International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-3, September 2019

A Highly Secure and Robust Copyright Protection Method for Grayscale Images using DWT-SVD

Poonam Kadian, Nidhi Arora, Shaifali M Arora

Abstract: ***Digital watermarking has emerged as a potential solution to copyright-related issues of digital data. A novel, highly secure robust digital watermarking method using DWT-SVD is presented in this paper. Instead of using the conventional watermark embedding process where the watermark gets embedded over the entire host image, the coefficients for embedding the watermark inside the host image has been identified in this proposed method. Such selection of pixels used for insertion of watermark makes this algorithm highly secure, robust, and imperceptible. The experimental results demonstrate the efficiency of the proposed method in aspects of high robustness and good imperceptibility.***

Keywords*: Digital watermarking, robust watermarking, transform domain, DWT-SVD, copyright protection, information hiding.*

I. INTRODUCTION

The current scenario of rapidly growing technology, the highly competitive environment and the role of internet in our lives have made it very convenient to upload our data on digital platforms. However, the availability of numerous data manipulation tools such as Photoshop Editors and PDF converters has made it very easy to copy digital data and manipulate it. This leads to copyright disputes of digital data. Information hiding techniques are capable of providing efficient solutions to these issues. Whilst someone sends his/her important information over the network it is desired that neither the information gets stolen nor it gets manipulated whether intentionally/ unintentionally. However, such information can easily be accessed and manipulated if it is not secured. To secure the copyright of the owner of such data, some information can be used as hidden information to that data which is known to its owner only. Digital watermarking is one such information hiding method that has emerged as a very effective method to provide copyright protection and copyright authentication to digital data. Fragile watermarking is a discipline of watermarking designed to provide copyright authentication specifically. The main feature of a fragile watermark is that if some manipulation is applied to the watermarked image, the hidden information also known as watermark gets vanished from the watermarked image. However, the other discipline of watermarking known as robust watermarking is exactly contrary to fragile watermarking. In robust watermarking, the watermark is inserted in the host image such that no manipulation can eliminate the watermark from the watermarked image. This feature of robust watermarking makes it suitable for the applications where copyright protection of digital data is required.

The process of watermarking consists of two main units: watermark insertion unit along with a watermark extraction unit [1-2]. Any information such as data, image, text, logo, and even the coefficients of the host image itself can be used as a watermark. During the watermark insertion process, information used as the watermark is embedded over the host image. The amount of embedding is decided by a unit known as the scaling factor. Higher is the value of scaling factor higher is the amount by which the host image gets transformed by watermark and hence resulting in lowering the perceptual quality of the watermarked image. So, to maintain the required quality of watermarked image it is necessary to select a suitable scaling factor for the algorithm. The resultant image of this embedding process is known as watermarked image and this image gets floated over the social networks where the malicious attackers try to modify it using image processing and geometrics tools available [4-7]. The attacked watermarked image then becomes the input to the extractor unit, where the owner can claim his copyright. The applied watermark on the host image in the insertion unit gets extracted from the attacked watermarked image at this stage. Then the retrieved watermark is compared with the original watermark, the amount of similarity decides the claim of the copyright of the owner. This amount of similarity is calculated by evaluating either Structural Similarity Index (SSIM) or Correlation Coefficients metrics of calculations [3, 11].

As compared to the relatively simpler spatial domain techniques, transform domain techniques have found to be more robust [8]. The transformation techniques such as DCT, DFT, and DWT can be applied in transform domain watermarking. Despite the disadvantages like computationally expensive,

Manuscript published on 30 September 2019
* Correspondence Author

Poonam Kadian*, CSE, GD Goenka University, Gurgaon, India. Email: poonamdsk@gmail.com,

Nidhi Arora, CSE, GD Goenka University, Gurgaon, India. Email: nidhi.arora1@gdgoenka.ac.in

Shaifali M. Arora, ECE, Maharaja Surajmal Institute of Technology, New Delhi, India. Email: shaifali04@msit.in

complex implementation, etc., the transform domain methods are used widely as they are capable of providing effective robustness against some common image processing as well as geometric attacks like blurring filtering, The addition of noise, changes in contrast, sharpening, etc [9-12]. The transform domain methods, when hybridized with other transformation methods like SVD, provide even better robustness than when used solely [3].

