IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-3, March 2019 E-ISSN: 2347-2693

Image Steganography Using Integer Wavelet Transform and Singular Value Decomposition

Shaik Shabina[1*], Ravipati Iswarya Lakshmi[2], Shaik Arshia[3], Vemuri Harshitha[4] ,Rayachoti Eswariah[5]

[1,2,3,4,5]Dept. of CSE, Vasireddy Venkatadri Institute of Technology, Guntur, Andhra Pradesh, India

[*]*Corresponding Author: shabinashaik21@gmail.com, Tel.:9133816846*

DOI: https://doi.org/10.26438/ijcse/v7i3.967971 | Available online at: www.ijcseonline.org

Accepted: 11/Mar/2019, Published: 31/Mar/2019

***Abstract*—**In this paper; we propose an image steganography method using singular value decomposition (SVD) and integer wavelet transform (IWT). The secret message which is in the form of watermark is embedded into the cover image by transforming the cover image using IWT and SVD. The proposed method provides more robustness against image processing and geometric attacks such as JPEG compression, low pass filtering and addition of noise, scaling, rotation and histogram equalization.

***Keywords*—**Integer Wavelet Transform (IWT); Singular Value Decomposition (SVD); PSNR(Peak Signal to Noise Ratio); Structural Similarity Index For Measuring Image quality (SSIM); Normalized Correlation(NC).

I. INTRODUCTION

Recent advancement in the field of multimedia technology,sharing,copying and distribution of digital data through internet,posed several challenges on data security.Digital steganography [1-4] is the possible way to handle these challenges and provides a secure way of data communication. This solution involves hiding secret information called copyright mark in a cover file so that existence of the secret message is not detectable.The hidden information is later extracted and used to ensure rightful ownership and authentication of the digital content.The cover file can be image, or video but the most commonly used are image files because i)digital images are being used quite frequently on the internet ii)the size of image is large and iii)digital images usually contain redundant bits.So we can hide secret data easily in a digital image without being suspected by human visual system.The commonly used image file formats which are used for steganography are graphic interchange format (gif),joint photographic expert group(jpeg)andbitmapformat(bmp)[8].Steganography[5,6,15, 16]has got a wide range of applications in digital media,which has been a source of motivation for this work.The key issue in the design of image steganography scheme are robustness, imperceptibility and security.Robustness refers to the capability of hidden data to survive both intentional manipulation,which aim to destroy the hidden information and unintentional manipulation which do not aim to remove the hidden data.The data hidden in host file has to be undetectable.This requires that embedding has to be done in a manner so that no visible distortion occurs in the stego image.Otherwise, one can guess that the host image has been modified. In order to achieve these goals of Steganography, several approaches have been proposed in both spatial and transform domain. The spatial domain techniques are computationally simple and less robust against intentional or unintentional attacks [7], whereas transform domain techniques require more computations but are more robust against common image processing attacks such as JPEG compression; low pass filtering, addition of noise etc. In this paper we limit our scope to transform domain and propose integer wavelet transform (IWT) based image Steganography method, which combines singular value decomposition (SVD). IWT provides faster computation of wavelet coefficients whereas SVD enables to have better perceptual quality of stego images with greater robustness against common image processing attacks. Thus, by combining SVD and IWT, we have improved performance of image Steganography. To validate the performance of the proposed method, we compare it with discrete cosine transform (DCT) and redundant discrete transform (RDWT) based image Steganography methods using peak signal to noise ratio (PSNR) and correlation coefficient (CC) metrics. Our proposed method consists of a watermark embedding phase and a watermark extraction phase. The main aim of the proposed method is to improve the quality of watermarked image and robustness of the watermark using IWT and SVD.

