

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

Image Steganography Using Hybrid Method LWT-DWT-SVD

Shallu Vohra¹, Binay Binod Kumar²

P.G. Student, Department of Electronics & Communication Engineering Gateway Institute of Engineering & Technology, Sonipat, Haryana, India¹

Assistant Professor, Department of Electronics & Communication Engineering Gateway Institute of Engineering & Technology, Sonipat, Haryana, India²

ABSTRACT: Steganography (pronounced STEHG-uh-NAH-gruhf-ee, from Greek *steganos*, or "covered," and *graphie*, or "writing") is the hiding of a secret message within an ordinary message and the extraction of it at its destination. Steganography techniques is used to hide the message inside common media, like photo, video, audio etc. Steganography techniques using spatial and transform domain are common in use. Both domain having their advantages as spatial domain gives better capacity and transform gives more robustness than spatial domain. So both capacity and robustness can be achieves by using both domain in single hybrid method. In this paper a novel method is described for image steganography is LWT-DWT-SVD. Experimental result shows that is method is more effective than existing method LWT-DCT-SVD. MSE, PSNR and correlation are the parameters used to measure effectiveness of methods. And effectiveness method also check against different value of noise attack on stego image.

KEYWORDS: Lifting Wavelet Transform, Discrete Wavelet Transform, Singular Value Decomposition, MSE, and PSNR.

I. INTRODUCTION

Steganography is by no means a modern practice. Simply meaning "covered writing". It is the way of hiding messages within other messages in order to cove the existence of the original. Examples of its use can be found throughout history, dating as far back as ancient Greece. Steganography has developed a lot in recent years, because digital techniques allow new ways of hiding information inside other information, and this can be valuable in a lot of situations. However, with growth of digital media use for data exchange and communication today providing great hosts for steganographic communication, interest in this practice is increase now days abundantly [3]. Steganography is a technique of sending secret information. Thus, no one excepting the sender and the intended recipient knows about the existence of the message. If the existence of hidden information in some steganography file is revealed, its content can easily be read. The advantage of steganography is the fact that a hidden message does not attract attention. On the other side the goal of cryptography is to make data unreadable by a third party, Encrypted messages, no matter how undecipherable, will induce suspicion. Thus, while cryptography protects the contents of the message, the steganography hides the message itself. The existence of the secret images, images with embedded information, can be detected by a specialized algorithm, named steganalysis. The steganographic algorithms have been detected by steganalysis algorithms and that more robust information protection approaches should be used. Steganography has various useful applications. However, like any other science it can be used for ill intentions.

II. RELATED WORK

This section will provide the brief description and highlights the contribution, remarks and factors of the work done by researchers.

1. Md. Maklachur Rahman, in this paper, an idea of watermarking is proposed and implemented. In proposed watermarking method, the original image is rearranged using zigzag sequence and DWT is applied on

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

rearranged image. Then DCT and SVD are applied on all high bands LH, HL and HH. Watermark is then embedded by modifying the singular values of these bands.

2. Prerna Gupta and Girish Parmar, in this paper, a non-blind watermarking scheme based on IWT and SVD has been implemented. Modifying singular values of the host image in IWT domain provides high robustness and simultaneously also increases the value of transparency. This technique can embed the watermark into salient features of the image using variable scaling factor.
3. Dipalee Borse, Shobnana patil, in this paper we have studied different transform domain steganographic methods. In Transform domain we focused on two major techniques are discrete cosine transform and discrete wavelet Transform. DCT in image processing is mainly used for compression of JPEG image. With steganography it provides greater security but the data embedding capacity is less than spatial domain techniques.
4. Parmar Ajit Kumar Maganbhai, Prof. Krishna Chouhan, in this review article we have studied and analyzed the different methodologies from various researchers in their research. The main goal of image steganography is to hide the existence of the data message from illegal intention. A novel, robust and secure hiding schemes that can resist steganalytic detection must be implemented.
5. N.D. Jambhekar, C.A. Dhawale, this paper focuses on some image steganographic methods used from many years, the methods used currently and the capabilities of steganography in future. In this paper discuss spread spectrum. Statistical method and transform domain for image steganography. The effectiveness of the steganographic algorithms will be increased by Security Enhancement discuss in this paper such as efficient embedding, reducing distortion, and suitable cover selection. Therefore, no any type of steganographic attack breaks the security mechanism implemented by the advanced steganographic algorithm.
6. Shikha, Vidhu Karan Dutt, this paper intends to give an overview of image steganography, its uses and techniques. It also show how a text document to be hide in an image file. The image steganography various methods have been proposed. In this paper, we propose a method that hide the secret messages in the image using matlab. Matlab in not only a programming language, but a programming environment as well. It is provide more security for secret communications. Thus the capacity of the hiding process to hide secret messages is also high in the proposed technique.

