FOREX Publication
Open Access | Rapid and quality publishing

International Journal of
Electrical and Electronics Research (IJEER)
Research Article | Volume 10, Issue 2 | Pages 122-125 | e-ISSN: 2347-470X

# Image Steganography Technique based on Singular Value Decomposition and Discrete Wavelet Transform

**Juhi Singh[1] and Mukesh Singla[2]**

*[1]Reserach Scholar, Department of Computer Science and engineering, Baba MastNath University, Rohtak Haryana, India, juhisingh17@gmail.com*
*[2]Professor, Department of Computer Science and engineering, Baba MastNath University, Rohtak Haryana, India, mukesh17singla@yahoo.co.in*

***Corresponding Author:** Juhi Singh; Email: juhisingh17@gmail.com;

**ABSTRACT-** Steganography is a technique of hiding information in digital media. In recent years plenty of work has been done in this domain, and the work can be compared on various parameters such as high robustness and large capacity to achieve a goal. This paper proposed the method of steganography in digital media using Singular Value Decomposition (SVD) and Discrete Wavelet Transform (DWT). The DWT is a frequency-domain technique comprising DWT which comparatively offers better robustness and high PSNR value of stego image over other techniques. The proposed method works well for information hiding against AWGN (additive white Gaussian noise) attack and fulfills the objective to achieve high robustness and high PSNR.

**Keywords:** Data Hiding, Steganography, SVD, DWT, PSNR.

ARTICLE INFORMATION

**Author(s)**: Juhi Singh, Mukesh Singla

**Special Issue Editor**: Dr. Vikash Yadav
**Received**: 25/03/2022; **Accepted**: 27/04/2022; **Published**: 22/05/2022;
**e-ISSN**: 2347-470X;
**Paper Id**: 0422SI-IJEER-2022-04;
**Citation:** 10.37391/IJEER.100212
**Webpage-link**:
https://ijeer.forexjournal.co.in/archive/volume-10/ijeer-100212

crossref member
CROSSREF.ORG
THE CITATION LINKING BACKBONE

This article belongs to the Special Issue on **Recent Developments in Communication Technology using Machine Learning Techniques**.

Publisher's Note: FOREX Publication stays neutral with regard to Jurisdictional claims in Published maps and institutional affiliations.

## 1. INTRODUCTION

Steganography stands for secret writing in any medium most popularly digital images. This paper utilizes DWT and SVD for data hiding. With the application of SVD, any image can be decomposed into three matrices and the same image can be regenerated with the three matrices. If any of the three matrixes is not available in that case regeneration of the original image is not possible [1, 2].use of SVD in this technique is to represent message image in term SVD matrix. The size of SVD matrices is very less so instead of sending a direct message-image, SVD coefficients are sent to the receiver side. The small size of the SVD coefficient makes the hiding process simple and improves the PSNR [3].

## 2. MATHEMATICAL BACKGROUND

Proposed technique is using two mathematical tools singular value decomposition (SVD) and discrete wavelet transform (DWT).

### 2.1 Singular Value Decomposition (SVD)

SVD transform has many properties like singularity and orthogonality. The SVD of any rectangular matrix produces three unitary matrices U, V and S. U and V are having singular values whereas S singular values are diagonal [4].

$$A_{n\times p}=U_{n\times n}\, S_{n\times p}\, V^T_{p\times p}$$

For example, a 3×3 matrix and its SVD decomposition are given below. It is visible that matrix A, U, V contains 9 elements but matrix S can be represented by principle diagonal elements because non-diagonal elements are zero.

$$\begin{vmatrix} 1 & 2 & 3 \\ -2 & -3 & 4 \\ 9 & 6 & -1 \end{vmatrix} = \begin{vmatrix} -0.1266 & 0.6722 & 0.7295 \\ 0.3452 & 0.7193 & -0.6029 \\ -0.9300 & 0.1755 & -0.3231 \end{vmatrix} \begin{vmatrix} 11.6318 & 0 & 0 \\ 0 & 4.7937 & 0 \\ 0 & 0 & 1.6499 \end{vmatrix} \begin{vmatrix} -0.7898 & 0.1696 & 0.1696 \\ -0.5905 & 0.0499 & 0.8055 \\ 0.1660 & 0.9843 & 0.0607 \end{vmatrix}$$

So, instead of sending a complete message image proposed technique sending only the S matrix and complete message image could reconstruct using USV matrices. The image's distinctive information is represented by the singular value of the singular-value matrix. After matrix transformation, the diagonal members of the singular-value matrix are sorted from large to small, with the first diagonal element having a larger value than the others. Furthermore, when the image is somewhat disrupted, the diagonal elements of the singular-value matrix acquired from singular-value decomposition do not vary appreciably, indicating that the singular-value decomposition of the matrix is rotation invariant. In this regard, adding the secret image after the image's singular-value decomposition can boost the algorithm's anti-attack performance.

