Review of Digital Watermarking Techniques

Pooja Kulkarni   Shraddha Bhise   Sadhana Khot

Computer Department, VIIT, Savitribai Phule Pune University

ABSTRACT
Digital watermarking is delicate to various attacks in spatial domain, Hence in most of the watermarking technique's transform domain is used. This paper takes a survey of such digital watermarking techniques and methods like Discrete cosine transform (DCT), Singular value decomposition (SVD), SVD-DCT, DWT-SVD with different approaches along with their applications, advantages and disadvantages. Further future work and implementation plan is also mentioned in the paper.

Keywords
DCT, Discrete Wavelet transform (DWT), SVD

1. INTRODUCTION
Now a days, billions of bits of information bring into existence in every half a second. And due to great acceptance of the Internet along with expeditious evolution of multimedia technology, users have more likelihood to use digital data (image, video and audio files, web publishing digital repositories and libraries). After all copying a digital data is very easy and fast, problems like, protection of rights of the content and proving ownership, arises. Digital watermarking is a solution to these problems as it has various applications like copyright protection, authentication, secret communication, and measurement. E-commerce, E-voting, medical safety, broadcasting monitoring, military and indexing can be protected by digital watermarking [7].Watermark remains intact to the cover image even if it is copied, is the characteristic of watermarking. Hence to certify ownership of data watermark is extracted and tested. Digital watermarking is the course of action of embedding a watermark in a multimedia object. This object may be image, audio, video and any digital content for the purpose of information hiding. Powerful watermarking technique should be selected for strong watermark embedding.

According to type of document like text, image, audio, video used for watermarking, various techniques are used. Depending on human perception these techniques are classified as visible and invisible methods of watermarking. According to application source based and destination based watermarking techniques are used. Whereas on the basis of domain in which the watermark is inserted, two categories are made i.e., spatial-domain, and transform-domain methods [7].

Inserting the watermark into the spatial-domain component of the cover image is a direct method. It is easy to implement and requires less computations [7]. But the basic problem in watermarking in spatial domain is that the watermark is more susceptible to attacks than transform domain[1]. Whereas ,magnitude of coefficients in a transform domain are modulated, while embedding watermark in the transform-domain techniques such as discrete cosine transform(DCT), discrete wavelet transform (DWT), and singular value decomposition (SVD) [4]. Transform-domain methods provide more information embedding and more robustness against many common attacks,. But the computational cost is bigger than spatial-domain watermarking techniques.

2. ALGORITHM DESCRIPTION
2.1 Watermarking using DCT Technique
While embedding watermark in image using DCT, low and mid frequencies are considered. Because during image compression process, high frequencies are disappeared. In image watermarking using DCT, initially DCT coefficient of original image is calculated. After performing this calculation, DCT coefficient of watermark image is calculated. And then different Alpha and Beta values are assigned to this DCT coefficient respectively. After embedding this watermark image into original image, we get Watermarked image as a output in frequency domain. And hence to get watermarked image in image (time) domain, we have to compute inverse DCT of watermarked image. This above DCT technique of embedding watermark is applied on image by partitioning original image into various blocks [1]. And then Alpha and Beta values are allocated to each block.

$$I_{ij} = X_{ij} + W_{ij}$$

Where X_{ij} is DCT coefficient of original image and W_{ij} is embedding factor. The watermark is embedded into spectral components of the image, refer fig (1).

DCT coefficient of watermark image, is scaling factor and is embedding factor. The watermark is embedded into spectral components of the image, refer fig (1).

Advantages- Watermarking performed using DCT based technology is more robust than spatial domain techniques. Watermarking carried out with this algorithm are robust against simple image processing operations like low pass filtering, brightness and contrast adjustment, blurring, etc. The watermark embedded using DCT technique will not be destroyed by any type of attack as the watermark is embedded into the middle frequency coefficients and hence visibility of image is also not get affected.[2]