III. TYPES OF STEGANOGRAPHY BASED ON COVER MEDIA

Steganography basically divides in four category text, audio, video and image. In text steganography the cover media is text message and secret message hide inside cover text. The message can be hidden in cover text by word shifting, line shifting, syntax, semantic or abbreviation based hiding techniques. A video is a combination of images and optionally sound. So, huge amount of secret data can be encoded in video files using steganography. Video files such as MPEG, MP4, and AVI etc. can be used for hiding secret information. In audio steganography a digital sound file such as MP3 or WAV can be used to embed secret message by shifting of binary sequence of that file.

In the case image steganography when cover media is an image file, it is called image steganography. In this type of steganography, the image files such as JPEG, GIF, BMP, PNG etc. are used to embed secret bits of information. Image steganography can be accomplished by exploiting the image format, spatial domain steganography, frequency domain steganography and adaptive steganography.

IV. IMAGE STEGANOGRAPHY IN MODERN TIME

Today is the era of digital processing, so steganography is now digital steganography. In digital image steganography following terminology is used:

Cover Image: The cover image is the carrier in which the secret data is hidden such as an image file.

Payload: The secret image to be hidden in cove image.

Stego Image: The image with embedded payload.

Steganography: The process using which the payload is embedded in the cover image.

Steganalysis: An attack on stego media using which the hidden payload is to be extracted from.

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

A. Concept of Image Steganography

Every image steganography includes the hiding image which is known as embedding process and extraction process for recovery of secret image that is hide under the cover media. In image steganography process secret image is hide under cover image using selected embedding algorithm. Embedded image is known as stego image. Which is transmit through communication channel and then recovery of secret image at destination is inversion of embedding process which is called extraction process. Various types of embedding methods available for image steganography.

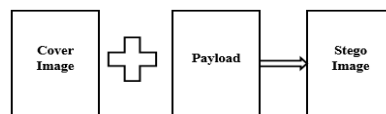


Fig. 1. Embedding process.

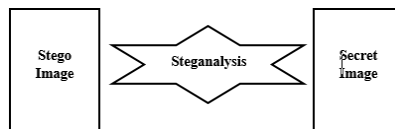


Fig. 2. Extraction process.

V. TECHNIQUES USED FOR STEGANOGRAPHY ALGORITHM

Lifting wavelet transform (LWT), discrete wavelet transform (DWT) and singular value decomposition (SVD) techniques used for hybrid proposed method for image steganography.

A. Discrete wavelet Transform

Discrete Wavelet Transform is used for digital images. Many DWTs are available. Depending on the application most suitable one should be used. Such as to hide text information integer wavelet transform can be used. When DWT is applied to an image it is decomposed into four sub bands: LL, HL, LH and HH. The LL part contains the most significant features. So if the information is hidden in LL part, the stego image is not much affected by the compression or other manipulations. Sometimes distortion may be produced in the stego image and then other sub bands can be used [12]. A two level DWT decomposition process is shown in Fig. 1.

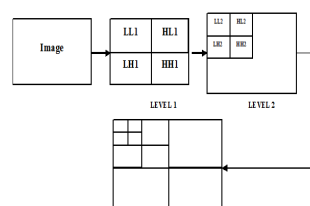


Fig. 3. DWT component

The function being expanded is discrete (i.e., a sequence of numbers), the resulting coefficients are called discrete wavelet transform (DWT). For example, if $f(n) = f(x_0 + n \Delta x)$

For some $x_0, \Delta x$, and $n = 0, 1, 2, \dots, M-1$, the wavelet series expansion coefficients for $f(x)$, the forward DWT coefficients for sequence $f(n)$.

$$W_{\phi}(j_0, k) = \frac{1}{\sqrt{M}} \sum_n f(n) \phi_{j_0, k}(n) \quad (1.1)$$

$$W_{\psi}(j, k) = \frac{1}{\sqrt{M}} \sum_n f(n) \psi_{j, k}(n) \quad \text{For } j \geq j_0 \quad (1.2)$$

The $\phi_{j_0, k}(n)$ and $\psi_{j, k}(n)$ in these equations are sampled version of basis functions $\phi_{j_0, k}(x)$ and $\psi_{j, k}(x)$ and $n=0, 1, 2, \dots, M-1$. Thus we employ m equally spaced samples over the support of the basis functions [2].

