International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 03 | March - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

A Segmentation-Driven Non-Blind DWT Watermarking Framework Ensuring Robustness, Transparency, and Security

Sanjay Patsariya [1], Anand Jha [2], Mahendra Kumar Pandey[3]

[1,2]*Department of Information Technology,RJIT, Gwalior,MP, India*
[3] *Department of Electronics & Communication Engg., RJIT, Gwalior, MP,India*

Abstract - Due to advancement in network technology, digital data is very popular medium for communication but eased to duplication and manipulation. Digital watermarking is the process of embedding digital evidence (also called watermark) into another digital signal (also called cover image) to proof content authenticity and copy right protection. The performance of watermarking technique can be assessed using various parameters like MSE, PSNR, SSIM and NCC. In this paper, Non-blind watermarking technique is proposed in transform domain using scrambling techniques to make this method robust and secure.

Key Words: Watermarking, frequency domain, MSE, PSNR, NCC.

1. INTRODUCTION

Due to the rapid growth in communication technology, Internet is most preferable medium for communication. In watermarking procedure, piece of information is inserted into a digital media i.e. video, audio, text or image. Digital watermarks are used to verify the authenticity, integrity of the digital data or to show the identity of its ownership [1]. Basically information hiding can be done by three methods i.e. Steganography, Cryptography and watermarking. A watermark/ logo are a form of image, audio etc. which can be inserted as digital evidence.

Table-1 : Illustrate purpose of watermarking, Steganography and Cryptography

Process	Method Adopted	Purpose
Watermarking	Insert watermark Image /logo onto cover Image	Copyright protection
Steganography	Use Cover Media to hide data	Message is kept secret
Cryptography	Data is encrypted	Protect content

2. CLASSIFICATION

The classification can be done on the basis of working domain, type of document used and human perception.

2.1 According to transform domain

The watermark embedding process can be done in mainly into two domain i.e. Spatial and Transform domain. The term spatial indicate to space. It is the 2D plane in case of image. Therefore, it refers to the image plane itself and based on directly manipulate the value of pixels [2]. The strength of this domain is easiness but robustness is the main concern, means information hiding in this domain is more vulnerable to attacks. One of the famous algorithms that belong to spatial domain method is LSB watermarking. In this method, the LSB of image pixels is changed or manipulated for the intended purpose. Spatial method is simple but vulnerable to cropping scaling and compression attack.
On other hand, in transform domain methods, the frequency component of digital media is changed. It deals with the rate of pixel change. To work in frequency domain, the host image and watermark is converted to appropriate signal using DCT, DWT, SWT, IWT transformation etc. DCT divide the images into various bands. The secret information embedded over the middle frequency band.
DWT divide image into various sub band i.e. HH, HL, LH, LL components. Fig. 1 illustrate block diagram of watermarking procedure.

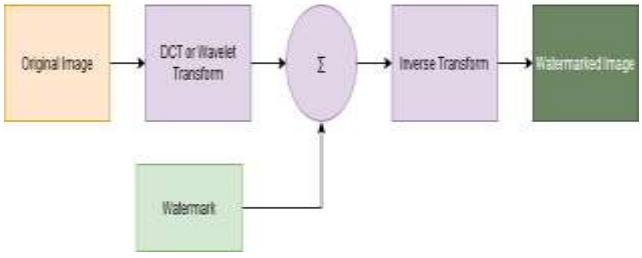

Fig-1: Illustrate watermarking procedure

2.2 According to type of document

On the basis of type of documents, watermarking may be Text, Image and audio.

a.	Text watermarking	It is the process to embed a watermark into text document.
b.	Image watermarking	An image watermark is embedded to create Watermarked image.
c.	Audio watermarking	A secret message in form of audio is inserted or embedded into an audio file[3].