### 2.2 Discrete Wavelet Transform (DWT)

DWT is a very popular mathematical tool in the field of signal analysis, processing, data hiding, filtering, and compression. DWT is a lossless tool and the mother wavelet is an orthogonal set of basis functions which is either scaled or dilated versions of it. To decompose any image in low (LL) and high (HH) components DWT proved to be an important tool. The Low-frequency component contains more information and the high component contains less information. So, any change in a cover image due to data hiding in the HH component causes less distortion in the cover image. HH component of DWT matrix will hold the secret data [5]. DWT has several advantages, including the ability to withstand multiple attacks while maintaining the image's original quality and ensuring the integrity of secret information collected.

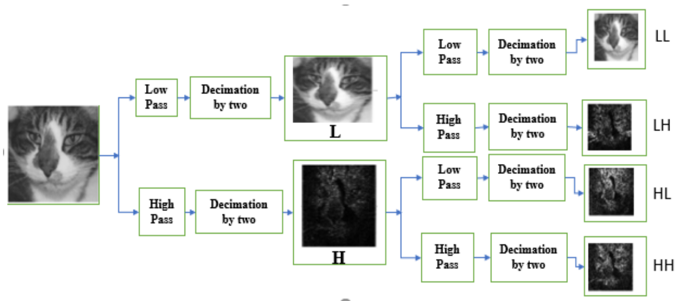


**Figure 1.** DFT Algorithm

## 3. LITERATURE REVIEW

Lots of research has been carried out in the field of Image Steganography. It's an emerging field of information hiding behind any digital media. This paper considers most of the research work based on SVD and DWT techniques. Some of the most popular papers are included here.

Ali Ahmed proposed a method based on LSB and Double XOR Operations. A technique that comprises LSB techniques is most simple and requires less time in execution. These techniques suffer in presence of noise, so frequency domain techniques are more suitable. Maximum PSNR achieved 55.67dB [6].

Franklin Tchakounte proposed the data hiding technique based on DCT and SVD. The first hiding step calculated the DC of the cover image by converting it into 8×8 non-overlapping blocks. On these non-overlapping matrixes SVD is applied which gives three matrices U, S, and V. Now secret data embedding is done in S matrix, and the same process is applied in reverse order to calculate the stego image. Result based on various parameters outperforms similar hiding procedures [7].

Yambem Jina Chanu1 proposed method used SVD for data hiding which first converts cover-image into non-overlapping 4×4 matrices. In this paper, SVD is applied on each non-overlapping matrices and secret binary data embedded in S matrix. Which yields a modified S matrix to generate a stego-image from inverse SVD? Experimental results show that procedure works very well in case of various attacks like compression, Gaussian noise [8].

Sandy et al. proposed a method for protecting human related information like thumb impressions. Fingerprint and secret images passed through SVD and DWT respectively. After selecting HH matrix again SVD was applied to it and SV's of the HH band with SVs of the secret image. Maximum PSNR and SSIM achieved in this method ranging in 54.38 dB and 0.9995 [9].

K Suresh Babu proposed a method based on JPEG compression and SVD decomposition. The first payload is compressed to a certain level to reduce the size of the payload. Cover image decomposed in SVs. Payload is made hidden in SV coefficients. Any change in the SV coefficient causes less effect on the cover image which increases PANR and high capacity [10].

Singh et al. proposed an integrated method to enhance a perceptual quality by using SVD and IWT into two parts, first is embedding and then recovery. The cover image is decomposed by IWT and embedding is being done on SVD matrix into into Low frequency component (LL) component. The proposed method achieves high robustness against the geometric attack and image processing attack [14].
Lakshmi Sirisa proposed a secure data hiding techniques into digital images with an aims to achieve high robustness by using decomposition DWT and SVD methods algorithm to achieve. DWT is used to decompose the cover image and secret data into four sub-bands that is LL, HL, LH and, HH then SVD decomposition is being used on secret data to generate S, U and V sub-bands. After embedding the proposed method produce three stego-images as in result of high PSNR [15].

In this paper, further sections contain the proposed method and experimental results.

