IJCSC 0973-7391 Vol 6 • Number 2 April - Sep 2015 pp. 208-213 **Impact Factor: 2.5** **Available at** www.csjournals.com

Digital Watermarking SVD-DWT-DCT Using Kalman Filter

Renuka kaur, Prof.Gulshan Goyal
Research scholar, Associate Professor
Chandigarh university, Chandigarh university

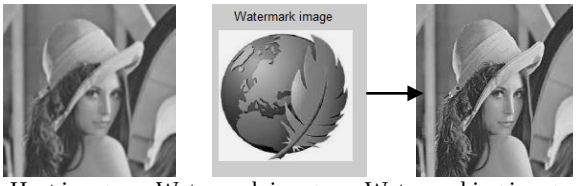
Abstract: This research paper describes the digital watermarking of transform domain. In image watermarking, information is embedded in cover image to prove ownership. This information must remain detectable even if image is manipulated. Applications of digital image watermarking are copyright protection, health care, fingerprinting, id card security, authentication & integrity verification. In this paper SVD-DWT-DCT watermarking technique using Kalman filter is describes.
Keywords: watermarking, Discrete Cosine Transform, Discrete Wavelet Transform, Digital watermarking, Single value decomposition, Kalman filter.

I. INTRODUCTION

1.1 DIGITAL WATERMARKING

Digital watermarking is the process of embedding secret data into a multimedia element (that is video, image, song, video, documentation) and this information embedded in such a way that it is extract and detect even if image is modified or altered. Digital image watermarking technique is to embedding a host image with information which is called watermark, and then watermark image will be transmitted and can be extracted at the receiver [2].

EXAMPLE



Host image Watermark image Watermarking image

Fig 1.1 Example of digital watermarking

1.2 REQUIREMENTS OF DIGITAL WATERMARKING

There are three main requirements of digital watermarking which describe below:

1. **Transparency**

The digital watermark should not affect the quality of the original image after it is watermarked [1]. Watermarking should not introduce visible distortions because if distortions are introduced it reduces the commercial value of the image.

2. **Robustness**

Cox et al. (2002) defines robustness as the "ability to detect the watermark after common signal processing operations". Watermarks could be removed intentionally or unintentionally by simple image processing operations like contrast or brightness enhancement, gamma correction etc. Hence watermarks should be robust against variety of such attacks [1].

3. **Capacity**

Cox et al. (2002) define capacity as "the number of bits a watermark encodes within a unit of time". This property describes how much data should be embedded as a watermark to successfully detect during extraction [1].

1.3 CLASSIFICATION OF IMAGE WATERMARKING

Image watermarking techniques can be classified from five perspectives as shown below:

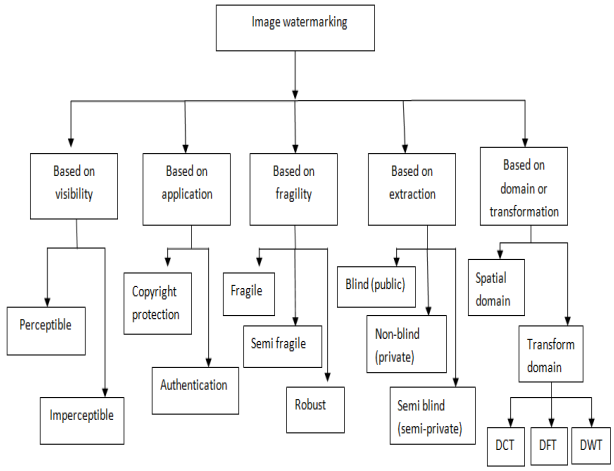


Fig 1.2 Classification of image watermarking [3]

1. **Based on Visibility**

Watermarks may be visible or invisible. A visible watermark is easily detected by observation while an invisible watermark is designed to be transparent to observer and detected using signal processing techniques [3].

2. **Based on Application**

The watermarking techniques are classified based on application such as copyright protection or authentication. Copyright protection is useful for ownership verification. Image authentication systems have applicability in law, commerce, journalism.

3. **Based on Fragility (Ability to Resist Attack)**

Based on fragility, watermarking schemes are classified as fragile, semi fragile. A fragile watermark is designed to detect slight changes to watermarked image with high probability. Fragile watermarking is used for content authentication and tamper detection [3]. Semi fragile

watermarking schemes are used to discriminate between malicious manipulations.

4. **Based on Extraction**

Image watermarking is classified as blind, semi blind or non blind. In blind watermarking, watermark is extracted without original image thus reducing storage requirements. Semi blind watermarking does not use original image for detection but answers the question in positive or negative form. Non blind watermarking systems require original image for extraction [3]. This kind of scheme is more robust than others because it requires access to secret material.