Disadvantage- Invariance property of system get destroyed because of block wise DCT. While performing quantization, some higher frequency components get stifle [1].
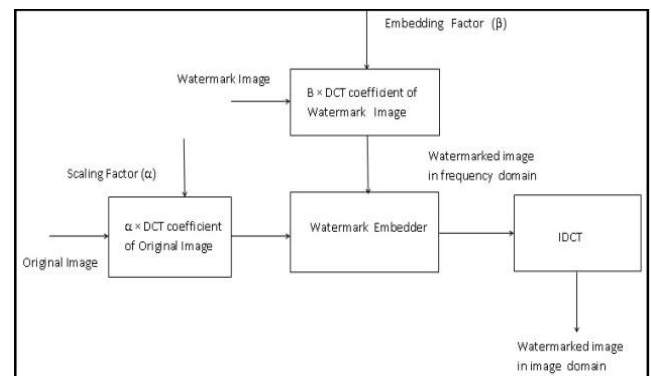

Figure1 : DCT Technique

2.2 Watermarking using DWT Technique

The DWT divides the given image into four components namely LL, HL, LH and HH where the first letter corresponds to applying either a low pass frequency operation or high pass frequency operation to the rows, and the second letter refers to the filter applied to the columns. In this algorithm, watermark is embedded into the host image by modifying the coefficients of high frequency bands i.e. HH subband refer fig (2)

This paper [3], describes a embedding and retrieval of watermark as follows-

Phase 1- Embedding of watermark-

1. A host Image is divided into 4 Bands using DWT: LL, HL, LH, HH(Diagonal).

2. Embedding of watermark is done in HH Band.

3. Block in which embedding is performed is found out using quard tree decomposition, and then DWT is performed on host image.

4. Watermark is resized and encoded by convolution coding.

5. Outputs of step 3 and 4 are combined together and adding of key for security is optional.

6. After modifying values of HH Band , apply IDWT, and obtain watermarked image.

Phase 2- Retrieval of watermark-

1. Perform DWT on Watermarked Image.

2. Perform DWT on HH band of the image.

3. Extraction of Watermark Can be done using formula

   Watermark=(Watermarked image-key)/host image

4. Perform Inverse Transformation on Watermarked Image and put the right Value of key if inserted to extract watermark.

Advantages- This technique is efficient to attacks like deblurring, salt and pepper attack, cropping, rotation, scaling, JPEG compression[3]
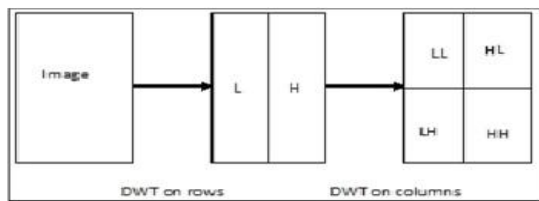

Figure2 : DWT Technique

2.3 SVD based Watermarking Algorithm

Another approach used for watermarking is based on a Singular Value Decomposition (SVD) method which provides robustness and security [4] and which is used for watermark casting and detection. SVD is a method in which a given image represented as a matrix 'A' is decomposed into a product of two orthogonal matrices 'U' and 'V' and 'S' matrix as -

$$A = USV^T \qquad (1)$$

Where matrix 'S' is a diagonal matrix which consists all nonnegative Eigen values of matrix A. Matrix 'U' and 'V' are orthogonal because product of matrix 'U' and transpose of 'V' is Identity matrix.

Steps for Embedding of watermark in SVD algorithm -

1) Consider that a host image is represented as a matrix 'A'.

2) Apply SVD on host image to get matrix 'U', 'S' and 'V' as shown in eq.(1).

3) Modify the 'S' matrix of host image using watermark image 'W'.

4) $S_* = S + \alpha W$ where α is any positive scalar factor, S_* is modified version of matrix 'S'.

5) Apply SVD on S_* to obtain its corresponding singular values as U_w, S_w and V_w.

6) Now, Watermarked image 'I' can be obtained by I = USwVT

The testing of algorithm on various images is done [4] and robustness is checked by applying six aspects: adding noise, low pass filtering, image compression, scaling, image cropping and rotation.

Advantage-Advantage of using SVD technique is that SV's of an image are stable [4] i.e. even if we make a little change in our image, suddenly the SV's of that image are not affected. Another advantage of using SVD technique is that there is no constraint on size of matrices, they can be either square or rectangle [4].