Waterfall Boat Leena

**Figure 2.** Message Image considered for Hiding Algorithm

## 4. PROPOSED ALGORITHM AND METHODS

The hiding process takes the message image and cover image as input and produces a stego image. If message image size is small, it generates less imperceptibility effect on the cover image that leads to better PSNR and high robustness.

### 4.1 Data Embedding Algorithm

The embedding steps are summarized in the following points and shown in a block diagram

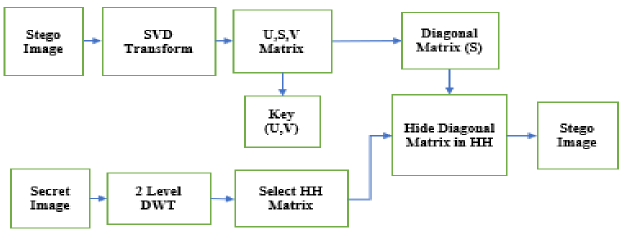


**Figure 3.** Steps of Data Hiding Algorithm

*Step 1*- Select a message and cover image
*Step 2*- Calculate SVD of message image and 2D DWT of cover image respectively
*Step 3*- SVD gives USV matrices and DWT gives LL, LH, HL, HH matrices
*Step 4*- Hide S Matrix in HH Matrix
*Step 5*- Send U, V matrices at the receiver end which is key in this technique
*Step 6*- Send Stego image through a channel to the receiver side

### 4.2 Data Extracting Algorithm
To retrieve the secret data the extracting steps summarized in the following points are shown in block diagram.

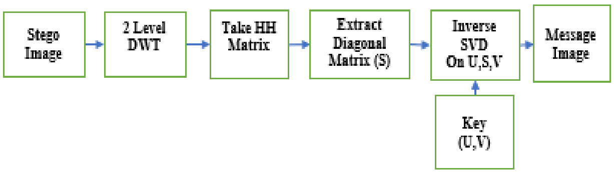


**Figure 4.** Data Extraction Algorithm

*Step 1*- Calculate DWT of stego image which decompose it in sub bands (LL, LH, HL, HH)
*Step 2*- Select HH matrix and extract S matrix from it
*Step 3*- Select U, V from key
*Step 4*- Make complete set of U, S, V matrices
*Step 5*- Take inverse SVD on USV matrices which gives a message image

Bluesea Moon Nature

**Figure 5.** Stego Images

## 5. SIMULATION RESULT
Proposed technique applied on various message images and cover images. The result has been tabulated in table 1 as improved performance of parameters based on the selected images. [11] The average value of PSNR of cover images and message images is comparatively very good. PSNR compares the two images and it must be higher than 37 dB. From the result table, it shows that there is little difference between the cover image and stego image after data hiding. Similarly negligible difference in original massage image and extracted image [13].

$$\text{PSNR (ImageX, ImageY)} = 10\log\left(\frac{x^2{}_{Max}}{MSE}\right)$$

$$\text{MSE} = \frac{1}{MN}\sum\sum(ImageX - ImageY)^2$$

**Table 1: Calculated result analysis of PSNR of Message image and stego image**

| Message Image | Stego Image | PSNR of Stego Image | PSNR of Message Image |
|---|---|---|---|
| **Leena** | Bluesea | 162.0305 | 797.4762 |
| | Moon | 162.0290 | 797.2742 |
| | Nature | 166.7277 | 797.2928 |
| **Boat** | Bluesea | 162.9855 | 798.9390 |
| | Moon | 162.9839 | 798.9340 |
| | Nature | 167.6828 | 798.9139 |
| **Waterfall** | Bluesea | 172.7999 | 811.9112 |
| | Moon | 172.7978 | 811.9173 |
| | Nature | 177.4949 | 811.8232 |
| **Average of proposed methodology** | | **167.5035** | **802.7202** |

## 6. SVD AND DWT AGAINST WHITE GAUSSIAN NOISE ATTACK ROBUSTNESS
In practical scenario any technique must subjected with noise while transmitting stego image from one place to other place. Under any circumstance hidden message not be effected by. So the robustness of any technique must be inquired after adding any unwanted signal. The proposed technique calculated the robustness in presence of AWGN with zero mean and finite variance. From the experiment it can be deduced that if variance of noise is less than 0.000001 the hidden message can be extracted without visible distortion. So the effect of noise attack on stego image is very less.

