International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

ELSEVIER
SSRN

IJIEMR Transactions, online available on 10th Dec 2019. Link :http://www.ijiemr.org/downloads.php?vol=Volume-08&issue=ISSUE-12

Title **A NOVEL COLOR IMAGE WATERMARKING SCHEME BASED ON DWT AND QR DECOMPOSITION**

Volume 08, Issue 12, Pages: 47-52.

Paper Authors

K.SAI KISHORE, M.AMARANATH REDDY
SIR C.V. RAMAN Institute of Technology & Science, AP, India

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

A NOVEL COLOR IMAGE WATERMARKING SCHEME BASED ON DWT AND QR DECOMPOSITION

K.SAI KISHORE[1], M.AMARANATH REDDY[2]
[1]PG Scholar, Dept of ECE, SIR C.V. RAMAN Institute of Technology & Science, AP, India
[2] Assistant Professor, Dept of ECE, SIR C.V. RAMAN Institute of Technology & Science, AP, India

Abstract: Image watermarking assumes critical part in applications like Copyright security and Confirmation. Strong watermarking is enter inquire about zone in these applications with a specific end goal to be impervious to most kinds of assaults. Notwithstanding Robustness, high intangibility, security, and expansive limit are other basic prerequisites in any watermarking plan. This paper shows another picture watermarking plan in view of the Discrete Wavelet Transform (DWT) and the Singular Value Decomposition (SVD). The dark scale picture watermark was installed straightforwardly in the particular estimations of the DWT sub-groups of the host picture. The plan accomplished a vast limit because of the repetition in the DWT space and in the meantime saved high subtlety because of SVD properties. Inserting the watermarking pixel's esteems with no alteration inside the wavelet coefficient of the host picture beats the security issue. Besides, the trial consequences of the proposed plot demonstrated an abnormal state of strength against the picture handling assaults.

Key words: Authentication; copyright security; heartiness; Image watermarking, Discrete Wavelet Transform, Particular Value Decomposition, Robustness, Imperceptibility

1. Introduction

Watermarking (information covering up) is the procedure of implanting information into a media component, for example, picture, sound or video for security purposes or copyright insurance. This implanted information can later be removed from, or recognized in the interactive media. A watermarking calculation comprises of an implanting calculation, and an extraction, or discovery calculation. The kind of data required by the indicator is an imperative foundation in characterization of watermarking plans:

· Non-daze plans require both the first picture and the mystery key(s) for watermark inserting.

· Semi-daze plans require the mystery key(s) and the watermark itself.

· Blind plans require just the mystery key(s).

Watermarking can be performed in the spatial or change space. Spatial space strategies are less complex yet are not as strong as change area strategies against different assaults. A standout amongst the most normal procedures in change area watermarking is to change the coefficients got from particular esteem deterioration (SVD) of the cover picture. The SVD based watermarking calculation was first displayed by Liu et al . In this calculation, the creators subsequent to applying solitary esteem disintegration to the cover picture adjust these coefficients by including the watermark. They apply SVD change again on the resultant grid for finding the altered particular values. These solitary esteems were joined with the known part to get the watermarked picture. In another comparable work, Chandra et al., insert particular estimations of the watermark in the particular estimations of whole host picture. The most vital disadvantage of SVD-based calculations is quality corruption of the watermarked picture. Moreover, the separated watermark isn't sufficiently vigorous against basic assaults in SVD-based calculations. Therefore specialists, more often than not join SVD with other calculations, for example, DCT and DWT. In [2], creators joined DWT with SVD method. In that paper, subsequent to decaying the host picture into four sub-groups, SVD is connected to each sub-band and particular estimations of the watermark is inserted into the sub-groups. In [6], DWT is joined with SVD system to shroud solitary estimations of watermark in high recurrence band (HH) of a picture. At the point when DWT is joined with SVD method, the watermarking calculation beats the customary DWT calculation concerning strength against Gaussian commotion, pressure and trimming assaults [7]. In our work, SVD is inserted in LL band of the cover picture and found that the outcomes are superior to prior one.