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

B. Wavelet Shifting Scheme

Lifting scheme is an effective way to of implementation of the wavelet filtering which also improves the speed of wavelet transform method. In the lifting scheme for the haar transform the prediction step predicts that odd element will be equal to the even element. The difference between the even value (the predicted element) and the actual value of the odd value replaces the odd element. For the forward transform iteration j and element i , the new odd element, $j+1,i$ would be [1].

$$\text{odd}_{j+1,i} = \text{odd}_{j,i} - \text{even}_{j,i} \quad (1.3)$$

In the haar transform which is based on lifting scheme the update step average of the even\odd pair (e.g., the even element S_i and its odd successor, S_{i+1}).

$$\text{even}_{j+1,i} = \frac{\text{even}_{j,i} + \text{odd}_{j,i}}{2} \quad (1.4)$$

The original value of add element has been replaced by the difference between this element and its predecessor. Simple algebra lets us the original value.

$$\text{odd}_{j,i} = \text{even}_{j,i} - \text{odd}_{j+1,i} \quad (1.5)$$

Putting this into the average we get.

$$\text{even}_{j+1,i} = \text{even}_{j,i} + \frac{\text{odd}_{j+1,i}}{2} \quad (1.6)$$

$$\text{even}_{j+1,i} = \text{even}_{j,i} + \frac{\text{odd}_{j+1,i}}{2} \quad (1.7)$$

The averages of even elements become the input for next iterative step of the forward transform. This shown in Fig. 4 below.

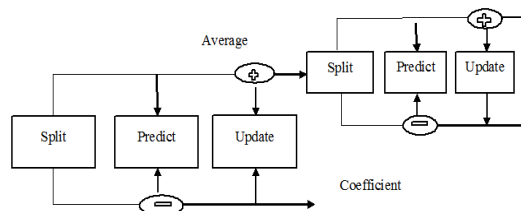


Fig. 4. 4 Step of 16 elements wavelets transform.

Fig. 5.

The split phase that starts with each forward transform. step moves and odd elements to the second half of the array, leaving the even elements in the lower half. At the end of the transform step the odd elements are replaced by the differences and the even elements are replaced by the averages. The even elements become the input for the next step, which repeatedly starts with the split phase. The result of the forward transform of lifting scheme haar transform is shown in Fig. 5. The starting element in the array contains the data average. The differences (coefficients) are ordered by increasing frequency.

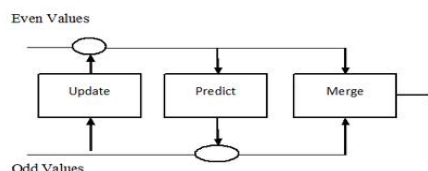


Fig. 6. Result of a wavelet transform with coefficient.

One of the elegant features of the lifting scheme is that the inverse transform is a mirror of the forward transform. In the case of the haar transform, additions are replaced by subtractions and subtractions by additions. The merge step replaces the split step [1].

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

C. Singular Value Decomposition

From the discernment of image processing, an image can be viewed as a matrix with non-negative scalar entries. SVD is an effective numerical analysis tool from linear algebra to decompose a rectangular matrix “A” into an orthogonal matrix U, diagonal matrix S, and the transpose of an orthogonal matrix V. SVD decomposes a given image A of size M×N as This decomposition (SVD) of A , and can be written as.