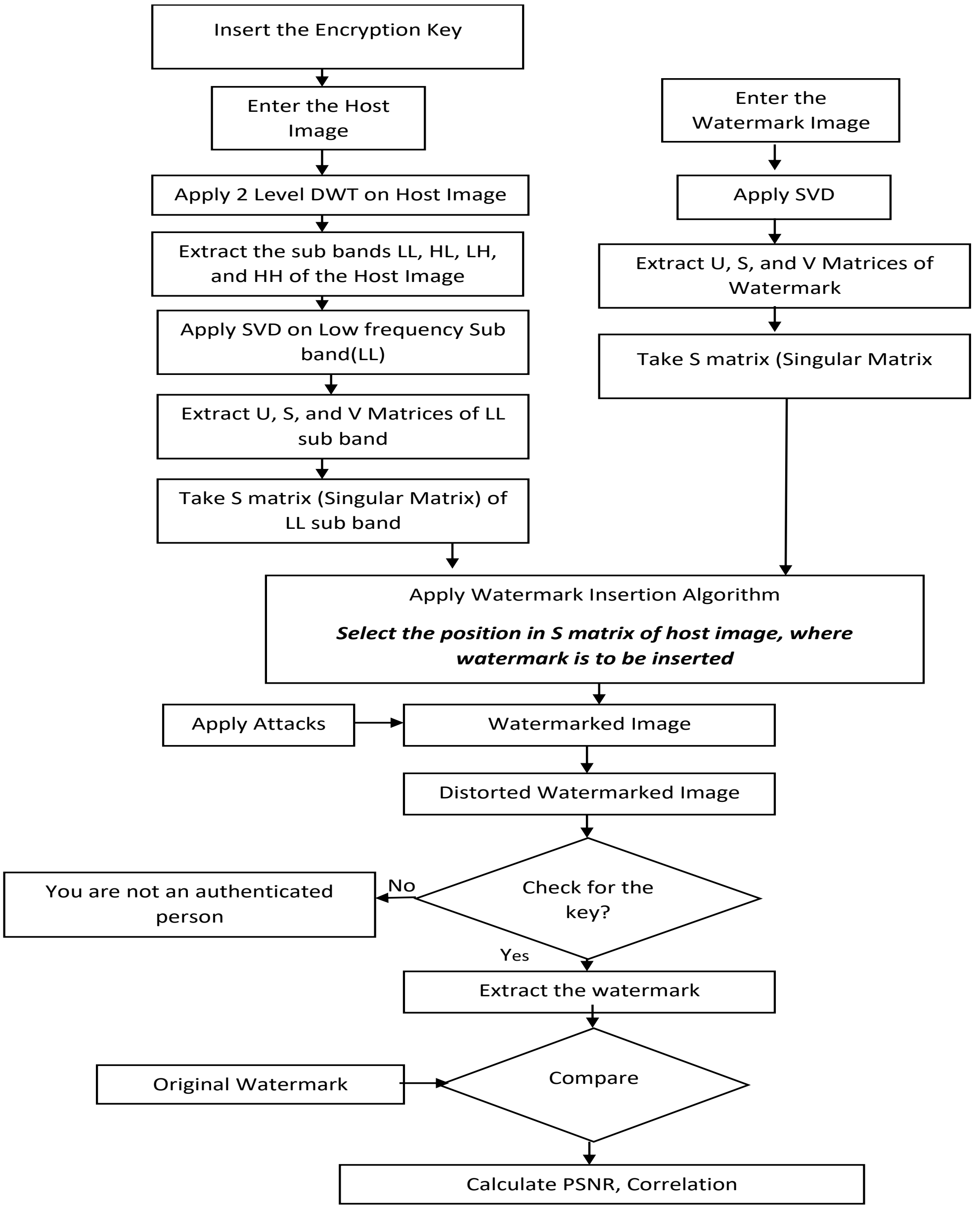

Insert the Encryption Key
Enter the Host Image
Apply 2 Level DWT on Host Image
Extract the sub bands LL, HL, LH, and HH of the Host Image
Apply SVD on Low frequency Sub band(LL)
Extract U, S, and V Matrices of LL sub band
Take S matrix (Singular Matrix) of LL sub band
Enter the Watermark Image
Apply SVD
Extract U, S, and V Matrices of Watermark
Take S matrix (Singular Matrix
Apply Watermark Insertion Algorithm
Select the position in S matrix of host image, where watermark is to be inserted
Apply Attacks
Watermarked Image
Distorted Watermarked Image
You are not an authenticated person
No
Check for the key?
Yes
Extract the watermark
Original Watermark
Compare
Calculate PSNR, Correlation

Fig:1: Flowchart of Watermark Insertion and Extraction Process.

In this work, a robust digital watermarking method based on DWT-SVD has been proposed.

