Modified Robust Watermarking Scheme based on DCT

Deepak Vats
M. Tech Student
Vivekanand Institute of Technology and Science, Ghaziabad, U.P. – 201015

Ajeet Singh
Assistant Professor
Vivekanand Institute of Technology and Science, Ghaziabad, U.P. – 201015

Abstract

In this research paper, a modified method for non-blind image watermarking that is robust against affine transformation and ordinary image manipulation is proposed. This method presents a watermarking technique based on Discrete Cosine Transform (RDWT). After applying DCT to both cover and watermark images, then IDCT is applied for watermark extraction from the watermarked image. The advantage of the reviewed technique is its robustness against most common attacks. Analysis and experimental results show higher performance (high PSNR and low MSE) of the proposed method in comparison with the previous RDWT-SVD method.

Keywords: Digital Image Watermarking, Redundant Discrete Wavelet Transform, Singular Value Decomposition

I. INTRODUCTION

In the internet age, multimedia (image, text, audio and video) data is requirement of the user and companies for their personal and social purposes. All multimedia files are transferred and kept on internet for accessing those files from anywhere. These multimedia files should be secured and authenticated by particular user or company, otherwise anyone can thieve data and sell to other company. So hiding the data or encrypting the data is necessary for the copyright purposes such that no unintended person can access its originality or authentication. There are many ways for hiding the information such as steganography, cryptography and watermarking etc. But in digital world, watermarking is most commonly used for copyright protection of digital information data. Digital watermarking is the pattern of bits inserted into the multimedia files or hiding the digital information into the carrier signal that identifies the file's copyright information. It is also used for the banknote authentication purposes. There are many classifications of watermarking which are used for various purposes.

1) Visible and Invisible watermarking
2) Robust and Fragile watermarking
3) Asymmetric and Symmetric watermarking
4) Public and Private watermarking
5) Steganographic and Non-Steganographic watermarking

All above classifications have different applications where these are used for hiding or copyright protection. According to the working domains, watermarking techniques are classified in two domains: spatial and frequency domain watermarking which is described in Fig. 1.

Sometimes both domains are used in combination for better results [1, 2]. A watermarking system is divided into three different steps: embedding, attack and detection which is shown in Fig. 2.

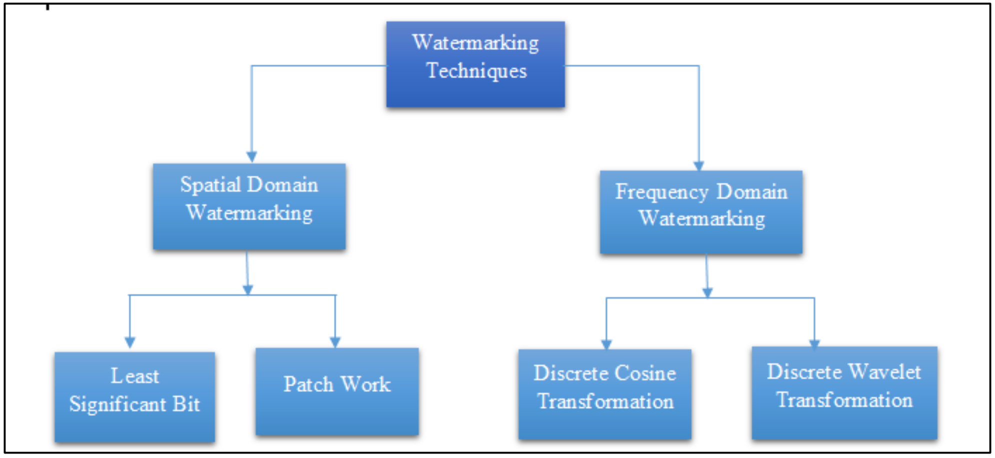

Watermarking Techniques
Spatial Domain Watermarking
Frequency Domain Watermarking
Least Significant Bit
Patch Work
Discrete Cosine Transformation
Discrete Wavelet Transformation