$$SVD(A) = [UDV] \tag{1.8}$$

$$SVD(A) = \lambda_1 U_1 V_1^T + \lambda_2 U_2 V_2 + \dots + \lambda_n U_n V_n^T \tag{1.9}$$

$$SVD(A) = UDV^T \tag{2.0}$$

Where, U and V are orthogonal matrices of size M×M and N×N, respectively. S is a diagonal matrix of size M×N having singular values. The columns of U are called the left singular vector of A, and the right singular vector of A. Calculating the SVD consist of finding the eigen values and eigen vectors of AA^T and $A^T A$. The eigen values vectors of AA^T make up the columns of V, the eigen vectors of $A^T A$ make up the columns of U. Also, the singular values in S are square root of eigen values from AA^T or $A^T A$. The singular values are diagonal entries of the S matrix and are arranged in descending order. The singular values are always real number. If the matrix A is real matrix , then U and V are also real It is worth noting that, the singular vectors of an image specify the image “geometry” similarly, left singular vectors represent horizontal details and right singular vectors represent the vertical details of an image, while the singular values specify the “luminance” (energy) of the image. Slight variations in the singular values do not affect the visual perception of the quality of the image [5].

VI. PROPOSED ALGORITHM

A novel proposed algorithm using techniques LWT, DWT and SVD is presented here of improved image steganography which is more effective than existing method LWT-DCT-SVD. The proposed method made of embedding and extracting process of the image described below by flow chart and then by embedding and extracting algorithm. Here embedding process for the formation of stego image and extraction process for recovery of secret image.

A. Embedding Process Flow Chart

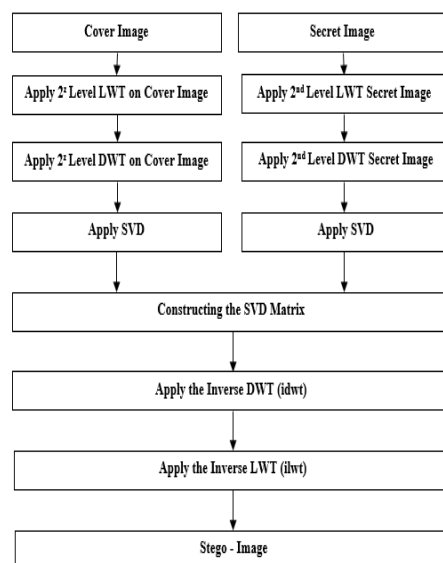


Fig. 7. Embedding process flowchart.

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

B. Extraction Process Flow Chart

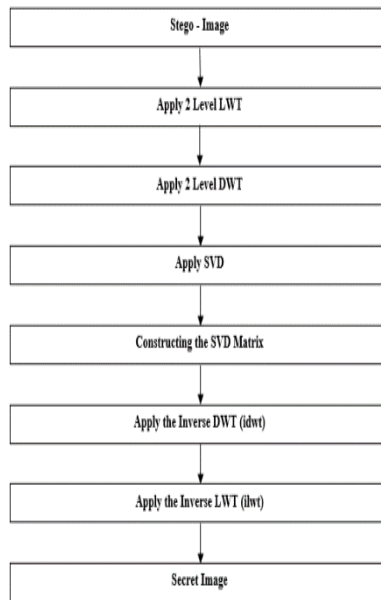


Fig. 8. Embedding process flowchart.

C. Algorithm for Embedding Process for Method LWT-DWT-SVD

Step1: Input cover image.



Fig. 9. Cover image.

Step2: Apply 1st level LWT on cover to decompose into four sub bands LL1, HL1, LH1, and HH1.



Fig. 10. 1st level LWT.

Step3: Apply 2nd level LWT on sub-band LL1 to decompose into four sub-bands LL2, HL2, LH2, and HH2.



Fig. 11. 2nd level LWT.

Step4: Apply 2 level DWT on sub – band (LL2).

Step5: Apply SVD on DCT sub-band of cover image $[U_y, S_y, V_y] = \text{svd}(x_r)$.

Step6: Input secret image



Fig. 12. Secret image.

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

Step7: Apply 1st level LWT on Secret image to decompose into four sub-bands L_L1, HL_1, LH_1, and HH_1.



Fig. 13. 1st level LWT.

Step8: Apply 2nd level LWT on (L_L1) sub-band to decompose into four sub-bands L_L2, HL_2, LH_2, and HH_2.



Fig. 14. 2nd level LWT.

Step9: Apply 2 level DWT on sub-band (L_L2) sub band to decompose into four sub-bands L_L4, H_L4, L_H4, and H_H4.

Step10: Apply SVD on DWT sub-band of secret image, $[U_w, S_w, V_w] = \text{svd}(L_{L4})$.