**Figure 6.** Message Image (Boat and Leena) recovered after AWGN with varying variance at 0.0000001, 0.000001, 0.0001 respectively

## 7. CONCLUSION
This paper discussed the hybrid Steganographic approach in digital images which leads to high PSNR and robustness as shown in *table 1*. To hide the data in digital images DWT and SVD techniques have been used in this paper. SVD helps to isolate the least piece of information without compromising the image quality. This paper has been achieved the aim to produce high PSNR and robustness against AWGN attack has

been studied. The method is working very well. So, the assumption made at the start of this technique proves to be correct in terms of experimental results. For robustness, the experiments ad been performed on message images Leena and Boat and the result shows very less noise. Further, this technique can be considered to provide a shield against various attacks. The proposed method is further used in many domains where secure communication of data is necessity such as biomedical application, secure communication, and military because of high PSNR and robustness.

## 5. ACKNOWLEDGMENT

This research is part of PhD work in the field of image steganography without any funding support/grant.

## REFERENCES

[1] Harsh Vikram Singh, "Steganography in images using LSB technique" International Journal of Latest Trends in Engineering and Technology (IJLTET), volume 5, issue 1, pp 426-430.

[2] H. Vikram Singh and J. Singh, "Highly Impertible Spatial Domain Steganography in Double Precision Images," 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT), 2018, pp. 768-771, doi: 10.1109/ICICCT.2018.8473067.

[3] Mandy Douglas, "Using SVD and DWT Based Steganography to Enhance the Security of Watermarked Fingerprint Images" TELKOMNIKA, Vol.15, No.3, September 2017, pp. 1368~ 1379 ISSN: 1693-6930, accredited A by DIKTI, Decree No: 58/DIKTI/Kep/2013 DOI: 10.12928/TELKOMNIKA.v15i3.6437

[4] Yambem Jina Chanu, "A Robust Steganographic Method based on Singular Value Decomposition", International Journal of Information & Computation Technology. ISSN 0974-2239 Volume 4, Number 7 (2014), pp. 717-726

[5] Vikram S.H. (2019) "DCT- and DWT-Based Intellectual Property Right Protection in Digital Images" First International Conference on Artificial Intelligence and Cognitive Computing. Advances in Intelligent Systems and Computing, vol 815. Springer, Singapore. https://doi.org/10.1007/978-981-13-1580-0_49.

[6] Ali Ahmed, "A Secure Image Steganography using LSB and Double XOR Operations", IJCSNS International Journal of Computer Science and Network Security, VOL.20, No.5, May 2020.

[7] Franklin Tchakounte, "An Efficient DCT-SVD Steganographic Approach Applied to JPEG Images", EAI Endorsed Transactions on Industrial Networks and Intelligent Systems 05 2020 - 10 2020 | Volume 7 | Issue 24 | e2.

[8] Yambem Jina Chanu1, "A Robust Steganographic Method based on Singular Value", International Journal of Information & Computation Technology, Volume 4, Number 7 (2014), pp. 717-726.

[9] Mandy Douglas "Using SVD and DWT Based Steganography to Enhance the Security of Watermarked Fingerprint Images", TELKOMNIKA, Vol.15, No.3, September 2017, pp. 1368~ 1379.

[10] K Suresh Babu, "Robust and High-Capacity Image Steganography using SVD" IET-UK International Conference on Information and Communication Technology in Electrical Sciences (ICTES 2007), Dr. M.G.R. University, Chennai, Tamil Nadu, India. Dec. 20-22, 2007. pp. 718-723.

[11] A. Singh, M.K. Dutta, "A robust zero-watermarking scheme for tele-phthalmological applications" Journal of King Saud University – Computer and Information Sciences 32 (2020) 895–908.

[12] H. I. Shahadi, A. T. Thahab and H. R. Farhan, A novel robust approach for image copyright protection based on concentric rectangles, Journal of King Saud University – Computer and Information Sciences, https://doi.org/10.1016/j.jksuci.2020.06.006

[13] Pan, P.; Wu, Z.; Yang, C.; Zhao, B. Double-Matrix Decomposition Image Steganography Scheme Based on Wavelet Transform with Multi-Region Coverage. Entropy 2022, 24, 246. https://doi.org/ 10.3390/e24020246

[14] Singh, Siddharth, Rajiv Singh, and Tanveer J. Siddiqui. "Singular value decomposition based image steganography using integer wavelet transform." Advances in signal processing and intelligent recognition systems. Springer, Cham, 2016. 593-601.

[15] Lakshmi Sirisha, B. "Image steganography based on SVD and DWT techniques." Journal of Discrete Mathematical Sciences and Cryptography 23.3 (2020): 779-786.

[16] Compton, A. E., and Stacey L. Ernstberger. "Singular Value Decomposition: Applications to Image Processing." Journal of Undergraduate Research 17 (2020): 99-105.