Fig. 1: Various Watermarking Techniques Used In Different Applications

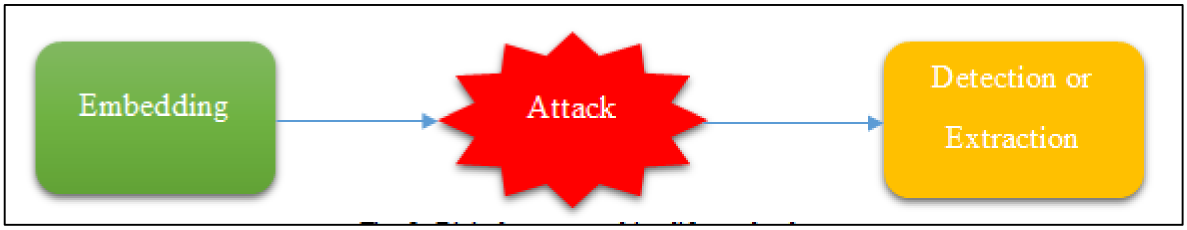


Fig. 2: Digital Watermarking Life Cycle Phase

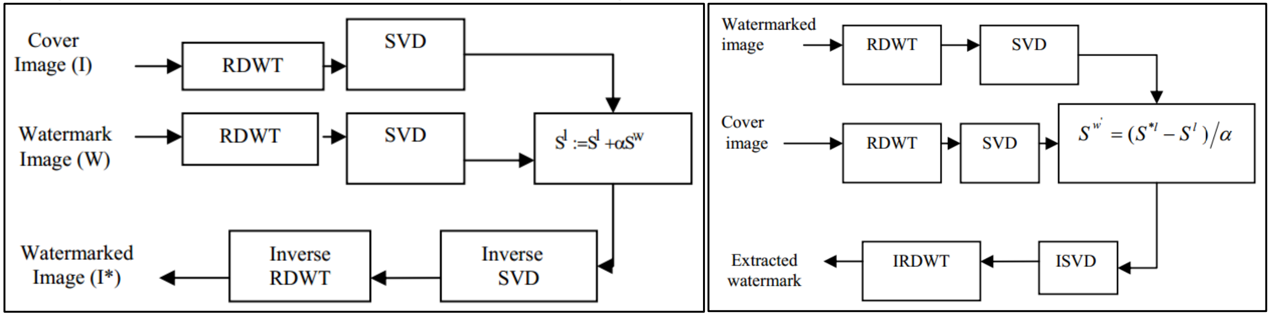
The information to be embedded in a signal is called a digital watermark, although in some contexts the phrase digital watermark means the difference between the cover signal and the watermarked signal. The signal where the watermark is to be embedded is called the host signal. In embedding, an algorithm accepts the host and the data to be embedded, and produces a watermarked signal. Then the watermarked digital signal is transmitted or stored, usually transmitted to another person. If this person makes a modification, this is called an attack. While the modification may not be malicious, the term attack arises from copyright protection application, where third parties may attempt to remove the digital watermark through modification. Detection (often called extraction) is an algorithm which is applied to the attacked signal to attempt to extract the watermark from it. In robust digital watermarking applications, the extraction algorithm should be able to produce the watermark correctly, even if the modifications were strong. In fragile digital watermarking, the extraction algorithm should fail if any change is made to the signal [3].