2.3 According to human perception

On the basis of human perception, watermarking may be visible, semi visible and invisible.

a.	Visible watermarking Procedure	The embedded information/watermark is perceptible to human visual system.
b.	Semi- visible watermarking Procedure	A semi transparent text or image overlaid on original/cover image. This type of watermark can also be noticeable with the human‘s eyes.
c.	Invisible watermarking Procedure	Watermark cannot be observed with human’s eyes or human visual system.

Fig. 2 illustrate the various watermarking scheme

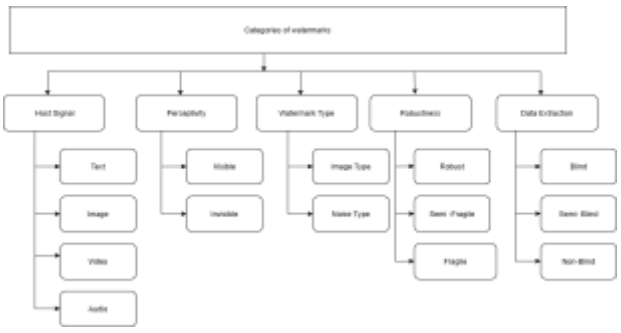

Fig.-2 Illustrate different type of watermark based on various parameters

3. LITERATURE SURVEY

A. Watermarking scheme based on DWT- SVD techniques proposed by Nesrin Abdul Razak[4] for RGB images . In this scheme, DWT is applied to both images i.e. host and watermark image and apply SVD on LL of both resultant images and generate watermarked image by apply algorithm. To evaluate the effectiveness of watermarked image PSNR and MSE parameter are used.

B. Watermarking scheme proposed by Amit K. Singh at al.[5] based on spatial domain to insert watermark into least significant bit of the cover image . The watermark is embedded in the spatial domain; therefore the watermark is vulnerability against various types of attacks.

C. Mayank Mishra et al. [6] proposed method by means of bit plane slicing scheme by applies DWT (Haar wavelet transform). Initially, grey scale cover image divides into 8 bit binary plane. DWT is put on to plane 1 and plane 1 is split into four sub-bands. HH sub –band is chosen for SVD.

$$S = P.Q.(R)^T$$

Where Q is diagonal matrix contain singular values, S indicate the HH sub-band. The matrix Q is used to embed watermark W. This result to matrix T is defined as

$T = Q + SW$, Where S is scaling factor .

The result of proposed method satisfies the reversibility property but proposed scheme is not applicable to colored image.

D. Saikrishna et al. [7] proposed a new approach of invisible and secure watermarking based on texturization. The key used initially to find out the position of embedding. In this approach the host image is classified to black and white texture region. Arnold and DWT transformation are employed to implement this scheme. Embedding is done using based on DWT and human visual system. This scheme proposed for grey scale watermarking.

4. PROPOSED ALGORITHM

In Proposed method, there are two part i.e. embedding and Extraction procedure of watermark into color cover image. To make watermarking robust against various attack SVD and DVT transform is used and scrambling method is used to make it secure .

4.1. Embedding Procedure

Fig. 3 shows the component of original image after DWT Transform. The following steps are used to insert watermark into cover image as depicted in fig. 4.

Step 1: Select Cover Image and watermark image

Step 2: Select watermark image and apply block based scrambling technique using secret key, in this technique the watermark is divided into 64×64 blocks.

Step 3: The scrambled watermark obtained in step 2 is used embedding purpose.

Step 4: Apply DWT and select LL sub band of both cover image and watermark images. Apply SVD on LL band of watermark and cover image and calculate singular matrix for watermarked image.

Step 5: calculate new singular matrix using combination of singular matrix with scaling factor (α)

$$S_{wm} = S_i + \alpha \times S_w$$

Where S_{wm} ,S_i , S_w indicate singular value of watermarked , Cover and Watermark images respectively.

Step 6. Use new singular value and apply inverse SVD and inverse DWT to merge new LL band to the unchanged sub band (HL, LH, HH) to obtained watermarked image.