Step11: Embedding image using equation, $S_{mark} = S_y + \alpha * S_s$.

Step11: Rebuild SVD matrix using equation, $LLL_1 = U_y * S_{mark} * V_y'$.

Step12: Apply inverse DWT (iDWT) on (LLL_1).

Step13: Apply 2 level inverse LWT (iLWT) on DWT inverse image (LL2_1) to get stego image.



Fig. 15. Stego image.

D. Algorithm for Extraction Process for Method LWT-DWT-SVD

Step 1: Input the stego image (LL4_1).

Step 2: Apply the 2nd level LWT on stego image (LL4_1) to decompose the image into four sub-bands LL2_sm, HL2_sm, LH2_sm, and HH2_sm.

Step 3: Apply DWT on sub-band of 2nd level LWT (LL2_sm).

Step 4: Apply SVD on DWT image (LL4_sm) and modify the matrix by using equation $S_{My} = U_s * S_{wrec} * V_s'$.

Step 5: Apply 2 level Inverse DWT (iDWT) on SVD matrix.

Step 6: Apply 2 level inverse LWT (iLWT) to sub-band to get extracted image.



Fig. 16. Secret image.

VII. PROPOSED ALGORITHM

The attack on steganography in images are broadly categorized in two types. Unintentional common signal processing and image manipulation and intentional attack by malicious attacker

A. Unintentional Image Manipulation

For the image processing purpose many image manipulations/modification are commonly used by the artists/author in preparing material for printing and making it suitable for publication in the internet for distribution. Common image manipulations include image processing such as rotation, resizing, cropping, sharpening, filtering, compression, printing\scanning, geometric transforming, compositing\mosaicking, colour tablets etc. Again for Internet applications,

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

image segmentation called tiling is used. It is expected that any embedded steganographed claiming to be robust should survive any of these image manipulations and remain detectable in the manipulated image. An embedded steganography must survive any image manipulation that does not damage or destroy the image characteristics beyond usability for the purpose, otherwise, its credential as a security of intellectual property right (IPR) is doubtful and questionable [4].

B. Intentional Attack by Malicious Attack

The signal processing related attack such as de-noising remodulations, collusions, averaging types of attacks may be triggered by malicious attacker. Removal attacks are steganograph attack that aims at removing the secret signal from the steganographed image without attempting to break the security of the algorithm. These types of attack do not attempt to find out the encryption techniques used or how the images has been embedded. It results in a damaged steganographed image, hence a damaged message signal, where no post processing can recover the message from the attacked data. Noising, histogram equalization, blur and sharpen attacks are included in this category [4].

VIII. PEAK SIGNAL TO NOISE RATIO AND MEAN SQUARE ERROR

PSNR is used to measure the quality of reconstruction of lossy and lossless compression (e.g., for image compression). In this case original data is the signal, and the error introduced by embedding process is noise. PSNR is an approximation to human perception of reconstruction quality. Even though a higher PSNR generally related to the reconstruction is of higher quality, in some cases it may not. PSNR is most easily defined via the mean squared error. MAX_I is the maximum possible pixel value of the image. When the pixels are represented using 8 bits per sample, this is 256. Mainly, when samples are represented by using linear PCM with B bits per sample, MAX_I is $2^B - 1$. For color images with three RGB values per pixel, and for gray image the definition of PSNR is the same except the MSE is the sum over all squared value differences divided by image size [4].

$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i, j) - k(i, j)]^2 \quad (2.1)$$

$$PSNR = 10 * \text{Log} (256^2 / MSE) \quad (2.2)$$

IX. CORRELATION COEFFICIENT

Correlational Coefficient is the similarity between original image and the steganography image correlation coefficient is 1.0 for no rotational and noise attack is added to secret image. Correlation coefficient starts deteriorating. The mathematical formulation for computing correlation coefficient is equal.

$$r = \frac{n \sum xy - (\sum x)(\sum y)}{\sqrt{n \sum (x^2) - (\sum x)^2} \sqrt{n \sum (y^2) - (\sum y)^2}} \quad (2.3)$$

Where n is number of pairs of images (x & Y). The value of r is such that $-1 < r < +1$ the + and - signs are used for positive linear correlations and linear correlations and negative linear correlations respectively [4].

