$ else $message(x)=1$.
 Move to the next block and at the end of the row move to the next row.
- Step10. Reshape the embedded message.
- Step11. Display processing time.
- Step12. Display the Recovered message.

The figure below shows the block diagram of DWT Technique:

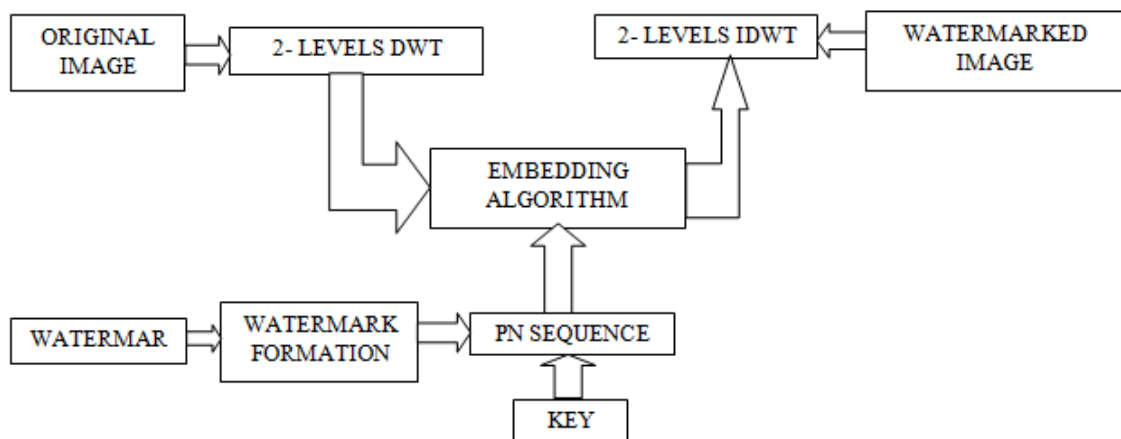


Figure 2.2.2: Block diagram of DWT Technique.

Figure 2.2.2 depicts the steganography technique using Discrete Wavelet Transform. In this DWT is applied to original image and then the watermark is embedded in image using embedding algorithm. In order to get image back in spatial domain, we perform IDWT

PROPOSED ALGORITHM FOR DWT TECHNIQUE

Embedding Procedure

Input: An $m \times n$ carrier image and a secret message/image.

Output: An $m \times n$ stego-image.

Algorithm: Steps-

Step1. Read the cover image (I_c).

Step2. Calculate the size of I_c .

Step3. Read the secret image (I_m).

Step4. Prepare I_m as message vector.

Step5. Decompose the I_c by using Haar wavelet transform.

Step6. Generate pseudo-random number (P_n).

Step7. Modify detailed coefficients like horizontal and vertical coefficients of wavelet decomposition by adding P_n when message bit = 0.

Step8. Apply inverse DWT.

Step 9. Prepare stego image to display.

Secret Image Recovery Mechanism

Input:

An $m \times n$ carrier image and an $m \times n$ stego-image.

Output: a secret message/image.

Algorithm: Steps-

Step1. Read the cover image (I_c).

Step2. Read the stego image (I_s).

Step3. Decompose the I_c and I_s by using Haar wavelet transform.

Step4. Generate message vector of all ones.

Step5. Find the correlation between the original and modified coefficients.

Step6. Turn the message vector bit to 0 if the correlation value is greater than mean correlation value.

Step7. Prepare message vector to display secret image.

III. APPLICATIONS:

The main application fields of steganography are:

- **Copyright Protection:** Most of the image steganographic techniques like digital watermarking can be used to protect a copyright on information. The photo collections and videos, sold on CDs and DVDs, often have hidden messages in the photos and videos respectively which allow detection of unauthorized use and hence disallow copying of protected CDs and DVDs.
- **Feature Tagging:** The data hiding technique can be used for feature tagging which helps in describing an item in a browser and also helps in allowing it to be found again by browsing or searching. The data hiding technique allows the metadata to move with the image regardless of the document format and image state (digital or analog).
- **Secret Communication:** The secret communication can be done with more security by using various steganographic techniques. The data to be send is hidden in cover image in order to get the stego-image and this stego-image is to be send to the destination and the hidden message is recovered back.
- **Use by defence:** The image steganography techniques are used by defence for embedding the important information into images where the distortion of the original image is not allowed, such as military imagery.
- **Intelligence services:** The confidential data with no change in intelligence services can be send by using most steganographic techniques. These data hiding techniques provide high security.
- **Steganography printers:** The steganography printer leaves a digital watermark on every single printed page, and allows us to identify the device with which a file was printed and also gives clues to the creator.