The type of information needed by the detector is an important criterion in classification of watermarking schemes:

1) Non-blind schemes require both the original image and the secret key(s) for watermark embedding.
2) Semi-blind schemes require the secret key(s) and the watermark itself.
3) Blind schemes require only the secret key(s) [4]

II. RDWT AND SVD

One of the most common techniques in transform domain watermarking is to modify the coefficients obtained from singular value decomposition (SVD) of the cover image. In SVD first algorithm [5], the authors after applying singular value decomposition to the cover image modify these coefficients by adding the watermark. When discrete wavelet transform (DWT) is combined with SVD technique, the watermarking algorithm outperforms the conventional DWT algorithm with respect to robustness against Gaussian noise, compression and cropping attacks [6, 7]. So, to overcome the shift variance drawback of DWT, redundant discrete wavelet transform (RDWT) is developed. The un-decimated discrete wavelet transform or sometimes called RDWT is used for watermarking process because it generated less distorted image when extracted. In RDWT, we modifies the filters at each level by up-sampling. It means RDWT contains the coefficients of DWT of shifted signal. When we combined RDWT with SVD process, then we can take advantages of both process in watermark embedding and extraction. Embedding and extraction process steps [8] are described in Fig. 3.



(a) (b)

Fig. 3: (A) RDWT-SVD Watermark Embedding (B) RDWT-SVD Watermark Extraction

III. DISCRETE COSINE TRANSFORM

The Discrete Cosine Transform (DCT) is used to transform a signal from the spatial domain into the frequency domain. The reverse process of transforming a signal from the frequency domain into the spatial domain is called the Inverse Discrete Cosine Transform (IDCT). A signal in the frequency domain contains the same information as that in the spatial domain. The order of values obtained by applying the DCT is coincidentally from lowest to highest frequency. The discrete cosine transform (DCT) represents an image as a sum of sinusoids of varying magnitudes and frequencies [9].

A. Watermark Embedding:

1) Watermark1 is taken. It is encrypted by using XOR operation. Encryption key E1 is used. We will get Encrypted E1 as output.
2) Encrypted E1 is now embedded in the watermark2. Key W1 is used and the image received in output is watermarked1.
3) Now watermarked watermark will be encrypted using XOR operation and key E2 is used. The output of this will be Encrypted 2.
4) Now the output received in step 3 will now be embedded in grey scale cover image. Key W2 is used. And the output received from this step will be final watermarked image.

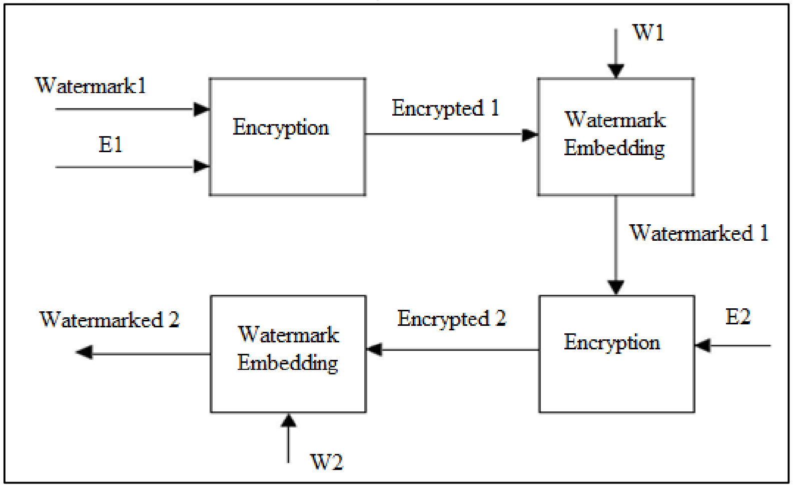


Fig. 4: Block Diagram Of The Watermark Embedding Algorithm

B. Watermark Extraction:

The watermark extracting algorithm of review paper is shown in Fig. 5.