X. EXPERIMENT AND RESULTS

The algorithm for embedding and extraction is developed in MATLAB version 6 steganography. Baboon image used for the experiment purpose as secret image. The Lena image used for the experiment is a cover image of size 512X512 and secret image used is of size 512X512 gray scale. The Lena image is the host image, on which invisible secret message image is embedded. The result of the experiment shows the perceptibility of steganography image is not lost due to steganography it resemble the original secret image (Baboon).

Here first compare the mse and psnr value of existing method (LWT-DCT-SVD) and proposed method (LWT-DWT-SVD) of image steganography. Result shows that proposed method has more PSNR value than existing method. The proposed algorithm is tested against noise attacks such as "Gaussian", "Salt & Pepper" and "Speckle" noise attacks for different levels of noise density. For "Gaussian" the noise density is selected as 0.01, 0.001 and 0.0001. For "Salt &

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

Pepper” the noise density is selected as 0.1, 0.01 and 0.001. For “Speckle” noise is taken as 0.01, 0.001 and 0.0001. The results for applying three different types of noise attacks on the specified stego image are shown in Table I. As noticed, the proposed algorithm (LWT-DCT-SVD) can withstand all types of noise attack.

The algorithm has shown robustness in terms of the peak signal to noise ratio PSNR especially for the “Speckle noise” is 91.83% and for Salt & Pepper noise where 91.01 % of the secret image has been recovered for Baboon. The algorithm has also recovered, 83.77 % for the Gaussian attack. However, as the density of the noise increases, a degradation is noticed in the quality of the stego image and hence in the recovered secret image. For example, the PSNR for steganographed image 42.8094 to 255850 for an increase of the noise density from 0.0001 to 0.01. Similar conclusions follow from the other results in Table I. As expected in steganography applications, the results match the fact at lower value of noise density the steanographed image is less corrupted and PSNR value is high and with the addition of more noise density to the steganographed image the quality of the image deteriorates very much and PSNR value decreases. PSNR measures are estimates of the quality of a distorted image compared with an original reference image. As expected in steganography applications, the results match the fact that the degradation in the recovered image reflects the amount of degradation in the stego image. The below figures shows that stego image for Lena under increasing levels of “Gaussian”, “Salt & Pepper” and “Speckle noise” density and their corresponding recovered secret image. The below figures also shows that correspondence between the noise level and the degradation in the recovered secret image.



Fig. 17. (a) Cover image. (b) Secret image. (c) Stego image. (d) Recovered image.

```

Command Window

The MSE value is 1.4526
The PSNR value is 46.5092

The correlation value of stegoed image is 1.0000
The correlation value of extracted image is 1.0000
The MSE value of noised image is 17.8543
The PSNR value of noised image is 35.6474
    
```

Fig. 18. MSE, PSNR and correlation values for LWT-DCT-SVD method.

```

Command Window

The MSE value is 1.4284
The PSNR value is 46.5823

The correlation value of stegoed image is 1.0000>>
    
```

Fig. 19. MSE, PSNR and correlation values for LWT-DWT-SVD method.

TABLE I. COMPARISON OF PSNR AND MSE VALUES FOR BOTH METHODS

Table IS.No	Method	MSE	PSNR	Correlation Coefficient
1	LWT-DCT-SVD	1.4526	46.5432	1.000
2	LWT-DWT-SVD	1.4284	46.6163	1.000

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

TABLE II. PSNR AND MSE OF SALT & PEPPER NOISED ATTACK FOR METHOD LWT-DWT-SVD

S. No.	Value of Noise	MSE Value	PSNR Value
1	0.0001	3.7475	42.4274
2	0.001	21.8564	34.7690
3	0.01	185.0249	25.4925

TABLE III. PSNR AND MSE OF GAUSSIAN NOISED ATTACK FOR METHOD LWT-DWT-SVD

S. No.	Value of Noise	MSE Value	PSNR Value
1	0.0001	8.1487	39.0539
2	0.001	66.4675	29.9387
3	0.01	642.8995	20.0843

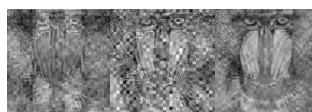
TABLE IV. PSNR AND MSE OF SPECKLE NOISED ATTACK FOR METHOD LWT-DWT-SVD

S. No.	Value of Noise	MSE Value	PSNR Value
1	0.0001	3.4319	42.8094
2	0.001	19.5614	35.2508
3	0.01	181.1251	25.5850



(a) (b) (c)

Fig. 20. (a) "Gaussian" noise attacked stego image (0.01). (b) "Salt & Pepper" noise attacked stego image (0.01). (c) "Speckle noise" attacked stego image (0.01).