- **Web based applications:** In web based applications, security is supposed as a main issue and poses new challenges related to providing secure and reliable data transmission over unreliable service providers. Steganography helps us to provide the solution to these issues.

IV. LITERATURE SURVEY:

Ritija Kakade, et al [1] introduced a new steganography technique that can be applied to secure the data during transmission. Also the data can be added in QR code for the ease of access of sending information. The various techniques of steganography used are the DWT technique and LSB steganography. The data to be steganographed had been encrypted using AES algorithm to improve the security.

Marwan Ali Albahar, et al [2] gave two solutions in data security field for ensuring that only legitimate receivers will have access to the intended data: steganography and cryptography. These solutions provided a high level of security. With the exponential growth of challenges in the field of computer security, the use of Bluetooth technology is expanding rapidly to expose many of these challenges on the surface. The MITM attack during Bluetooth pairing process is one of these challenges. A novel method based on steganography was introduced in order to secure the pairing process and prevent MITM attacks.

Sujarani Rajendran, et al [3] proposed a new symmetric key based image hiding technique. Pseudo random keys are generated by using 1D logistic map and those keys are used for choosing the pixel position of cover image randomly for hiding the secret image. The main security part of the projected method is the selection of pixel position in the cover image. Peak Signal Noise Ratio (PSNR) and Mean Square Error (MSE) measures are used for comparison and the result analysis showed that the proposed scheme provided efficient level of security.

Vijay Kumar Sharma, et al [4] reviewed the steganographic techniques and their uses and attacks on these. The steganography is commonly known as covert writing and mainly used in hidden communication. A reliable internet communication is free from the attacks if steganography is used.

Vandana Yadav, et al [5] used new technique for steganography in a HSI color cover images, which hides secret message in the edges of the carrier images using 2-bit LSB substitution for embedding. To get true edges, canny edge detection technique has been used. The amount of data to be embedded plays an important role on the selection of edges. The main advantage of using HIS color mode is that it produced a image with a significantly large file size hence we hide large amount of confidential message. The proposed technique had better and higher embedding capacity.

Mirza Abdur Razzaq, et al [8] blended security technique using encryption, steganography and watermarking. By using large secret key, the original image has been encrypted through XOR operation by rotating pixel bits to right. For steganography, encrypted image has been changed by least significant bits (LSBs) of the cover image and we obtained stego image. In order to ensure the ownership, the stego image has been watermarked in the time domain and frequency domain. The proposed approach is efficient, simpler and secured and it provided significant security against threats and attacks.

Wid A. Awadh, et al [10] presented a new text steganography approach for hide loaded secret English text file in a cover English text file to ensure security of data in cloud computing. The proposed approach improved data security, data hiding capacity, and time.

Mandeep Kaur, et al [11] used three different techniques such as Huffman encoding, Deoxyribonucleic acid and State Transition. Initially, for the compression, Huffman is applied over the text, and then for the encryption, Deoxyribonucleic acid is applied over the compressed data and lastly for updating the location in the image, State Transition algorithm has been used. The application of these algorithms provided high security in comparison with the traditional algorithms. The implementation of these algorithms is done with respect to message bits. Total three images are used for the evaluation of traditional and proposed techniques in which the message bit varies from fifty to hundred. The simulation analysis concluded that the proposed method is efficient, more secure and proficient in comparison with other techniques such as LSBs, LF-DCT and MF-DCT. The parameters PSNR and MSE are used for the evaluation of their performance.

Muhammad Zaheer, et al [12] used compressed sensing theory for the security and payload capacity enhancement of an image steganography system for an audio message. However, in order to make use of compressed sensing, there is the conversion of audio message into an equivalent grayscale image which is sparsified using 2D-DCT and thresholding. Further, the sparsified image is compressed using the proposed compressed sensing algorithm and due to which not only the security was enhanced but also the payload capacity was improved; without losing imperceptibility of the system. The pixels of the cover image are chosen chaotically and the compressed image is embedded in those pixels. In order to reconstruct the grayscale image which is then converted back to the audio message, the compressed sensing reconstruction algorithm is used at the receiver end. The proposed system has high imperceptibility, high security and robust against different image processing attacks. The secret audio message has high PSNR value after reconstruction.