Grayscale images have been used as a host image and as the watermark image. During the insertion process instead of embedding the watermark over the entire host image, the coefficients from the host image have been identified using the SVD method. This will lead to a highly imperceptible and robust watermarking algorithm. The results are compared with the conventional DWT-SVD algorithm where the entire host image has been used for insertion of a watermark. The efficiency of the proposed algorithm has been verified by using watermarking parameters such as SSIM, CC, and PSNR and its resistance to attacks have also been presented. The paper has been organized as the watermark embedding and insertion algorithm has been explained in Section 2, the results and conclusion have been demonstrated in section 3 and 4 respectively.

II. The Watermarking Embedding and Extraction Process

A. *Watermark Embedding*

The Watermark insertion and extraction algorithm have been presented in Fig.1. The steps followed for the watermark insertion process are as follows:

- Step 1: Decide the encryption key for the Watermarking system.

- Step 2: Enter the Host Image.
- Step 3: Apply 2 Level DWT on the host Image.
- Step 4: Apply SVD on LL sub-band extracted from DWT, and thus extract U, S, and V matrices of the low-frequency sub-band of the host image.
- Step 5: Enter the image to be used as a watermark and apply SVD on that image to extract U, S, and V matrices of the watermark image.
- Step 6: Take Singular values of both the images and identify the coefficients in the S matrix of host image where the S values of watermark are inserted.
- Step 7: Construct the watermarked image from the S values obtained from step 6.

B. *Watermark Extraction*

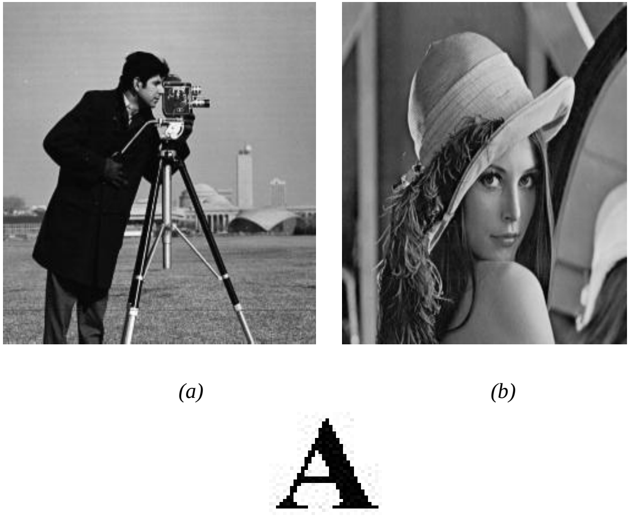
The watermarking extraction process has been carried out as follows:

- Step 1: Check for the key entered if the inserted key is wrong then the person is not authenticated to extract the watermark. However, if the entered key is correct then extract the watermark by following the next steps.
- Step 2: Apply IDWT on the attacked watermarked image.
- Step 3: Apply SVD and reconstruct the extracted watermark image.

Step 4: Calculate PSNR and Correlation to assess the robustness and imperceptibility of the extracted watermark.

III. Experimental Results

Two JPEG images Lena and Cameraman each of size 512X512 has been taken for the analysis of algorithm as depicted in Fig. 2(a-b respectively). An image of size 256X256 has been taken as the watermark image as shown in Fig 2 (c). Attacks like blurring, cropping, Gaussian noise, salt, and pepper noise, resize, sharpening, and rotation has been imposed on the watermarked image.



(a) *(b)*

(c)

Fig. 2 (a-c): Host Images (cameraman, and Lena) and watermark Image.

The extracted watermarks from the attacked watermarked images by both DWT-SVD and the proposed algorithm has been presented in Fig.3. The column 1 and 3 of this figure represents the recovered watermark from the cameraman image by DWT-SVD and the proposed algorithm respectively, whereas column 2 and 3 are showcasing the recovered watermarks from Lena Image.

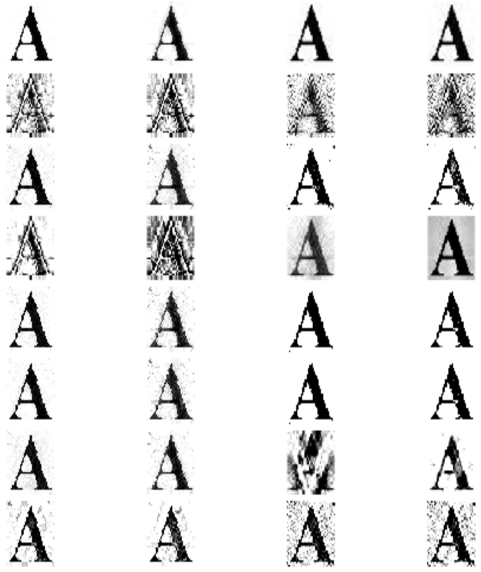


Fig. 3: The Extracted watermarks

The proposed algorithm has been compared with two states of the art methods presented in [3, 13]. To evaluate the robustness and imperceptibility of the algorithm presented in this paper, PSNR and CC have been calculated. The results obtained for PSNR in dB (Decibels) has been presented in Table-I.