5. **Based on Domain of Transformation**

In spatial domain methods, watermark information is embedded directly into image pixels. The images are manipulated by altering one or more number of bits that make up pixels of the image [3]. In frequency domain methods, watermark information is embedded in the transform domain.

1.4 DIGITAL IMAGE WATERMARKING BASIC MODEL

The basic model of digital image watermarking consists of two parts, first part is the watermark embedding process and the second part is the watermark detection process which shown below: Watermarked embedding represents sender, the Watermark is embedded into the cover image with the secret key that ensures the security of watermarking process [2]. The output is the watermarked image.

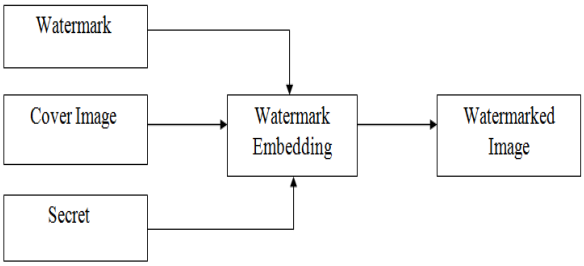


Fig 1.3 Watermarked Embedding [2]

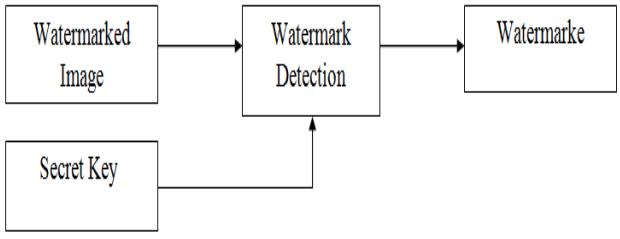


Fig 1.4 Watermarked Detection [2]

Watermark detection represent receiver side, the detector detects the watermark from the watermarked image by using the secret key to recover the watermark.

II. TRANSFORM DOMAIN

Transform domain uses the transform coefficients to embed the watermark. Transform domain techniques are very robust against attacks, because the watermark is spread in images. Images can be represented in spatial domain and transform domain. The transform domain image is represented in terms of its frequencies; however, in spatial domain it is represented by pixels. In simple terms transform domain means the image is segmented into multiple frequency bands [1].

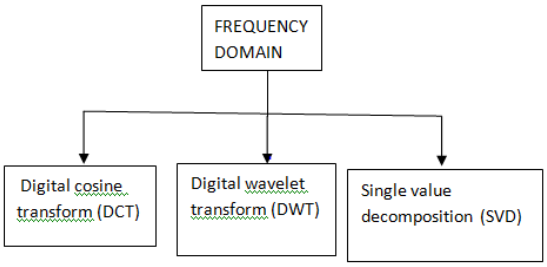


Fig 1.5 Classification of frequency domain

A. DWT TECHNIQUE

In the last few years wavelet transform has been widely studied in signal processing in general and image compression in particular. In some applications wavelet based watermarking schemes outperforms DCT based approaches [1]. The basic idea of discrete wavelet transform (DWT) in image process is to multi differentiated decompose the image into sub image of different spatial domain and independent frequency district. Then transform the coefficient of sub image [7]. After the original image has been DWT transformed, it is decomposed into 4 frequency districts which is shown below:

1. One low frequency district (LL)
2. Three high frequency districts (LH,HL,HH)

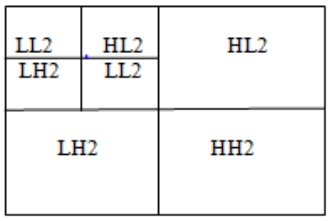


Fig 1.6 DWT decomposition [7]

2.1 CHARACTERSTICS OF DWT

1. The wavelet transform decomposes the image into three spatial directions such as horizontal, vertical and diagonal.

a. Horizontal band (LH)
b. Vertical band (HL)
c. Diagonal band (HH)
d. Lowest band (LL)

2. Wavelet Transform is computationally efficient and can be implemented by using simple filter convolution [1].
3. Magnitude of DWT coefficients is larger in the lowest bands (LL) at each level of decomposition and is smaller for other bands (HH, LH, HL) [1].
4. The larger the magnitude of the wavelet coefficient the more significant it is.

5. Watermark detection at lower resolutions is computationally effective because at every successive resolution level there are few frequency bands involved [1].
6. High resolution sub bands helps to easily locate edge and textures patterns in an image.