2.4 DCT-DWT Technique

In [5], The method proposed uses DCT and 3 levels DWT. DWT of host image is found out and DCT of watermark image is obtained and inserted into high frequency band of DWT of host image.

2D DCT is calculated by 1D transformation on each row first and then 1D transformation again on each column. In 2D DWT, 1D DWT is performed first on each row also known as horizontal filtering and then 1D DWT is again performed on each column also known as vertical filtering. In this technique, while embedding the watermark; using DCT, watermark image is transformed and using 2D DWT host image is decomposed by L-levels. When low frequency band information and high frequency band information images are then obtained, then higher DWT is better. To hide the watermark image, one key is used. For completing the insertion of watermark, values of wavelet coefficients of selected blocks are changed and then inversing of the wavelet transform of the image is done by L level to obtain watermarked image. Watermark extraction can also be done in same with embedding but in reverse order. The entire technique is explained in fig (3).
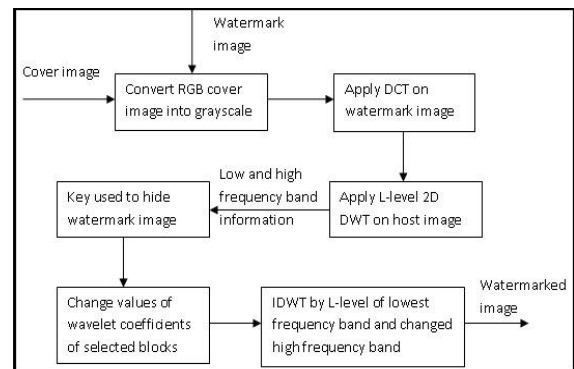

Figure3 : Modified Algorithm for combined DCT and DWT

Advantage- Imperceptibility and robustness are achieved successfully, where normalized correlation is high and computational time required is low [5]. Disadvantage- DWT is major part of this method but disadvantage is it needs to calculate the 3level DWT each time which can take more computation time than level1 DWT. This method works on gray-scale images is another disadvantage [5]. Application- This technique can be applied more in invisible watermarking [5].

2.5 Combination of DWT-SVD Technique
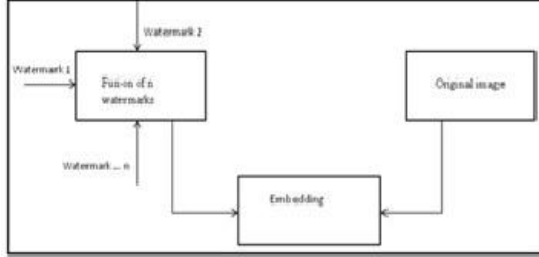
**Figure4 : Embedding of watermark by DWT-SVD using wavelet fusion algorithm**

In paper [6] , multiple watermark images are fused together and watermarked image is obtained by embedding together the resultant fused watermark and original image, refer fig (4). This process involves two Phases.

Phase1: Fusing multiple watermarks. Here, primary and secondary watermarks are fused together to obtain a fused image. This fused image is used as an watermark W in embedding in phase 2.

Phase 2: Embedding of resultant fused watermark image into original image using DWT-SVD algorithm. This can be done by using below steps-

1. The host image is divided into 4 sub-bands using one level DCT.

2. As explained in section C, SVD based watermarking algorithm, according to the mentioned steps [1-5] of embedding of watermark, Aw i.e. watermarked image is obtained.

Also using this algorithm we can extract the fused watermark back from the watermarked image in the presence of severe attacks, refer fig (5).
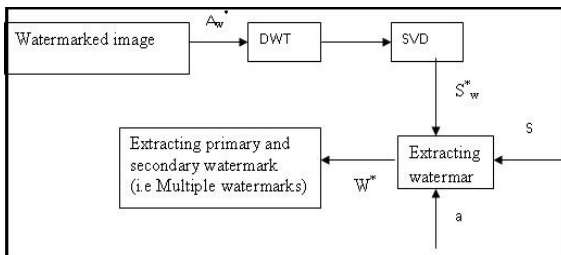
Figure5 : Extraction of watermark using DWT-SVD

This process involves two Phases

Phase 1: The extraction of fused image By using one-level DWT, conversion of watermarked image is done and the fused watermark W* is obtained by following steps [1-3] of detection of watermark given in section C, SVD based watermarking algorithm.