Table-I: Evaluated PSNR for Watermarked Images

The result obtained by the approach presented in [3, 13]	**The result obtained by the approach presented in [3, 13]**	**Proposed Method**	**Proposed Method**
Cameraman	**Lena**	**Cameraman**	**Lena**
41.57	45.9	52.78	54.82

As depicted by the values of Table-I, the proposed method has significantly improvised PSNR in comparison to the approach used by [3, 13].

Table-II is showcasing the correlation values achieved by the proposed method. Comparison with the two existing DWT-SVD methods [3, 13] validates that the proposed method can provide a higher correlation. A graphical representation of the correlation comparison has been shown in Fig. 4.

From Table I and II, it is evident that the method proposed in this paper provides significant improvements in terms of PSNR and Correlation.

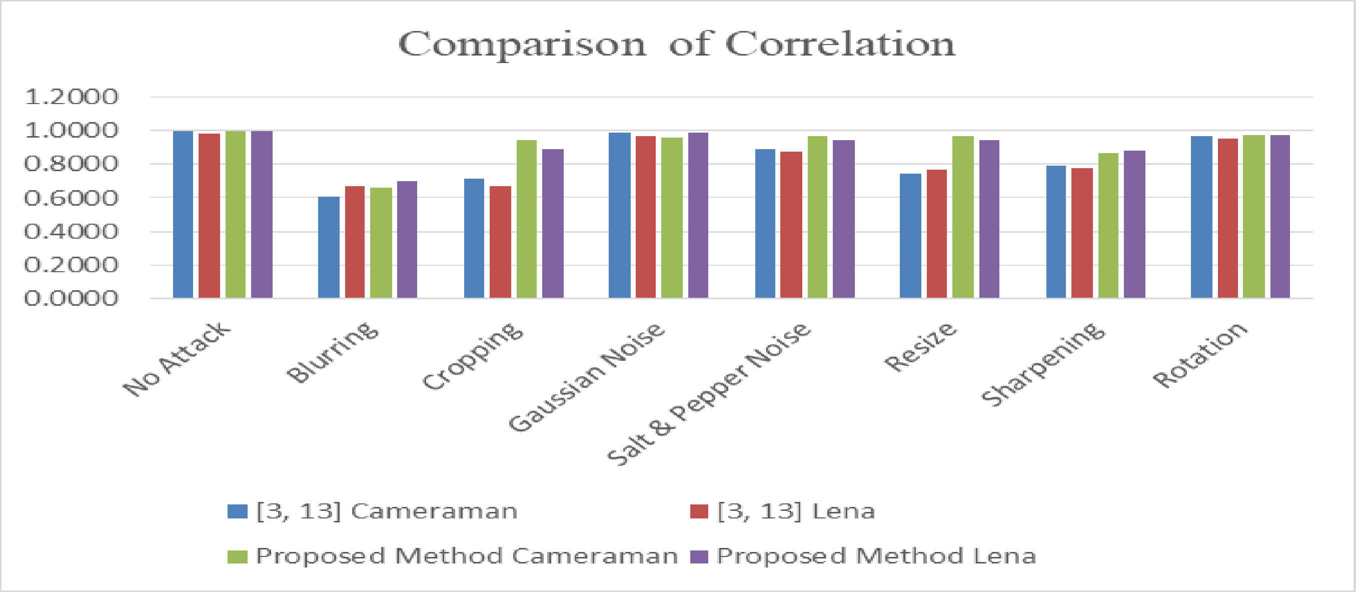


Fig.4: Correlation comparison of Cameraman and Lena image

Table-II: Correlation Comparison of Extracted Watermarks with the Original watermark.

	[3, 13]	**[3, 13]**	**Proposed Method**	**Proposed Method**
Images/Atta-cks	Cameraman	Lena	Cameraman	Lena
No Attack	0.9990	0.9845	0.9999	0.9983
Blurring	0.6108	0.6658	0.6576	0.6970
Cropping	0.7140	0.6672	0.9441	0.8922
Gaussian Noise	0.9929	0.9702	0.9579	0.9921
Salt & Pepper Noise	0.8918	0.8726	0.9640	0.9401
Resize	0.7466	0.7713	0.9640	0.9401
Sharpening	0.7942	0.7741	0.8657	0.8843
Rotation	0.9636	0.9517	0.9737	0.9744

IV. CONCLUSION

A highly secure robust watermarking method has been presented in this paper. In transform domain watermarking, DWT has been used widely in the literature. The hybridization of DWT with SVD has provided improved robustness in comparison to DWT when used solely. In this paper, an encryption key has also been inserted that leads to enhanced security of the resultant watermarking system. The simulation results prove the fact that this algorithm is increasing the robustness (as depicted by the results of PSNR) and imperceptibility. To verify the efficiency of the algorithm, the results have been empirically analyzed with existing DWT-SVD method. The analysis demonstrates the efficacy of this proposed algorithm.