B. DCT TECHNIQUE

DCT is widely used in digital image watermarking since it has strong robustness. It has many frequency coefficients, such as single direct current DC coefficient, low frequency coefficients, mid frequency coefficients, and high frequency coefficients [2]. By the different characters of these coefficients, we can obtain different effects upon digital watermarking system.

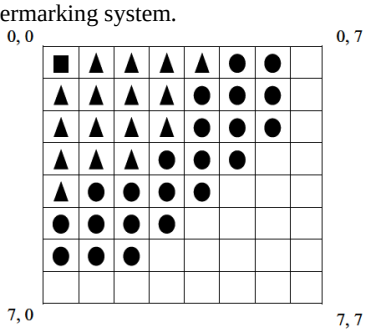


Fig 1.7 Coefficient of DCT [2]

C. SVD TECHNIQUE

Singular value decomposition is used to approximate large, unmanageable matrices to smaller invertible square matrices. The application of the singular value decomposition to an image compresses without significant data loss and to reduce the space required to store images [16]. SVD transformation preserves both one way and non symmetric properties. SVD in digital image has advantage like the size of matrices from SVD transformation is not fixed and can be a square or a rectangle.

The singular values of the host image are modified to embed the watermark image by employing multiple singular functions [4].

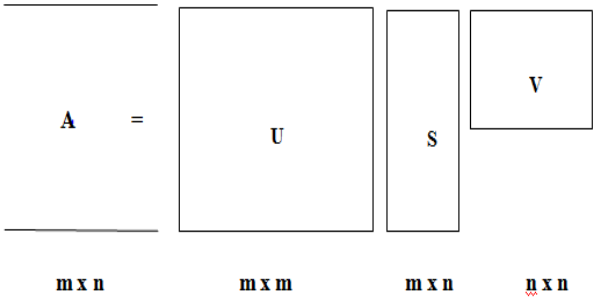


Fig 1.8 Factoring A to USV [19]

2.1 VARIOUS ATTACKS ON DIGITAL IMAGE WATERMARKING

Watermarked image is transmitted through watermark channel and due to channel there may be possible attacks or distortions on watermarks. It includes signal processing or geometric attacks. These attacks may be intentional that is malicious or unintentional which is accidental [7].

2.1.1 Signal Processing Attacks

Signal processing attacks are also known as Image Processing Attacks or Non geometric Attacks. Some common signal processing attacks are Gaussian noise, salt and paper noise, compression etc.

2.1.2 Geometric Attacks

Geometric attacks attempt to destroy synchronization of detection. It makes detection process difficult and sometimes even impossible. Unintentional geometric attacks have manipulations in image processing like scaling images for web site, changing digital video's aspect ratio, printing, scanning marked documents and cropping an image to extract a region of interest [7]. Geometrical distortions are classified basically into two types [5].

a) Global geometric attack affects all the pixels of the image in similar manner.
b) Local geometric attack affects different portions of an image in different ways.

2.2 PROPOSED WORK

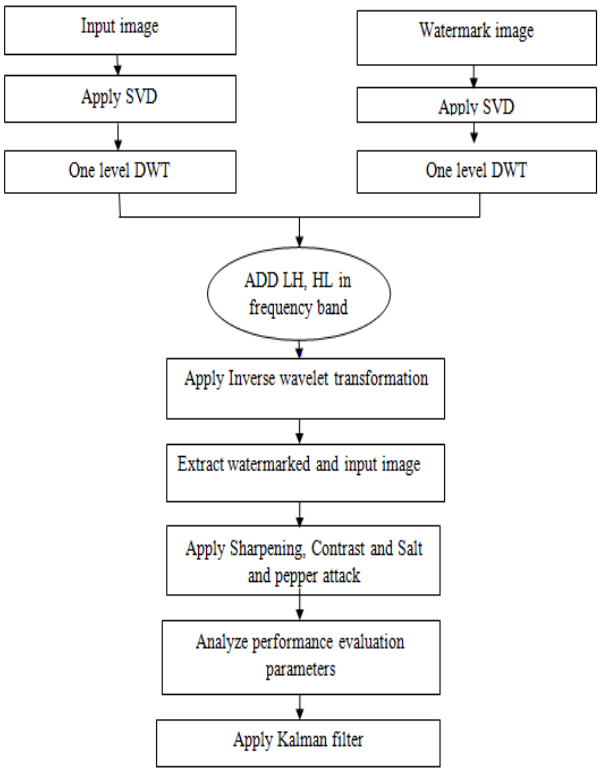


Fig 1.9 Steps of proposed work

Step 1: Input an original image and watermark image.
Step 2: Modify original image with alpha probability factor.
Multiplication of USV matrices.

$$A=USV^{T} \quad [16]$$

Step 3: To divide an input image into four sub bands such as HH,HL,LH,LL.
Step 4: Again divide sub band HL or HH into four smaller sub band.