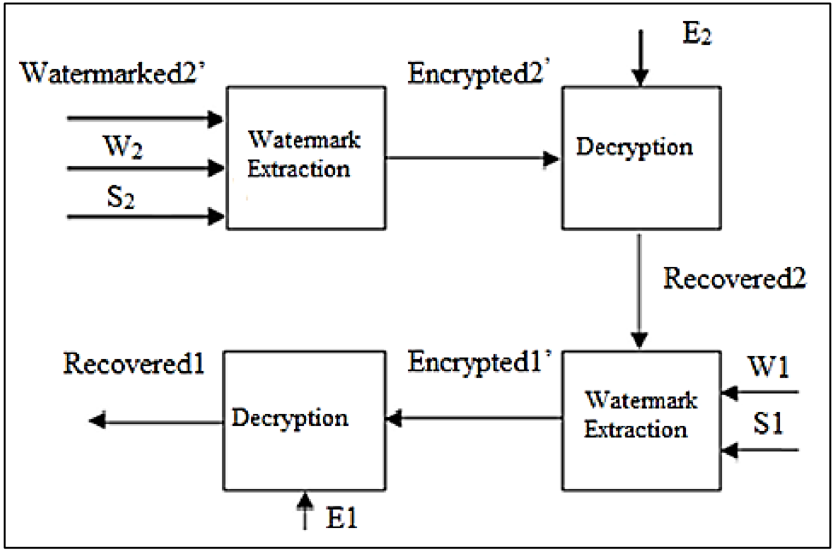


Fig. 5: Block Diagram of The Watermark Extracting Algorithm

1) Apply the proposed procedure to extract encrypted watermark2 from Watermarked2 using key W2. Say the recovered image is encrypted.
2) Decrypt Encrypted2' using XOR key with E2. Output of this step is called Recovered2.
3) Apply procedure to extract encrypted watermark1 from Recovered2 using Key W1. Recovered image is called Encrypted1'.
4) Decrypt Encrypted1' using XOR key with key E1. Output of this step is called Recovered1.

IV. EXPERIMENTAL RESULTS

In this paper, we used gray scale fruits image (512x512 pixels) as a cover image and flowers image as a watermark image of same size which is shown in Fig. 6. When watermarks are extracted, similarity of the watermarked and cover image can be defined by the PSNR (Peak Signal to Noise Ratio) criterion:

$$\mathrm{PSNR} = 10 * \log_{10}\left[\frac{\max((X(i,j))^2}{\mathrm{MSE}}\right] \tag{1}$$

And MSE (Mean Square Error) is defined as:

$$\mathrm{MSE} = \frac{1}{m * n}\sum_{i=1}^{m}\sum_{j=1}^{n}[X(i,j) - Y(i,j)]^2 \tag{2}$$

Where m and n are the dimensions of the images X and Y. PSNR is measured in db. Larger values of PSNR indicate better watermark concealment.

We compared the watermarked image with the original image and we got higher PSNR and lower MSE than previous work which is shown in Table I.

Table – 1
Comparison Of PSNR And MSE Of Previous And Proposed Work

	PSNR (dB)	*MSE (dB)*
RDWT-SVD [8]	*37.6298*	*0.0002*
Proposed DCT based Work	*39.2551*	*0.0001*