REFERENCES

1. Cox, Ingemar J., Joe Kilian, F. Thomson Leighton, and Talal Shamoon.: "Secure Spread Spectrum Watermarking for Multimedia," *IEEE Transactions on Image Processing, 1997*, 6(12), pp. 1673-1687.
2. Kutter, Martin, and Fabien AP Petitcolas.: "Fair benchmark for image watermarking systems in Security and Watermarking of Multimedia Contents," *International Society for Optics and Photonics, 1999*, 3657, pp. 226-240.
3. Arora, S.M.: "A DWT-SVD based Robust Digital Watermarking for Digital Images," Procedia Computer Science, 2018, 132, pp.1441-1448
4. Roldan LR, Hernández MC, Chao J, Miyatake MN, Meana HP (2016) Watermarking-based color image authentication with detection and recovery capability. IEEE Lat Am Trans 14(2):1050–1057.
5. Roy A, Maiti AK, Ghosh K (2015) A perception based color image adaptive watermarking scheme in YCbCr space. In: 2nd IEEE international conference on signal processing and integrated networks (SPIN).
6. Yadav N, Singh K (2015) Transform domain robust image-adaptive watermarking:prevalent techniques and their evaluation. In: IEEE international conference on computing, communication and automation.
7. Shukla D, Tiwari N, Dubey D (2016) Survey on digital watermarking techniques. Int J Sig Process Image Process Pattern Recogn 9(1):239–244
8. Maity HK, Maity SP (2015) Multiple predictors based RW scheme with adaptive image partitioning. In: IEEE international conference on advances in computing, communications and informatics.
9. PushpaMalaSetal(2015)Digital image watermarking techniques: a review.IntJ Comput Sci Secur 9(3):140–156.
10. Maiorana Eetal(2016) High- capacity watermarking of high dynamic range images.EURASIP J Image Video Process. Springer
11. Kadian, Poonam, Nidhi Arora, and Shaifali M. Arora. "Performance Evaluation of Robust Watermarking Using DWT-SVD and RDWT-SVD." In *2019 6th International Conference on Signal Processing and Integrated Networks (SPIN)*, pp. 987-991. IEEE, 2019.
12. Ambadekar, Sarita P., Jayshree Jain, and Jayshree Khanapuri. "Digital Image Watermarking Through Encryption and DWT for Copyright Protection." In *Recent Trends in Signal and Image Processing*, pp. 187-195. Springer, Singapore, 2019.

13. Vaidya Petal (2015) Adaptive digital watermarking for copyright protection of digital images in wavelet domain. In: 2nd international symposium on computer vision & internet, vol 58. Elsevier, Procedia Computer Science, pp 233–240.

AUTHORS PROFILE

Ms. Poonam Kadian received her B.Tech degree in Electronics and Communication Engineering from Kurukshetra University, India, in 2005 and the M.Tech degree in Digital Communication from Shobhit University in 2011. She is a research scholar at GD Goenka University, Gurgaon, Haryana. She has an experience of more than 9 years and her fields of interests are Image processing, Machine learning, Artificial Intelligence.

Dr. Nidhi R. Arora holds a Ph.D. in the field of Information Retrieval from INHA University South Korea. Her dissertation work focused on designing a ranking algorithm to produce top-k search results for keyword query on data graphs. She is currently working as Associate Professor at GD Goenka University. Her research interests are in the field of Deep Learning, Natural Language Processing, and Machine Learning. She has publications in top conferences and journals such as DEXA, DASFAA, Expert Systems With Applications (ESWA) and New Generation Computing.

Dr. Shaifali Madan Arora is an Associate Professor at MSIT, New Delhi. She has done her B.Tech from GNDU, Amritsar, India, M.Tech from GNDEC, Ludhiana, India and Ph. D. from GGSIPU, New Delhi. She has teaching experience of more than 15 years. She is a life member of ISTE. Her areas of interest include Digital image and signal processing, Artificial intelligence, Microprocessors and controllers, Machine Learning. She has various research publications in quality national and international journals and conferences.