Integer Wavelet Transform:

IWT, which is an extension of DWT, not only inherits the excellent energy compaction and detail description abilities

of DWT but also has faster calculating speed than DWT. Figure 1 shows an example of 1 level-IWT based on the lifting technique in which an 8×8 image is decomposed to four frequency bands: low frequency, horizontal, vertical and diagonal directions, which are denoted as CA, CV, CH, and CD. In our study, the CA of IWT is utilized for image watermark embedding for the following reasons:

1) IWT has remarkable abilities for spatial localization, frequency spread, and multi-resolution, which can ensure both the watermarking robustness and invisibility.
2) The CA component of IWT aggregates the main energies of images and thus is invariant towards various compression and filtering attacks, which can further enhance the watermarking robustness.
3) The IWT on images is a mapping procedure from integer to integer and thus avoids fractional computations, which can save computational costs. .

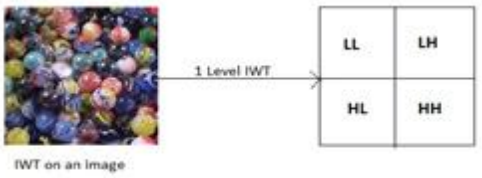

Fig1: Division of sub-bands using IWT

Singular Value Decomposition:
Singular Value Decomposition (SVD) is a matrix factorization technique in which a rectangular matrix is decomposed into three matrices. Its mathematical representation is given as follows:

$$M = USV^T$$

• Where M is a m × n matrix with real or complex entries.
• U is an m× m unitary matrix with real or complex entries.
• S is a diagonal m × n matrix with non-negative real numbers on the diagonal.
• V is an n × n unitary matrix with real or complex entries.

Inspired by Priyanka et al.'s scheme [9], in our study, we modify the value of entries in the left singular vector matrix U to embed a watermark. In this manner, we not only utilize the notable stability and robustness of SVD against common signal processing, such as filtering, noise addition, and geometrical attacks, such as cropping, rotation, etc. but also overcome the false positive problem as analysed in [9]. In Figure 2 we can observe the process of Singular Value Decomposition.

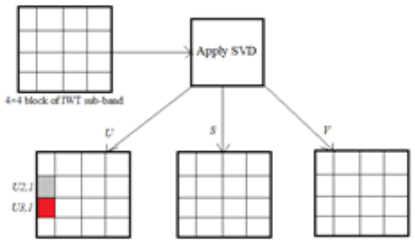

Fig2: Process of SVD

II. RELATED WORK

G. Prashanti and K. Sandhyarani[10] in 2015 have done survey on recent achievements of LSB based image steganography. In this survey authors discuss the improvements that enhance the steganographic results such as high robustness, high embedding capacity and un-detectability of hidden information. Along with this survey two new techniques are also proposed. First technique is used to embed data or secret messages into the cover image and in the second technique; a secret gray scale image is embedded into another gray scale image. These techniques use four state table that produce pseudo random numbers. This is used for embedding the secret information. These two methods have greater security because secret information is hidden on random selected locations of LSBs of the image with the help of pseudo random numbers generated by the table. It is relatively simple to detect the hidden data. It does not offer robustness against small modifications (including compression) at the stego images.

G. Prashanti and K. Sandhyarani [19] have done survey on recent achievements ofLSB based image steganography. In this survey authors discuss the improvements thatenhance the steganographic results such as high robustness, high embedding capacity andun-detectability of hidden information. Along with this survey two new techniques are alsoproposed. First technique is used to embed data or secret messages into the cover imageand in the second technique a secret gray scale image is embedded into another gray scale
image. These techniques use four state table that produce pseudo random numbers. This isused for embedding the secret information. These two methods have greater securitybecause secret information is hidden on random selected locations of LSBs of the imagewith the help of pseudo random numbers generated by the table. 2014-2015: SavitaGoel et al. in [20] proposed a new method ofD. Debnath et al. [11] proposed a security scheme in which steganography is used along with cryptography to provide better security to embedded data. In their method first data is encrypted then it is embedded into cover image using steganographic method. Proposed algorithm transforms any kind of message into text with the help of manipulation tables, and then carries out hill cipher

methods to it and finally hides the data into red, blue, and green pixels of the cover image. They use number of image quality parameters like MSE, PSNR, AD, SC, NAE and MD. The hill cipher can be difficult to break with a cipher text only attack but it succumbs to a known plain text attack.