Phase 2: Extraction of multiple watermarks. From fused images, primary, secondary watermarks are extracted.

Advantage- This method improves the capacity of embedded information and robustness without affecting the original quality of original image [6].

Application- Applications involving embedding of multiple images as watermark [6].

In [7], SVD performs watermarking on singular values of cover image hence they work in less time, hence this approach requires minimum efforts for calculation. If SVs are modified to some extent that will not change the visual appearance of the cover image, hence can get better robust and transparent watermarking. When the image is divided into four subbands at level-1 DWT namely LL,LH, HL, HH; LL Is divided further to get other level of decomposition and LL is low-frequency part which is receptive for human eyes, hence watermark embedding is done in other subbands. This method proposes that host image has to decomposed into four subbands by one-level DWT and SVD is applied to only intermediate frequency subbands. Watermark is partitioned into two parts W1 and W2 and SVs of HL and LH subbands are changed with W^1 and W^2 and then SVD is applied.
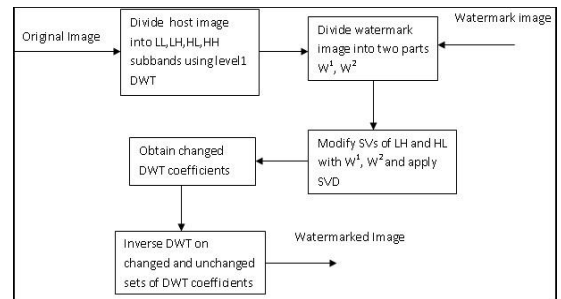
$$S^k + \alpha W^k = U_w{}^k S_w{}^k V_w{}^{kT}$$

where α is scale factor which controls the strength of watermark.

Then changed DWT coefficients for two parts is obtained

$$A^{*k} = U^k S_w{}^k V^{kT} ; \qquad k = 1; 2$$

After performing inverse DWT on two parts of changed DWT coefficients and unchanged DWT coefficients watermarked image is obtained. The entire technique is explained using fig (6).
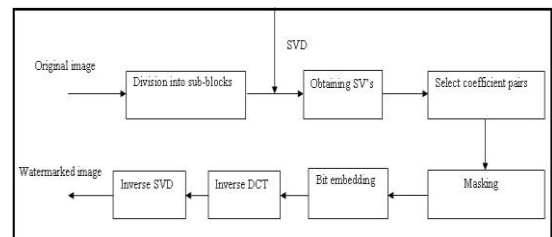

Figure6 : DWT-SVD Technique

2.6 Hybrid SVD-DCT algorithm

This technique involves two steps as

Step:1 Applying SVD to sub-blocks of cover image block.

Step:2 Applying DCT on the sub-blocks comprised of the first singular values (SVs) of each image block.

Figure7 :Hybrid SVD-DCT Technique

Referring fig (7), the watermark is embedded in the cover image through the following steps:

1. Select the coefficients pairs to be modified in the potential positions of the SVD-DCT block

2. Manipulate the frequency mask

3. Weight the watermark amplitude

4. Embedding of watermark bits

5. Take inverse DCT and then inverse SVD to obtain the watermarked image.

Advantage- There is a problem of not placing the watermark in perceptually insignificant regions of the image because of many common signal and geometric processes affect these components. This is solved by using this technique by embedded watermark only in the largest SVs which correspond to the energy of the most perceptually significant regions in the original image, in order to achieve high robustness against perceptivity preserving operations. And this technique is highly robust against some typical general content-preserving attacks and geometric distortion attacks.

Application- For image copyright protection [8].