Saher Manaseer, et al [14] worked with a new technique to embed the secret message into colored images. Two versions of the proposed algorithm, named standard LSB and Condition Based LSB respectively, were used. The proposed method measured PSNR (Peak Signal to NOISE Ratio) and MSE (Mean Squared Error) for the two versions that showed the standard LSB version outperforms the Based LSB version.

Brij Mohan Kumar, et al [6] presented a cryptography based technique to authenticate the images and is used to prevent image forgery. Digital Revolution has sparked a renewed interest in the field of cryptography. It focused specifically on the techniques employed in hiding information in digital image files.






Harini .V, et al [7] proposed a method to enhance the security by embedding data in colour images. The cover image is first converted to any one plane process and encrypted by using Chaos encryption. Adaptive LSB replacement algorithm is used for hiding the secret message bits into the encrypted image. The significant key is used to extract the secret data. The technique is particularly helpful in applications such as medical and military imaging. The proposed methodology provided better performance in terms of number of slices, number of IOBs and is implemented in FPGA (field programmable gate array). The design architecture when implemented on FPGA Spartan III offered high processing speed. In the area of Secure Communication, this method gave an impulse for the researchers to a very fast, programmable & cost effective hardware solution.



Mr. Jayesh Sharma, et al [13] reviewed different security and data hiding techniques that are used to implement a steganography such as LSB, ISB, MLSB etc.

V. RESULTS AND DISCUSSION

The algorithms are tested in MATLAB. The result with cover image and secret image are shown. The cover image size is 256x256 and secret image size is 32x32. Comparative analysis LSB based, DCT based & DWT based steganography has been done on basis of parameters like PSNR, MSE on images shown below in table A and the results are evaluated. If PSNR ratio is high then images are of best quality.

Table A: Comparison of LSB, DCT and DWT Techniques on the basis of PSNR and MSE Values.

COVER IMAGE	LSB	DCT	DWT
	PSNR: 22.7209 MSE: 50.2601	PSNR:34.3621 MSE:24.0031	PSNR: 24.5075 MSE:232.1313
	PSNR: 22.7209 MSE: 50.2601	PSNR:31.1742 MSE:50.0105	PSNR: 24.5075 MSE: 232.1313
	PSNR: 22.8421 MSE:40.6178	PSNR:33.8497 MSE:27.0089	PSNR:24.5075 MSE:232.1313
	PSNR: 31.2671 MSE: 48.5695	PSNR: 5.9840 MSE: 16393.7978	PSNR: 24.4734 MSE: 232.1312
	PSNR: 32.2707 MSE: 38.5483	PSNR: 1.4817 MSE: 46228.151	PSNR: 24.4734 MSE: 232.1312

	PSNR: 31.1147 MSE: 50.3039	PSNR: 2.9079 MSE: 33287.458	PSNR: 24.4734 MSE: 232.1312
	PSNR: 32.3735 MSE: 37.6464	PSNR: 9.4436 MSE: 7391.25	PSNR: 24.4734 MSE: 232.1312

VI. EVALUATION OF IMAGE QUALITY

For comparing stego image with cover results requires a measure of image quality, commonly used measures are Mean-Squared Error, Peak Signal-to-Noise Ratio.

A. Mean-Squared Error: The mean-squared error (MSE) between two images $I_1(m,n)$ and $I_2(m,n)$ is:

$$MSE = \frac{\sum M, N [I_1(M, N) - I_2(M, N)]^2}{M * N}$$

M and N are the number of rows and columns in the input images, respectively. Mean-squared error depends strongly on the image intensity scaling. A mean-squared error of 100.0 for an 8-bit image (with pixel values in the range 0-255) looks dreadful, but a MSE of 100.0 for a 10-bit image (pixel values in [0,1023]) is barely noticeable.

B. Peak Signal-to-Noise Ratio: Peak Signal-to-Noise Ratio (PSNR) avoids this problem by scaling the MSE according to the image range.

$$PSNR = 10 \log_{10} \frac{256^2}{MSE}$$

PSNR is measured in decibels (dB). PSNR is a good measure for comparing restoration results for the same image, but between images comparisons of PSNR are meaningless.