(a) (b) (c)

Fig. 21. (a) Extracted image from "Gaussian" noise attack stego image. (b) Extracted image from "Salt & Pepper" noise attack stego image. (c) Extracted image from "Speckle" noise attack stego image.

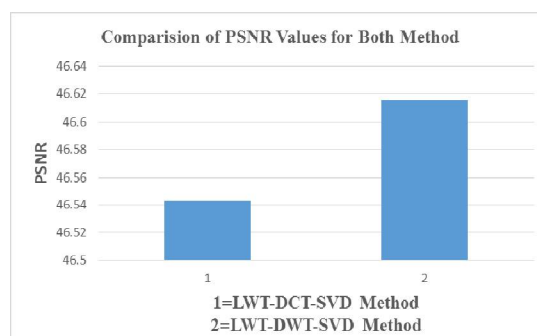


Fig. 22. Comparison chart of PSNR value for both method.

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

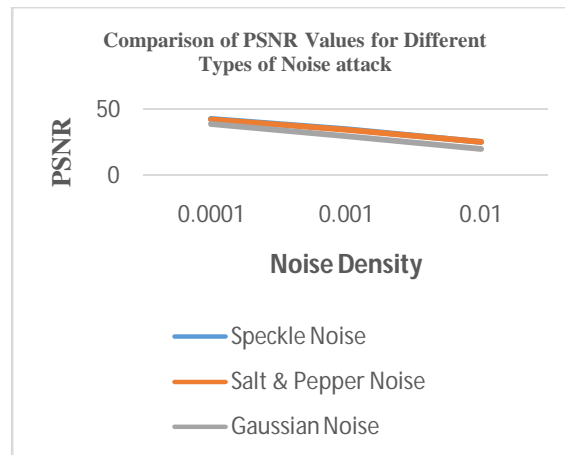


Fig. 23. Comparison graph for PSNR value of various noise attack on stego image for LWT-DWT-SVD method.

XI. CONCLUSION

In this work two approaches of steganography based on LWT-DCT-SVD and LWT-DWT-SVD are suggested. These proposed steganography algorithms using LWT, DWT, DCT and SVD transformation that contributes more robust in comparison with many steganography algorithms. Proposed method showed robustness to speckle, salt & pepper, Gaussian noise attacks. When the attacker is trying to remove the secret image, he will desperately distort the image to a degree makes it impossible to be used in any application. The proposed method LWT-DWT-SVD is more effective than existing method LWT-DCT-SVD. The steganographed image quality is good in terms of imperceptibility. All the results obtained for the recovered images and the stego image are identical to the original images. The methodologies are having robust efficiency of steganographed image with data hiding ability.

XII. FUTURE WORK

The proposed steganography algorithms using LWT, DWT, DCT and SVD transformation that contributes more robust in comparison with many steganography algorithms. In this work stego image is attacked by different types of noise but in future we can test the effectiveness of these methods against other types of attacks such as cropping, rotational and resizing. In future the proposed algorithms can be improved using full band LWT-DCT-SVD and LWT-DWT-SVD and further can be extended to color images and video processing.