Della Baby et al. [12] proposed a "Novel DWT based Image Securing method using Steganography". In their work new steganography technique is prosed in which multiple RGB images are embedded into single RGB image using DWT steganographic technique. The cover image is divided into 3 colors i.e. Red, Green and Blue color space. These three color spaces are utilized to hide secret information. Experimental results obtained using this system has good robustness. Value of PSNR and SSIM index have been used by authors to compare the quality of stego image and original cover image. Proposed method has good level of PSNR and SSIM index values. Authors have found that their experimental results are better than existing approaches and have increased embedding capacity because of datacompression. So overall security of their approach is high with less perceptible changes in stego image.

H. Yang et al. [13] presented a new adaptive LSB based method for image steganography. It uses the pixel adjustment technique for better stego image quality. This adaptive LSB substitution results in high hidden capacity. In [14] LSB based image steganography method is proposed. To hide the data common bit pattern is used. According to the message and the pattern bits LSB's of pixels are modified. This method has low hidden capacity.

III. METHODOLOGY

The proposed method of IWT and SVD based steganography mainly contains two steps. The first step is embedding a secret message into an image and the second step is extraction of that secret message from the image. For embedding we follow the algorithm1 and for extraction we follow the algorithm2.

a) Watermark Embedding Algorithm:

Watermark embedding procedure is explained as follows and it is shown in fig

Step 1: Consider any color image as cover image denote it by 'I'. Get R, G, B channels of cover image 'I'.

Step 2: Consider the blue component of the cover image 'I', and divide it into blocks of size 20 × 20. When compared to red and green channels blue channel is more resistant to changes.

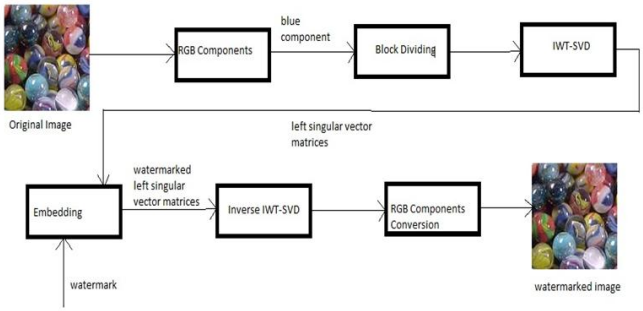

Fig3: Embedding procedure of IWT-SVD based watermarking

Step 3: Apply IWT to each block in the blue channel 'B' to get the multi-resolution sub-bands LL, HL, LH, and HH.
Step 4: Apply SVD on LH and HL sub-band of each blocks of B channel to obtain USV^T
Step 5: Apply Algorithm1.
Step 6: Apply Inverse SVD.
Step 7: Apply Inverse IWT.
Step 8: Combine R, G, B channels to get watermarked image 'WI'.

It helps to improve the copyright protection of the cover image and robustness of the watermark in the watermarked image.

Algorithm1:
Input: $U_{2,1}$ and $U_{3,1}$
Output: Watermarked $U_{2,1}$ and $U_{3,1}$
1: $U_{avg} = (|U_{2,1}| + |U_{3,1}|)/2$
2: if w=1 then
3: if $|U_{3,1}| - |U_{2,1}| < T$
4: $U_{2,1} = \text{sign}(U_{2,1}) \times (U_{avg} - T/2)$
5: $U_{3,1} = \text{sign}(U_{3,1}) \times (U_{avg} + T/2)$
6: else
7: No change
8: end if
9: else if w=0 then
10: if $|U_{2,1}| - |U_{3,1}| < T$
11: $U_{2,1} = \text{sign}(U_{2,1}) \times (U_{avg} + T/2)$
12: $U_{3,1} = \text{sign}(U_{3,1}) \times (U_{avg} - T/2)$
13: else
14: No change
15: end if
16: end if

b) Watermark Extraction Algorithm

Extraction of watermark image from watermarked image is explained as follows and it is shown in fig4.