3. COMPARATIVE STUDY
1. Original image of size 256×256 pixels and watermark image of size 20×50 pixels [9].

Table1 :Result of various attacks on DCT watermarked images using PSNR

SR NO	ATTACK	PSNR (dB)(After attack)
1	Unsharp	10.7890
2	Gaussian Noise	10.8990
3	Salt and Pepper	15.5372
4	Rotation	8.8837

2. Original image of size 256×256 pixels and watermark image of size 20×50 pixels [9].

Table4 :Result of various attacks on DWT watermarked images using PSNR

SR NO	ATTACK	PSNR (dB)(After attack)
1	Unsharp	11.7937
2	Gaussian Noise	10.8675
3	Salt and Pepper	22.9970
4	Rotation	8.9904

3. Original image of size 512×512 pixels and watermark image of size 16×16 pixels [10].

Table2 :Performance results in terms of PSNR for DCT-SVD

SR NO	ATTACK	PSNR (dB)(After attack)
1	Unsharp	34.749
2	Gaussian Noise	39.68
3	Salt and Pepper	38.971
4	Rotation	33.129

4. Original image of size 256×256 pixels and watermark image of size 256×256 pixels [11].

Table3 :Performance results in terms of PSNR for DWT-SVD

SR NO	ATTACK	PSNR (dB)(After attack)
1	Gaussian Noise	33.53
2	Salt and Pepper	35.77
3	Rotation	34.41

4. CONCLUSION
Thus, this paper focuses on digital image watermarking in frequency domain and digital watermarking techniques like DCT, DWT, SVD, DCT-SVD, DWT-SVD, their advantages, disadvantages and applications. Comparative study of various techniques is also provided in this paper. Both embedding and extraction of watermark is being done using the techniques mentioned in this paper. For checking the robustness of these methods various attacks on watermarked images are performed like Salt and Pepper noise, Rotation, Gaussian noise and unsharping. DCT-SVD shows better results among these methods compared in terms of PSNR after attack on watermarked image.

5. ACKNOWLEDGEMENT

6. REFERENCE
[1] Shahin Shaikh, Manjusha Deshmukh,"Digital Image Watermarking In DCT Domain", International Journal of Emerging Technology and Ad-vanced Engineering ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 4, April 2013

[2] Prabhishek Singh, R S Chadha "A Survey of Digital Watermarking Techniques, applications and Attacks" International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 9, March 2013.

[3] Chirag Sharma, Deepak Prashar, "DWT Based Robust Technique of Watermarking Applied on Digital Images",

International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-2, May 2012

[4] Ruizhen Liu and Tieniu Tan, "A Svd-Based Watermarking Scheme For Protecting Rightful Ownership*", MULTIMEDIA IEEE TRANSA-TIONS, ISSN 1520-9210 VOL. 4, ISSUE 1

[5] Reena Anju and Vandana "Modified Algorithm for Digital Image Wa-termarking Using Combined DCT and DWT ", International Journal of Information and Computation Technology. ISSN 0974-2239 Volume 3, Number 7 (2013), pp. 691-700 International Research Publications House

[6] Ezz El-Din Hemdan, Nawal El-Fishawy, Gamal Attiya, Fathi Abd El-Samii, "Hybrid Digital Image Watermarking Technique For Data Hiding", 30th NATIONAL RADIO SCIENCE CONFERENCE (NRSC 2013) April 16-18, 2013, National Telecommunication Institute, Egypt

[7] Chih-Chin Lai,Member, IEEE, and Cheng-Chih Tsai, " Digital Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition", IEEE TRANSACTIONS ON INSTRUMENTATION AND MEASUREMENT, VOL. 59, NO. 11, NOVEMBER 2010

[8] Zhen Li, Kim-Hui Yap and Bai-Ying Lei, "A New Blind Robust Image Watermarking Scheme In Svd-Dct Composite Domain", 2011 18th IEEE International Conference on Image Processing.

[9] Pooja Dabas , Kavita Khanna, "Efficient Performance of Transform Domain Digital Image Watermarking Technique over Spatial Domain", International Journal of Advanced Research in Computer Science and Software Engineering , Volume 3, Issue 6, June 2013 ISSN: 2277 128X.

[10] A.Rajani,Dr.T.Ramashri,"IMAGE WATERMARKING ALGORITHM USING DCT, SVD AND EDGE DETECTION TECHNIQUE", Interna-tional Journal of Engineering Research and Applications(IJERA) ISSN: 2248-9622 Vol. 1, Issue 4, pp.1828-1834

[11] Praful Saxena, Shanon Garg and Arpita Srivastava, "DWT-SVD Semi-Blind Image Watermarking Using High Frequency Band", 2nd Inter-national Conference on Computer Science and Information Technology (ICCSIT'2012) Singapore April 28-29, 2012