REFERENCES

- [1] Rafael C. Gonzalez, Richard E. Woods, "Digital Image Processing", 3rd ed. Prentice Hall, pp. 278–364, 2008.
- [2] A. Jensen, Ander La Cour-Harbo, "Ripples in Mathematics", 1st ed. Springer-Verlag Berlin Heidelberg, pp. 11-25, 2001.
- [3] Orooba Ismaeel Ibraheem Al-Farajji "New Technique of Steganography Based on Locations of lsb" International Journal of Information Research and Review, Vol. 04, Issue, 01, pp.3549-3553, January, 2017.
- [4] Tapas Bandyopadhyay, B Bandyopadhyay, B N Chatterji, "Attacks on Digital Watermarked Images in the Internet Environment and their Counter Measure", Vol 4, No. 4, pp. 155-159, March-April 2013.
- [5] Jo. Cherian, Mereena, Achu Thomas. "A Survey on DWT and LWT based Digital Image Watermarking", International Journal of Research in Computer Applications & Information Technology Vol 4, Issue 3, pp. 27-32, May-June, 2016.
- [6] Parmar Ajit Kumar Maganbhai, Prof. Krishna Chouhan "A Study and literature Review on Image Steganography", International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 6 (1), pp. 685-688, 2015.
- [7] Sumathy Kingslin1, R. Anusuya2 "A Comparative Study on Pattern Based Image Steganography", International Journal of Computer Science and Engineering Communications, Vol.4, Issue.2, Page.1307-1310, 2016.
- [8] Amritpal Singh1, Satinder Jeet Singh2 "An Overview of Image Steganography Techniques", International Journal of Engineering and Computer Science, Volume 3 Issue, pp. 7341-7345, 7 July, 2014.
- [9] Md. Maklachur Rahman. "A DWT, DCT and SVD Based Watermaking Techniques to Protect the Image Piracy", International Journal of Managing Public Sector Information and Communication Technologies (IJMPICIT), Vol. 4, No. 2, June 2013.

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 8, August 2017

- [10] V.Uma, K.Vanishree. "A DWT based reversible watermarking for lossless recover", International Journal of Scientific and Engineering Research (IJSER), Volume 3, Issue 5, , pp.151-156, May 2012.
- [11] Anuradha Goswami, sarika Khandewal, "Hybrid DCT-DWT Digital Image Steganography", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 5, Issue 6, pp.228-233, June 2016.
- [12] Chakra Rao, Rudra Pratap Das, "Hybrid data hiding scheme in images using DWT, DCT and SVD", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 4, Issue 11, pp. 9322-9329, November 2015.
- [13] Nallagarla Ramamurthy, S. Varadarajan, "Effect of Various Attacks on Watermarked Images", International Journal of Computer Science and Information Technologies, Vol. 3 (2), pp. 3582-3587, 2012.
- [14] Vaishali p, pradyumna bhat, "International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering and Control Engineering", Vol. 3, Special Issue 1, , pp. 65-68, April 2015.
- [15] Sudhanshi Sharma, Umesh Kumar," Review of Transform Domain Techniques for Image Steganography", International Journal of Science and Research (IJSR), Volume 4 Issue 5, pp-194-197, May 2015.
- [16] Pooja Rani, Approva Arora, "A Survey on Comparison between DCT and DWT Techniques of Image Compression", Volume 4 Issue 3, pp.1587-1589, March 2015.
- [17] Rowayda A. Sadek, "SVD Based Image Processing Applications: State of The Art, Contributions and Research Challenges", Vol. 3, No. 7, pp. 26-34, 2012.
- [18] Pratap Chandre Mandal, "A Study of Steganography Techniques Using Discrete Wavelet Transform", Volume 5, No. 5, May 2014, pp.7-14.
- [19] Gandharba Swain, Saroj Kumar Lenka, "Classification of Image Steganography Techniques in Spatial Domain: A Study", International Journal of Computer Science & Engineering Technology (IJCSET), Vol. 5 No., pp. 219-23203 Mar 2014.
- [20] Amritpal Singh, Satinder Jeet Singh, "An Overview of Image Steganography Techniques", Volume 3 Issue, pp. 7341-7345, 7 July, 2014.
- [21] Omkar Shetye, Chinmay Vanmali, Moses Fernandes, Prachi Patil. "Survey on Different Techniques of Image Steganography", Volume 138 – No.3, pp. 36-38 March 2016.
- [22] Ronak Doshi, Partik Jain, Lalit Gupta, "Security and Its Applications in Security", International Journal of Modern Engineering Research (IJMER), Vol.2, Issue.6, pp-4634-4638, Nov-Dec. 2012.
- [23] Sudhanshi Sharma, Umesh Kumar, "Review of Transform Domain Techniques for Image Steganography", International Journal of Science and Research (IJSR), Volume 4 Issue 5, pp. 194-197, May 2015.
- [24] Amy Tun, Yadana Thein, "Digital Image Watermarking Scheme Based on LWT and DCT", International Journal of Engineering and Technology, Vol. 5, No. 2, pp. 272-277, April 2013.