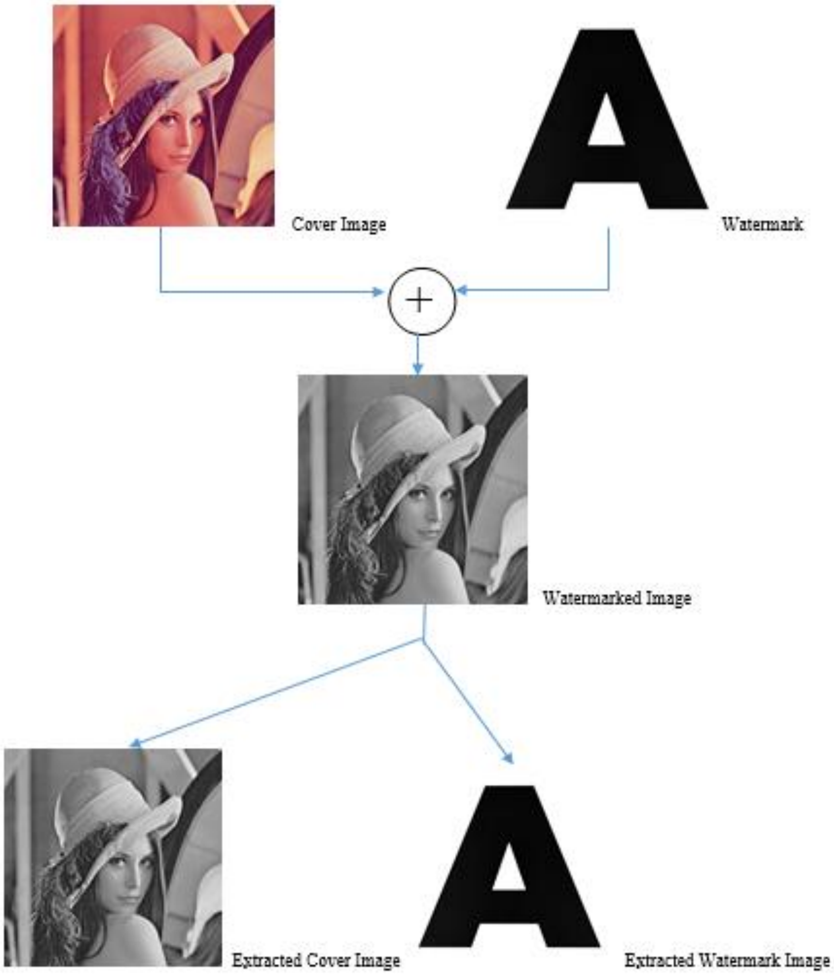


Fig. 6: Showing watermarking and extraction of cover and watermark image using DCT

V. CONCLUSION

We presented a watermarking method based on DCT to embed a watermark image which can be as large as the cover image. Inverse DCT provides high robustness against common attacks. High PSNR and lower MSE of watermarked image is another beneficial point of the algorithm as the result of DCT implementation. These results demonstrated that the proposed method is more robust to various attacks compared to previous DWT and RDWT-SVD based methods. It is known that frame expansion increases robustness with respect to additive noise. Another advantage of this method is the possibility to embed a large watermark in the cover image.

REFERENCES

[1] Frank Y. Shih and Scott Y.T. Wu, “Combinational image watermarking in the spatial and frequency domains,” Elsevier Science Ltd on behalf of Pattern Recognition Society, vol. 36, pp. 969 – 975, 2003.

[2] D. Asatryan, N. Asatryan, “Combined spatial and frequency domain watermarking,” Proceedings of the 7th International Conference on Computer Science and Information Technologies, pp. 323–326, 2009.

[3] https://en.wikipedia.org/wiki/Digital_watermarking

[4] A. Sverdlov, S. Dexter, A.M. Eskicioglu, “Robust DCT-SVD Domain Image Watermarking For Copyright Protection: Embedding Data In All Frequencies”, Proceedings of the 13th European Signal Processing Conference (EUSIPCO2005), Antalya, Turkey, September 2005.

[5] R. Liu, T. Tan, “An SVD-based watermarking scheme for protecting rightful ownership”, IEEE Transactions on Multimedia, vol. 4, pp. 121–128, 2002.

[6] L. Liang, S. Qi, “A new SVD-DWT composite watermarking”, Proceedings of IEEE International Conference on Signal Processing (ICSP) , 2006.

[7] V. Santhi, A. Thangavelu, “DWT-SVD combined full band robust watermarking technique for color images in YUV color space”, International Journal of Computer Theory and Engineering, vol. 1, no. 4, pp. 424-429, Oct. 2009.

[8] Samira Lagzian, Mohsen Soryani and Mahmood Fathy, “A new robust watermarking scheme based on RDWT-SVD,” International Journal of Intelligent Information Processing, Volume 2, Number 1, March 2011.

[9] Huang-Chi Chen, Yu-Wen Chang and Rey-Chue Hwang, “A Watermarking Technique based on the Frequency Domain,” Journal of Multimedia, vol. 7, no. 1, pp. 82-89, Feb. 2012.