Step 5: Apply DWT in sub band.
Step 6: Inverse Discrete Wavelet Transformation (IDWT) is used to extract an image.
Step 7: Kalman filter is used for noise removal.
Step 8: Watermarked image is display as output and evaluating the performance using performance evaluation parameters like Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), Robustness of an image.

2.3 RESULTS

2.3.1 DWT-DCT watermarking technique

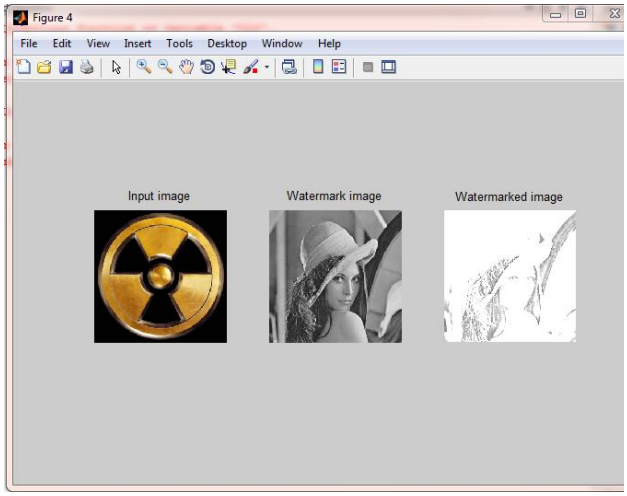


Fig 1.10 Output image first image is input image that is original image, second is watermarke image and third image is watermarked image with DWT-DCT technique.

2.3.2 SVD-DWT-DCT watermarking using kalman filter

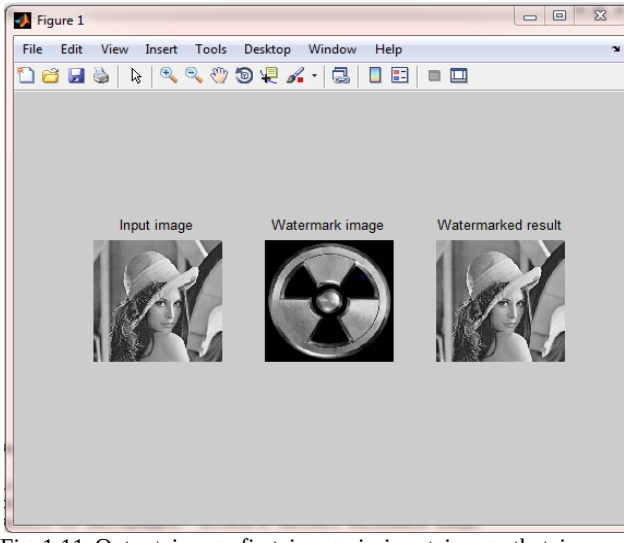


Fig 1.11 Output image first image is input image that is original image, second is watermarke image and third image is watermarked image with SVD-DWT-DCT technique using kalman filter.

Table 1.1 COMPARISON OF EXISTING AND PROPOSED TECHNIQUE

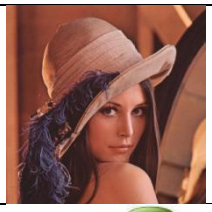
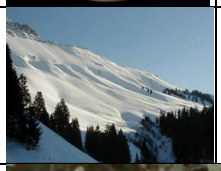
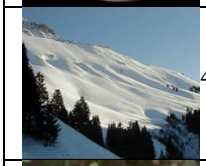
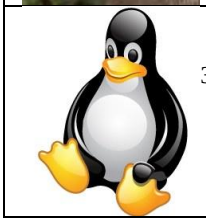
Input Image	DWT-DCT		SVD-DWT-DCT using kalman filter	
	MSE	PSNR	MSE	PSNR
	250.95	24.17	36.88	32.50
	250.95	24.17	34.01	32.60
	135.78	26.72	36.00	32.60
	250.85	24.63	35.67	32.40
	137.74	26.82	34.54	32.50
	222.39	24.72	26.40	34.79