VII. CONCLUSION

The main objective of image steganography is to conceal the secret data using cover images. In this research three different techniques of steganography viz LSB, DCT, DWT are applied to various digital images and respective PSNR and MSE values are calculated. From the calculation of these error metrics we get to know the effect of noise during transmission. If PSNR ratio is high then images are of best quality. The technique which has the highest PSNR and lowest MSE values for the particular digital image should be used for steganography. For different digital images we get different results. This is because incase of LSB, the PSNR values depend on the information bits. Also PSNR depends on the pixel intensity change from the original image and the stego image. For DCT technique, the PSNR value depends on image formats (that are .jpg, .bmp, .png) and hence different values for different images. But in case of DWT, the values are same because DWT explicitly focuses on size. Since size of every image is 256x256 and hence the values are same.

REFERENCES

- [1]. Ritija Kakade, Nikita Kasar, Shruti Kulkarni, Shubham Kumbalpuri, Sonali Patil, "Image Steganography and Data hiding in QR code", IRJET, Vol 04, 2017.
- [2]. Marwan Ali Albahar, Olayemi Olawumi, Keijo Haataja, Pekka Toivanen, "A novel method for Bluetooth pairing using Steganography", IJITS, No. 1, Vol 09, 2017.
- [3]. Sujarani Rajendran, Manivannan Doraipandian, "Chaotic Map Based Random Image Steganography using LSB Technique", IJNS, Vol 19, No.4, 2017.
- [4]. Vijay Kumar Sharma, Dr. Devesh Kr Srivastava, Dr. Pratistha Mathur, "A Study of Steganography based data hiding techniques", IJERMT, Vol 6, 2017.
- [5]. Vandana Yadav, Sanjay Kumar Sharma, "A new approach for Image Steganography using Edge Detection Method for Hiding Text in Color Images using HSI Color Model", IJSRSET, Vol 03, 2017.
- [6]. Brij Mohan Kumar, Prof. Y.S Thakur, "An Introduction to Steganographic Techniques in the field of Digital Image Processing", IJESC, Vol 07, 2017.

- [7]. Harini.V, Vijayaraghavan, “FPGA Implementation of Secret Data Sharing through Image by using LWT and LSB Steganography Technique”, IJESC, Vol 07, 2017.
- [8]. Mirza Abdur Razzaq, Mirza Adnan Baigh, Riaz Ahmad Shaikh, Ashfaque Ahmad Memon, “Digital Image Security: Fusion of Encryption, Steganography and Watermarking”, IJACSA, Vol 08, No. 5, 2017.
- [9]. D. Suneetha, Dr. K. Kiran kumar, “A Novel Algorithm for Enhancing the Data Storage Security in Cloud through Steganography”, ACST, Vol 10, No. 9, 2017.
- [10]. Wid A. Awadh, Ali S. Hashim, “Using Steganography for secure data storage in cloud computing”, IRJET, Vol 04, 2017.
- [11]. Mandeep Kaur, Rupinder Kaur Randhawa, “Hybrid approach for improving data security and size reduction in Image Steganography”, IRJET, Vol 04, 2017.
- [12]. Muhammad Zaheer, I.M Qureshi, Zeeshan Muzaffar, Laeeq Aslam, “Compressed Sensing Based Image Steganography System for secure transmission of Audio message with Enhanced Security”, IJCSNS, Vol 17, No. 7, 2017.
- [13]. Mr. Jayesh Surama, et al, “Steganography Techniques”, IJEDR, Vol 05, 2017.
- [14]. Saher Manaseer, Asmaa Aljawawdeh, Dua Alsoudi, “A New Image Steganography Depending on Reference and LSB”, IJAER, Vol 12, No. 9, 2017.
- [15]. Divya Suryawamshi, Meetali Salvi, Soumya Pandey , “Image Steganography for criminal cases”, IJEDR, Vol 05, 2017.
- [16]. Mamta Yadav, Amita Dhankar, “Image Steganography Techniques: A Review”, IJRST, Vol 2, 2015.
- [17]. Ashadeep Kaur, Rakesh Kumar, Kamaljeet Kainth, “Review Paper on Image Steganography”, IJARCSSE, Vol 6, 2016.
- [18]. Rakhi, Suresh Gawande, “A Review on Image Steganography methods”, IJAREEIE, Vol 2, 2013.

IOSR Journal of Engineering (IOSRJEN) is UGC approved Journal with Sl. No. 3240, Journal no. 48995.

Miftah Ul Uroos, " Steganography: A Comparative Survey Conducted on Digital Images" IOSR Journal of Engineering (IOSRJEN), vol. 08, no. 10, 2018, pp. 52-61.