2. Previous Methods

In prior days, for the transmission of information with high security there exist different techniques. Among them cryptography is one of the technique which is utilized to transmit information as mystery written work. Human being from ages had two inalienable needs: (a) to impart and share data and (b) to convey specifically. These two needs gave rise to the specialty of coding the messages such that just the planned individuals could approach the data. Unapproved individuals couldn't extricate any data, regardless of whether the mixed messages fell in their grasp.

The art and science of concealing the messages to introduce secrecy in information security is recognized as cryptography. The word 'cryptography' was coined by combining two Greek words, 'Krypto' meaning hidden and 'graphene' meaning writing. In the process of cryptography, the main aim is that to transmit the original data in the form of secret codes which may not visible to unauthorized person. The information can be hidden by using these methods:

i. By writing the original data in the form of special characters.

ii. By shifting and jumbling the letters of the data.

iii. By writing the original data in the form of decimal code or gray code etc.

In the process of cryptography, at the transmitting side the original data is encrypted in the form of code as we mentioned above. The encrypted code is transmitted through the channel and it is decrypted at the receiving side. The key should be available at both the transmitter and the receiver side. There may be a chance that an unauthorized person may access our data by decoding our encrypted data. To overcome the disadvantage of cryptography, another method used is Steganography. Steganography is similar but adds another dimension to Cryptography. In this method, people not only want to protect the secrecy of an information by concealing it, but they also want to make sure any unauthorized person gets no evidence that the information even exists. For example, invisible watermarking. In Steganography, an unintended recipient or an intruder is unaware of the fact that observed data contains hidden information. In cryptography, an intruder is normally aware that data is being communicated, because they can see the coded/scrambled message. Steganography is the art and science of invisible communication. This is accomplished through hiding information in other information, thus hiding the existence of the communicated information. The word steganography is derived from the Greek

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

words "stegos" meaning "cover" and "grafia" meaning "writing" defining it as "covered writing". In image steganography the information is hidden exclusively in images. Steganography differs from cryptography in the sense that where cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret . Steganography and cryptography are both ways to protect information from unwanted parties but neither technology alone is perfect and can be compromised. Once the presence of hidden information is revealed or even suspected, the purpose of Steganography is partly defeated. The strength of Steganography can thus be amplified by combining it with cryptography. In the process of Steganography, cover image is used to hide the watermark image and it is transmitted over the channel. At the receiving side, the watermark is extracted by leaving the cover image. In this process some details of watermark image is lost as we are not considering cover image. To overcome the disadvantage of Steganography we go for watermarking technique. DWT AND SVD

A. DWT

Wavelets are special functions which, in a form analogous to sines and cosines in Fourier analysis, are used as basal functions for representing signals [7]. For 2-D images applying DWT corresponds to processing the image by 2-D filters in each dimension. The filters divide the input image into four non-overlapping multi-resolution sub-bands LL1, LH1, HL1 and HH1. The sub-band LL1 represents the coarse-scale DWT coefficients while the sub-bands LH1, HL1 and HH1 represent the fine-scale of DWT coefficients. According to the character of HVS, human eyes are sensitive to the change of smooth district of image, but not sensitive to the tiny change of edge, profile and streak. Embedding the watermark in the higher level sub bands increases the robustness of the watermark. However, the image visual fidelity may be lost, which can be measured by PSNR. With the DWT, the edges and texture can be easily identified in the high frequency band .Therefore it's hard to conscious that putting the watermarking signal into the big amplitude coefficient of high-frequency band of the image DWT transformed. Then it can carry more watermark signal and has good concealing effect. Whenever an image is subjected to dwt transform the details of watermark image is observed on the cover image. So that any person viewing at the channel can have information that something is there behind the cover image.