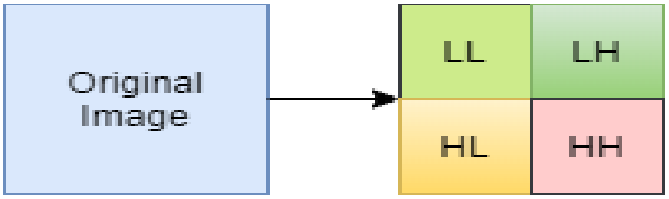

Fig.-3: Shows DWT operation on Image

4.2. Extraction Procedure

The watermark extraction is the reverse process of watermark embedding process. The steps involved in extraction procedure is as under

Step 1: Select watermarked image and apply DWT transform and select LL sub band to apply SVD.

Step 2: Calculate new singular matrix using combination of both singular matrix with scaling factor (α)

$S_{w\_n} = (S_{wm} - S_w)/\alpha$;

Where, S_{w_n} , S_{wm} and S_w represent new singular value , watermarked image and original/ cover image singular value respectively.

Step3: Using extracted singular value and orthogonal matrix, the watermark can be obtained by

$$W = U_w \times S_{w\_n} \times V'_m$$

Step 4: Apply reverse Scrambling method using the same secret key to obtain the original watermark.

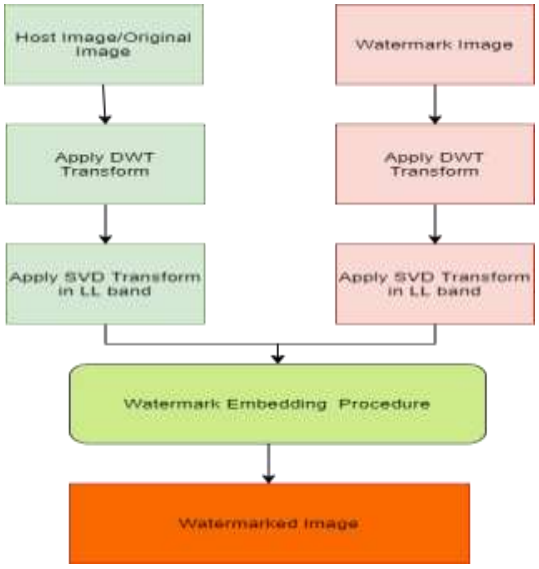

Fig.-4 Watermark Embedding Procedure

5. SIMULATED EXPERIMENTAL RESULTS

The effectiveness of watermarking techniques can be measured by the MSE, PSNR and NCC. All result obtained using MATLAB software by using color image of size 512×512.

MSE and PSNR measure the imperceptibility level and NCC measure robustness.

$$MSE = \frac{\sum_{L,M}[w(l,m)-h(l,m)]^2}{L*M}$$

(1)

$w(l,m)$: watermarked Image

$h(l,m)$: Host or original image

$$PSNR = 10\log_{10}\left(\frac{f^2}{MSE}\right)$$

(2)

f is the maximum fluctuation in input image data type.

Structural similarity index measure (SSIM) is used to measure the similarity between two images. The human visual perception system is highly skilled of recognize structural information from the image. SSIM use three key features to compare i.e . Luminance, contrast and structure. Table 2 depicts the various fidelity parameters obtained from the proposed methods.

Table-2: Effect on fidelity parameter at various S.F

Strength Factor(α)	SME	PSNR	SSIM	NCC(Without Attack)
0.01	0.000069	41.5528	0.9998	1.0000
0.02	0.000279	35.5322	0.9993	1.0000
0.05	0.0017	27.5734	0.9958	1.0000
0.1	0.0070	21.5528	0.9840	1.0000
0.5	0.1748	7.5734	0.7433	1.0000
1.0	0.6994	1.5528	0.4595	1.0000

6. ROBUSTNESS ANALYSIS

Robustness in watermarking refers to the ability of a watermarking system to withstand various attacks or distortions and still allow the embedded watermark to be correctly detected or extracted. Table 3 illustrates the robustness of methods against various attacks.