Table 2.2 ROBUSTNESS OF DIGITAL WATERMARKING

Image	Sharpened				Salt and pepper attack	
	MSE	**PSNR**	**MSE**	**Contrast**	**MSE**	**PSNR**
	64.82	30.01	244.29	24.29	65.23	30.04
	64.54	30.02	244.29	24.29	64.96	30.02
	49.70	31.21	130.12	29.13	50.08	31.21
	48.67	31.34	244.65	24.69	64.84	31.56
	54.85	30.76	131.78	24.78	65.75	30.07
	39.03	32.03	51.35	30.41	39.76	32.00

III. CONCLUSION

In this research paper kalman filter is used in watermarking technique. By using kalman filter enhanced the peak signal to noise ratio. There are many watermarking technique such as SVD, DCT, DWT for watermarking. To compare the DWT-DCT with SVD-DWT-DCT by apply kalman filter using parameters such as PSNR, MSE, robustness of an image. By using DCT block technology, watermarking is embedded into the middle frequency band of wavelet transformation domain. And before embedding this watermark image has been discrete cosine transformed in order to improve its robustness. By using Kalman filter mean square error gets reduced.

REFERENCES

[1] M.P Vidyasagar, Song Han, "A Survey of Digital Image Watermarking Techniques", 2005, 3rd IEEE International Conference on Industrial Informatics (INDIN), Perth, Australia.

[2] A.Mohammad and M.Z.Akram, "Properties of digital image watermarking", 2013, IEEE 9th International colloquium on signal processing and its applications, Malaysia.

[3] S.J Vaishali and R.G Sachin, "Comprehensive survey of image watermarking ", july 2013,International Journal of Advances in Engineering & Technology, Vol. 6, Issue 3, pp. 1271-1282

[4] H.G Víctor, C.R. Clara, "Algoritmo de Marca de Agua Basado en la DWT para Patrones Visualmente Reconocibles",2006, IEEE LATIN AMERICA TRANSACTIONS, VOL. 4, NO. 4.

[5] K. Nikita and G. R. Sinha. "Image watermarking using 3-level discrete wavelet transform (DWT)", 2012, International Journal of Modern Education and Computer Science (IJMECS) 4.3: 50.

[6]K. Prayoth "An Optimal Robust Digital Image Watermarking Based on Genetic Algorithms in Multiwavelet Domain", 2009,wseas transactions on signal processing.

[7] J. Mei, Li Sukang ,"A Digital Watermarking Algorithm Based On DCT and DWT", 2009, Proceedings of the 2009 International Symposium on Web Information Systems and Applications (WISA'09), Nanchang, P. R. China, May 22-24, 2009, pp. 104-10.

[8] Hu Guan and Zhi Zeng, "A Novel Robust Digital Image Watermarking Algorithm based on Two-Level DCT",2014, IEEE International S&T Cooperation.

[9] D.Nilanjan and B.Debalina "DWT-DCT-SVD Based Blind Watermarking Technique of Gray Image in Electrooculogram Signal", 2012, IEEE 12th International Conference on Intelligent Systems Design and Applications.

[10] S S Bedi, Ashwani Kumar, "Robust Secure SVD Based DCT – DWT Oriented Watermarking Technique for Image Authentication", March 2009, International

Conference on IT to Celebrate S. Charmonman's 72nd Birthday, Thailand.

[11] K.Prayoth and A.Kitti "An Optimal Robust Digital Image Watermarking Based on Genetic Algorithms in Multiwavelet Domain",jan 2009, Wseas transactions on signal processing , Issue 1, Volume 5, ISSN: 1790-5052.

[12] S.G. Sudhanshu, A.G. Ashok, "Combined DWT-DCT Digital Watermarking Technique Software Used for CTS of Bank", 2014, International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT).

[13] L. Li, X. He-Huan "A novel image watermarking in redistributed invariant wavelet domain", 2011, The Journal of Systems and Software.

[14] D. Gabor, "Theory of communication", 1946, Journal of Institution of Electrical Engineers, vol. 93, pp. 429–457.

[15] Adel, M.H.Robert and G.Gheorghita, "High Capacity Steganographic Method Based Upon JPEG", 2009, IEEE, The Third International Conference on Availability, Reliability and Security.

[16] C. Kuo-Liang, "On SVD-based watermarking algorithm", 2007, Applied Mathematics and Computation.

[17] S.P. Surya, R. Paresh, "A Robust Watermarking Approach using DCT-DWT", 2012, International Journal of Emerging Technology and Advanced Engineering.

[18] H. poonam, "A Review of Digital Watermarking Strategies", 2014, International Journal of Advance Research in Computer Science and Management Studies.

[19] S. Sura Ramzi, "Digital ImageWatermarking Using Singular Value Decomposition", 2010, Third Scientific Conference Information Technology, Vol. 7, No. 3.