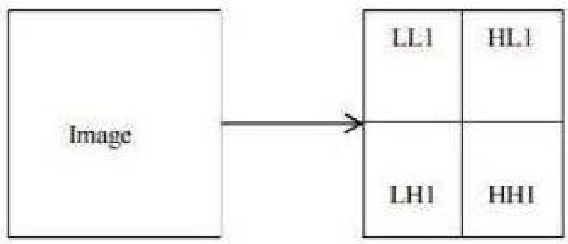

Fig-1: Single Level DWT

Due to its excellent spatio-frequency localization properties, the DWT is very suitable to identify the areas in the host image where a watermark can be embedded effectively. In particular, this property allows the exploitation of the masking effect of the human visual system such that if a DWT coefficient is modified, only the region corresponding to that coefficient will be modified. In general most of the image energy is concentrated at the lower frequency sub-bands LLx and therefore embedding watermarks in these sub-bands may degrade the image significantly. Embedding in the low frequency subbands, however, could increase robustness significantly. On the other hand, the high frequency sub-bands HHx include the edges and textures of the image and the human eye is not generally sensitive

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

to changes in such sub-bands. This allows the watermark to be embedded without being perceived by the human eye. The compromise adopted by many DWTbased watermarking algorithm, is to embed the watermark in the middle frequency sub-bands LHx and HLx where acceptable performance of imperceptibility and robustness could be achieved.to overcome the disadvantage of dwt we are going for the combination of dwt-svd domain.

B. SVD

SVD is an effective numerical analysis tool used to analyze matrices. In SVD transformation, a matrix can be decomposed into three matrices that are of the same size as the original matrix. From the view point of linear algebra, an image is an array of nonnegative scalar entries that can be regarded as a matrix. The singular value decomposition of a matrix is a factorization of the matrix into a product of three matrices. Given an m×n matrix A, where m ≥ n, the SVD of A is defined as $A = U\Sigma V^T$ where U is an m×n column-orthogonal matrix whose columns are referred to as left singular vectors; Σ =diag (σ1, σ2, . . . , σn) is an n×n diagonal matrix whose diagonal elements are nonnegative singular values arranged in descending order; V is an n×n orthogonal matrix whose columns are referred to as right singular vectors. SVD efficiently represents intrinsic algebraic properties of an image, where singular values correspond to brightness of the image and singular vectors reflect geometry characteristics of the image. Since slight variations of singular values of an image may not affect the visual perception, watermark embedding through slight variations of singular values in the segmented image has been introduced as a choice for robust watermarking .

3. Proposed DWT-SVD Based Watermarking

A. Watermark Embedding

The proposed watermark embedding algorithm is shown in Figure 2.

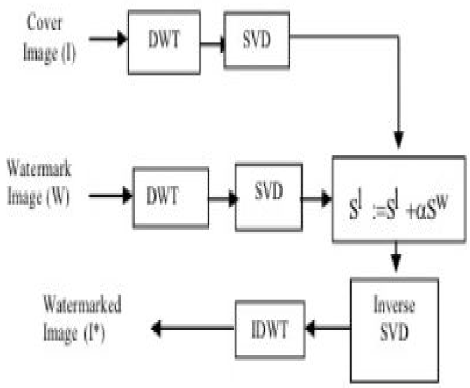

Fig-2: Block Diagram of the proposed watermark Embedding Algorithm

The steps of watermark embedding algorithm are as follows:

1. Apply DWT to the cover image to decompose it into LL, HL, LH, and HH subbands.

2. Apply SVD to the low frequency subband LL of the cover image:

$$I^I = U^I S^I V^I$$

3. Apply DWT to the visual watermark.

4. Apply SVD to the low frequency subband of watermark:

$$W = U^W S^W V^W$$

5. Modify the singular values of the cover image with the singular values of watermark image

$$S^{*I} = S^I + \alpha S^W$$

where is scaling factor, SI and Sw are the diagonal matrices of singular values of the cover and watermark images, respectively.

6. Apply inverse SVD on the transformed cover image with modified singular values

$$I^{*I} = U^I S^{*I} V^I.$$

7. Apply inverse DWT using the modified coefficients of the low frequency bands to obtain the watermarked image.

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

1. **Flow chart for the above Algorithm**

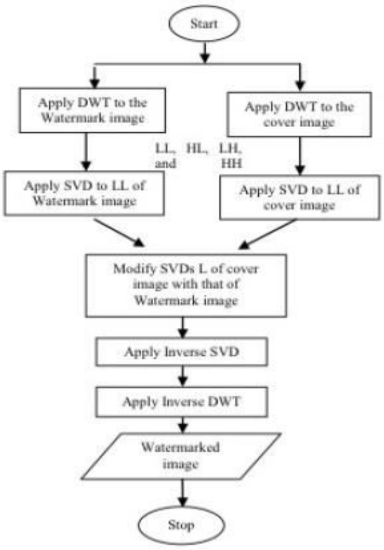

Fig-3: Flow Chart of Watermark Embedding

B. Watermark Extraction

The proposed watermark extracting algorithm is shown in Figure 4.