Step 1: Get R, G, B channels of watermarked image 'WI'.
Step 2: Consider the blue component of the cover image 'I', and divide it into blocks of size 20 × 20.

Step 3: Apply IWT to each block in the blue channel 'B' to get the multi-resolution sub-bands LL, HL, LH, and HH.

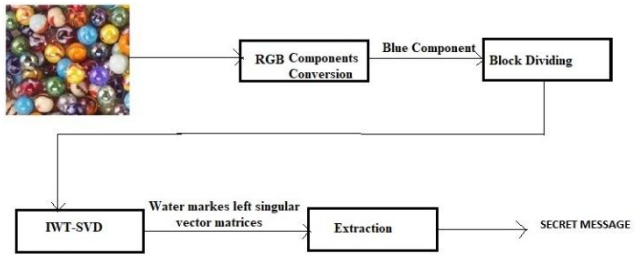

Fig4: Extraction procedure of IWT-SVD based watermarking

Step 4: Apply SVD on LH and HL sub-band of each blocks of B channel to obtain USV^T.
Step 5: Apply Algorithm2.
Step 6: Apply Inverse SVD.
Step 7: To get the watermark apply inverse IWT.

Algorithm2:

Input: x, y
Output: data
1. Function [ew] = extract(x, y)
2. if x>y
3. then ew=1;
4. else if x<=y
5. then ew=0;
6. end
7. end

IV. RESULTS

As per this proposed method, a color image of size 100×100 is considered as cover image as shown in Fig. 5.

Fig5: Original image

After applying the proposed method the resultant watermarked image is shown as Fig.6.

Fig6: Watermarked Image

Table 1 summarizes PSNR value of watermarked image and SSIM,NC values of extracted watermark image when the watermarked image is not attacked and undergoes any attack like Gaussian noise, salt & pepper noise, Poisson noise, Gaussian blur.

Table1: PSNR,SSIM&NC values

Attack / Operation	PSNR	SSIM	NC
No attack	85.76	1.000	0.994
Gaussian noise	65.46	0.996	0.997
Salt & Pepper noise	65.45	0.998	1.000
Poisson noise	85.76	1.000	0.993
Gaussian blur	79.18	0.997	0.998

This experiment is conducted on 50 images. Out of 50 images, some images along with their watermarked images and recovered images are displayed in table2.

Table2: output analysis

Figure name	A)original image	B)watermarked image	C)recovered image
Tom & Jerry			
Flowers			
Snowfall			
Waterfalls			
House			

Table3: PSNR, SSIM&NC values of Flowers

Image Name	Attack / Operation	PSNR	SSIM	NC
Flowers	No attack	85.76	1.000	0.994
	Gaussian noise	65.46	0.996	0.997
	Salt & Pepper noise	65.45	0.998	1.000
	Poisson noise	85.76	1.000	0.993
	Gaussian blur	79.18	0.997	0.998

Table4: PSNR, SSIM&NC values of Waterfalls				
Image Name	**Attack / Operation**	**PSNR**	**SSIM**	**NC**
Waterfalls	No attack	85.76	1.000	0.994
	Gaussian noise	65.46	0.996	0.997
	Salt & Pepper noise	68.45	0.978	1.000
	Poisson noise	85.76	1.000	0.993
	Gaussian blur	79.18	0.967	0.899

Table5: PSNR, SSIM&NC values of Snowfall				
Image Name	**Attack / Operation**	**PSNR**	**SSIM**	**NC**
Snowfall	No attack	85.76	1.000	0.995
	Gaussian noise	67.46	0.996	0.997
	Salt & Pepper noise	65.45	0.968	1.000
	Poisson noise	88.76	1.000	0.993
	Gaussian blur	79.18	0.967	0.997