Table-3: Illustrate NCC value between watermark and watermark extracted after attack.

Name of Attack	NCC
Gaussian attack with variance 0.001	0.7812
Gaussian attack with variance 0.002	0.8102
Salt and Pepper with noise density 0.001	0.9807
Salt and Pepper with noise density 0.002	0.9559
Poisson attack	0.9992

Name of Attack	Watermarked Image after attack	Extracted Watermark
Gaussian attack with variance 0.001		
Gaussian attack with variance 0.002		
Salt and Pepper with noise density 0.001		
Salt and Pepper with noise density 0.002		
Poisson attack		

Fig-5: Effect of attack on watermarked and Extracted watermark image.

Fig.-6: Image Watermarking when alpha=0.01

Fig.-7: Image Watermarking when alpha=1

7. SCRAMBLING ANLYSIS

Scrambling/segmentation in watermarking is the process of rearranging or permuting the watermark data before embedding it into the host media to enhance security. Fig. 6 and 7 depict the effect of scaling factor. Fig 9 shows the visual effect of segmentation on various block size.

Block Size	Scrambled Image
64×64	
32×32	
16×16	
8×8	

Fig.-9: Effect of block size in image scrambling

8. CONCLUSION

Watermarking has emerged as a powerful tool for ownership rights and authenticity of digital media. Digital watermark can be inserted into any digital media in a way they are indiscernible to human eyes but are detectable only to owner's computer algorithm for the retrieval of watermark from the cover image. Lots of work has been done on gray scale image .In this paper, Block based (64×64) scrambling/segmentation technique is proposed to secure watermark or to breach the correlation among pixels. An "attack" is the process that may harm information conveyed by the watermark. Dimensional reduction technique (SVD) and watermark is inserted using Transform domain (DWT) to make watermarking technique more robust against various attacks. In a good watermarking technique, the watermark should be retained even after different types of attack [8].

REFERENCES

[1] Patsariya, S., Dixit, M.: A Survey on Watermarking and Its Techniques. Algorithms for Intelligent Systems. 71–78 (2021). https://doi.org/10.1007/978-981-33-4893-6_7.

[2] Singh, A.K., Sharma, N., Dave, M., Mohan, A.: A novel technique for digital image watermarking in spatial domain. 2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing. (2012). https://doi.org/10.1109/pdgc.2012.6449871.

[3] Pandey, M.K., Parmar, G., Patsariya, S.: An Effective Way to Hide the Secret Audio File Using High Frequency Manipulation. Communications in Computer and Information Science. 125–130 (2011). https://doi.org/10.1007/978-3-642-18440-6_15.

[4] Razak N. A. : Digital Image watermarking base on DWT and SVD techniques. Journal of Network, Communication and emerging technology(JNCET) , volume 8,issue 02 (2018).

[5] Singh A.K ,Sharma N., Dave M.,Mohan A. : A novel Technique for Digital Image Watermarking in Spatial Domain. 2nd IEEE International conference on Parallel , Distributed and Grid Computing (2012)

[6] Mishra, M., Rout, N.K., Budipi, N.R.: Bit Plane Slicing Based Digital Watermarking Technique in Dwt Domain. International Journal of Engineering and

Advanced Technology. 8, 525–529 (2019). https://doi.org/10.35940/ijeat.e7301.088619.

[7] Saikrishna, N., Resmipriya, M.G.: An Invisible Logo Watermarking Using Arnold Transform. Procedia Computer Science. 93, 808–815 (2016). https://doi.org/10.1016/j.procs.2016.07.299.

[8] Sunesh , Kumar H.:Watermarks Attacks And Application in Watermarking. National Workshop-Cum Conference on Recent Trends in Mathematics and Computing (RTMC)(2011)