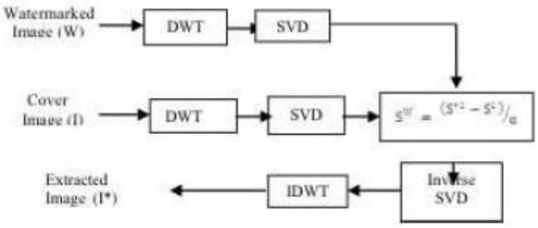

Fig-4: Block diagram of the proposed Watermark Embedding Algorithm

The steps of watermark extracting algorithm are as follows and the flow chart will as same as shown for watermark embedding:

1. Using DWT, decompose the watermarked image I* into 4 sub bands: HH, HL, LH and LL.

2. Apply SVD to low frequency sub band LL: I∗ = U∗ S∗ V∗

3. Extract the singular values from low frequency sub band of watermarked and cover image S_ = (S∗ −S) ÷ α where S contains the singular of the cover image.

4. Apply inverse SVD to obtain low frequency coefficients of the transformed watermark image.

5. Apply inverse DWT using the coefficients of the low frequency sub-band to obtain the watermark image.

Results

In this study, we used gray scale image as our host image of size252 × 252, and the watermark image is of same size. In our experiments, we used the scaling factor □ □ 0.1. below figure shows cover image, watermark, watermarked image and the extracted watermark.

FIG: Original water mark image

Fig: duplicate images

Fig:water marking image

When watermarks are extracted, similarity of the watermarked and cover image can be defined by the PSNR (Peak Signal to Noise Ratio) criterion:

$$PSNR = 10log_{10}(255^2 \div MSE)$$

where MSE (Mean Square Error) is defined as:

$$MSE = (1 \div M \times N)\sum_{x=1}^{M}\sum_{y=1}^{N}(P(x,y) - P'(x,y))^2$$

where m and n are the dimensions of the images X and Y. PSNR is measured in Db The PSNR value obtained in DWT-SVD domain is higher than that of DWT.

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

4. Conclusion

We introduced another watermarking technique in view of DWT-SVD to insert a watermark picture which can be as huge as the cover picture. Changing particular estimations of the cover picture in DWT space gives high strength against regular assaults. High PSNR also, connection coefficient of watermarked picture is another useful purpose of the calculation as the outcome of DWT usage. Another preferred standpoint of this technique is the likelihood to implant a vast watermark in the cover picture. This work can be additionally broadened with variety in DWT like RDWT.

References

[1] D. Kundur, D. Hatzinakos, Towards robust logo watermarking using multiresolution image fusion, IEEE Transcations on Multimedia 6 (2004) 185–197.

[2] Q. Li, C. Yuan, Y.Z. Zong, Adaptive DWT-SVD domain image watermarking using human visual model, ICACT-2007, 2001, pp. 1947–1951.

[3] D.S. Chandra, Digital image watermarking using singular value decomposition, Proceedings of the 45th Midwest Symposiumon Circuits and Systems (MWSCAS'02), vol. 3, 2002, pp. 264–267.

[4] Liu, R. and Tan, T. (2002) An SVD-based watermarking scheme for protecting rightful ownership, IEEE Transactions on Multimedia, Vol.4, No.1, Pp. 121-128.

[5] 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.

[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 mJournal of Computer Theory and Engineering, vol. 1, no. 4, pp. 424-429.

[8] C.C. Chang, C.C. Lin, Y.S. Hu, “An SVD oriented watermark embedding scheme with high qualities for the restored images”, International Journal of Innovative Computing, Information and Control (ICIC), vol. 3, no. 3, pp. 609-620.

[9] P. B. Paul, and X. Ma, “Image Adaptive Watermarking Using Wavelet Domain Singular Value Decomposition”, IEEE Transactions on Circuits and Systems for Video Technology, vol.15, no.1, pp.96-102.