Table6: PSNR,SSIM&NC values of Tom& Jerry				
Image Name	**Attack / Operation**	**PSNR**	**SSIM**	**NC**
Tom&Jerry	No attack	87.76	0.987	0.974
	Gaussian noise	68.46	0.999	0.995
	Salt & Pepper noise	63.45	0.997	1.000
	Poisson noise	87.76	1.000	0.994
	Gaussian blur	89.18	0.993	0.997

Table7: PSNR, SSIM&NC values of House				
Image Name	**Attack / Operation**	**PSNR**	**SSIM**	**NC**
House	No attack	85.76	1.000	0.944
	Gaussian noise	65.56	0.996	0.957
	Salt & Pepper noise	65.45	0.998	1.000
	Poisson noise	85.76	1.000	0.993
	Gaussian blur	79.48	0.987	0.938

V. CONCLUSION AND FUTURE SCOPE

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

REFERENCES

[1] Fridrich, J.:"Steganography in digital media: Principles, algorithms, and applications". Cambridge University Press (2010).

[2] Atawneh, S., Almomani, A., Sumari, P.: Steganography in digital images: common approaches and tools. IETE Technical Review 30(4), 344-358(2013).

[3] Cheddad, A., Condell, J., Curran, K., Kevitt, M.P. Digital image Steganography: survey and analysis of current methods. Signal Processing 90(3), 727-752(2010).

[4]Cox, J., Miller, M.L., Bloom, J.A., Fridrich, J., Kalker, T. "Digital Watermarking and Steganography". Elsevier (2008).

[5] Katzenbeisser, S., Petitcolas, F.A.P.: "Information hiding techniques for Steganography and digital watermarking". Artech House Inc., Norwood(2000).

[6]Johnson, N.F., Jajodia, S. "Exploring Steganography: seeing the unseen". IEEE Computer 31(2), 26-34(1998).

[7]Westfield, A., Pfitzmann, A." Attacks on steganographic systems". In: Lecture Notes in Computer Science, vol. 1768, pp. 61-75. Springer (2000).

[8] Singh, S., siddiqui, T.J.: "Transform domain techniques for image steganography. Information Security in Diverse Computing Environments", 245-259. IGI global (2014).

[9] Maheshkar S(2017) Region-based hybrid medical image watermarking for secure telemedicine applications. Multimed Tools Appl 76(3):3617-3647.

[10] G.Prashanti, K. Sandhyarani, "A New Approach for Data Hiding with LSB steganography", Emerging ICT For Bridging the Future – proceedings of the 49th Annual Convention of the Computer Society of India CSI, Springer 2015, pp. 423-430.

[11]D.Debnath, S.Deb, N.Kar, "An Advanced Image Encryption Standard Providing Dual Security: Encryption Using Hill Cipher and RGB Image Steganography",IEEE International Conference on Computational Intelligence and Networks (CINE), Jan. 2015, pp.178-183.

[12]D.Baby, J.Thomas, G. Augustie, E. George, N.R. Michael, "A Novel DWT based Image Securing method using Steganography", International Conference on Information and Communication Technologies (ICICT),Procedia Computer Science, April 2015, pp. 612-618.

[13] H.Yang, X. Sun and G. Sun, "A High-Capacity Image Data Hiding Scheme Using Adaptive LSB Substitution" ,Journal of Radio Engineering Vol. 18, No. 4, pp. 509-516,2009

[14] S. Channalli and A. Jadhav, "Steganography an Art of Hiding Data", International Journal on Computer Science and Engineering (IJCSE), 2009 pp. 137-141.

[15] R. Eswaraiah, Sai Alekhya Edara, E. Sreenivasa Reddy , " Color Image Watermarking Scheme using DWT and DCT Coefficients of R, G and B Color Components"International Journal of Computer Applications (0975 – 8887) Volume 50 – No.8, July 2012.

[16]R.Eswaraiah & E.Sreenivasa Reddy,"Robust Watermarking Method for Color Images Using DCT Coefficients of Watermark"Global Journal of Computer Science and Technology Graphics & Vision Volume 12 Issue 12 Version 1.0 Year 2012Online ISSN: 0975-4172 & Print ISSN: 0975-4350.

