Namrata R. Deshmukh *et al*, International Journal of Computer Science and Mobile Applications,
Vol.3 Issue. 11, November- 2015, pg. 1-4 **ISSN: 2321-8363**

Digital Image Watermarking- Review

Namrata R. Deshmukh[1], Dr. M. H. Kondekar[2]

[1]Student, of TYMCA (A),MIT (E) College, Aurangabad (M.S). namratadeshmukh114@gmail.com

[2]Asst. Prof.MCA Dept. MIT (E) College, Aurangabad (M.S). mhkondekar@gmail.com

Abstract

Today's world is a digital world. In every field there is varied use of digital form information. This information handled on Internet and multimedia network system in digital form. The copying of digital content without quality loss is not so difficult. Understanding the need of copyright, protection and authentication, there is great need of prohibiting illegal access mechanism which gave rise to the powerful solution named as "watermarking". It makes possible to identify owner, author or consumer of a document as well as broadcast monitoring.

Continuation

The fingerprinting resulted watermarking as one of the most widely used security providing technique in the digital world. This paper aims gives a deep insight on digital image watermarking with certain applications.

Keywords: Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT), frequency-domain Watermarking

Introduction:

Digital image processing is a rapidly developing area with various raising applications in computer science and engineering. [1] It is the act of hiding the message related to a digital signal i.e. image, song, video within signal itself. A digital watermark is an invisible signature embedded inside an image to show authenticity and ownership. The specialty of watermark is that it remains intact to cover work even if it is copied. So, to prove the ownership or copyright data watermark is extracted and tested.

Even if the watermarked image is extracted then also it is very difficult to prove the ownership and copyrights of an image to recover watermark back from watermarked image. [2] So our main idea is to find such regions known as patches, which are very stable and resistant to attack. For that we can use following types

a) DCT (Discrete Cosine Transformation)
b) DWT (Discrete Wavelet Transformation)
c) DFT (Discrete Fourier transformation)

a) DCT:

1) A Digital watermarking has been proposed for copyright, protection and authentication of multimedia data in a network environment.
2) Since it makes possible to identify authorized consumer of document.
3) For that one new watermarking method is used which add a code to digital image.
4) This method operates in a frequency domain embedding a pseudo random sequence of real numbers in a selected set of DCT coefficient.
5) To ensure watermarking invisibility, watermarking costing is performed by exploiting the masking characteristics of the human visual system.
6) The embedded sequence is extracted without making any changes to the original image.
7) So, that proposed technique represents major improvement between watermarking and original image. [3]

Major potential of DCT:

1) Semantically meaningful watermark pattern.
2) Good perceptual invisibility.
3) Acceptable Robustness.
4) Various user selected options.
5) Reasonable Execution Time.
6) Fast and suitable for robustness against JPEG compression. [3],[4]

Problem area Of DCT:

1) Block effect.
2) Effect of picture cropping.
3) One of the main problems of DCT is blocking effect.
e.g. In DCT images are broken into blocks 8*8 or 16*16 or bigger. The problem with these blocks is that when the image is reduced to higher compression ratios these blocks becomes visible. This has been termed as blocking effect.
4) Then watermarking not revealed it means non watermarked image.

b) Discrete Wavelet Transform:

1) Wavelet transform is time domain localized analysis method with the windows size fixed and forms convertible.
2) There is quite good time differentiated rate in high frequency part of signal DWT transformed. Also there is quite good frequency differentiated rate in its low frequency part.
3) The basic idea of DWT in image process is to multi-differentiated decompose the image into sub image of different spatial domain and independent frequent distinct.
4) Then transform the coefficient of sub image. After the original image has been DWT transformed.
5) It decompose into 4 frequency district and 3 high frequency districts (LH.HL,HH)[4]

Major potential of DWT:

1) No need to divide the input coding into non overlapping 2-D blocks. It has higher compression ratios avoid blocking artifacts.
2) Allow good localization both in time spatial frequency domain.
3) Transformation of whole image introduces inherent scaling.
4) Better identification of which data is relevant to human perception higher compression ratio.
5) Higher flexibility: Wavelet function can be freely chosen.[3],[4]

Problem area Of DWT:

1) The cost of computing DWT as compared to DCT may be higher.
2) The use of larger DWT basis functions or wavelet filter produces blurring and ringing noise near edge regions in an images or video frames.
3) Longer compression time.

c) DFT:

1) The DFT approach has one advantage in comparison with spatial domain method. First, it is translation invariant and rotation resistant, which translates to strong robustness to geometric attacks.
2) On the other hand, according to fast Fourier transform (FFT) methods introduce round-off errors, which can lead to loss of quality and errors in watermark extraction. It states that this disadvantage is much more important for hidden communication than for watermarking.
2) Because of its resistance to geometric attacks and the distribution of energy, FFT watermarking methods are developed to create robust watermarking schemes resistant to the degradation attacks of the watermarked image in the transmission
Channel such as print-scan process (PS process).
3) The robustness of the watermarking method to the print-scan process would enable the use of the method in the protection of the printed images, thus enabling the use of digital watermarks in the protection of analog media.
4) However, the PS process is very difficult to model. It engenders a number of linear (translation, rotation, and scaling) and nonlinear attacks (pixel distortions and noise addition).
5) These attacks are not only user and equipment dependent, but also time-variant.
The common property of these methods is the implementation of the binary vector of length l, which is acquired by a pseudorandom generator.
6) This vector is embedded in the magnitude of the Fourier transform of a cover work, as a circle of radius r around the center of the cover work. To control the strength of the implementation, the implementation factor α is used.[5]

Application:

In this section we discuss some of the scenarios where watermarking is being already used as well as other potential applications.

1) Authentication

In this section we are using cryptographic security. There are two significant benefits that arise from using watermarking: first, as in the previous case, the signature becomes embedded in the message, second, it is possible to create soft authentication algorithms.
(an example is image compression with different levels)[6]

2) Copy and Playback Control

The message taken by the watermark may also contain information about copy and display permissions. Then a secure information can be added in copy or playback control which is useful to extract automatically this permission and block further processing if required.

3) Signaling

The constraints are helpful when transmitting signaling information in the hidden channel. The advantage of this channel is that no bandwidth increase is required.

4) Labeling

The hidden message could also contain labels (example to annotate images or audio). The annotation may also contain a separate file, but with watermarking its result become more difficult to destroy this label, since it becomes closely tied to the object.

5) Fingerprinting

It allows acquisition devices (such as video cameras, audio recorders, etc) to insert information about the specific device (e.g., an ID number) and date of creation.

6) Additive Noise

In watermark there may be a transmission error while transferring data from analog to digital and digital to analog. However, an attacker may introduce noise [7]. This will typically force to increase the threshold at which the correlation detector works.

7) Filtering

Low-pass filtering, for instance, does not introduce considerable degradation in watermarked images or audio, but can dramatically affect the performance, since spread spectrum-like watermarks have a non negligible high frequency spectral contents.

8) Cropping

In many cases the attacker is interested only in a small portion of the watermarked object, such as certain parts of picture or frames of a video. In order to survive, the watermark is necessary where this attack takes place.

9) Compression

This is an unintentional attack which occur generally in multimedia applications but practically all the audio, video and images that are currently being distributed via Internet have been compressed.

10) Rotation and Scaling

This is used to recover rotation angle and scale factor of a distorted image. [8] The embedded watermark and the locally generated version do not share the same spatial pattern anymore.

11) Statistical Averaging

It is possible to improve the estimate by simple averaging. This is a good reason for masks to create the watermark.

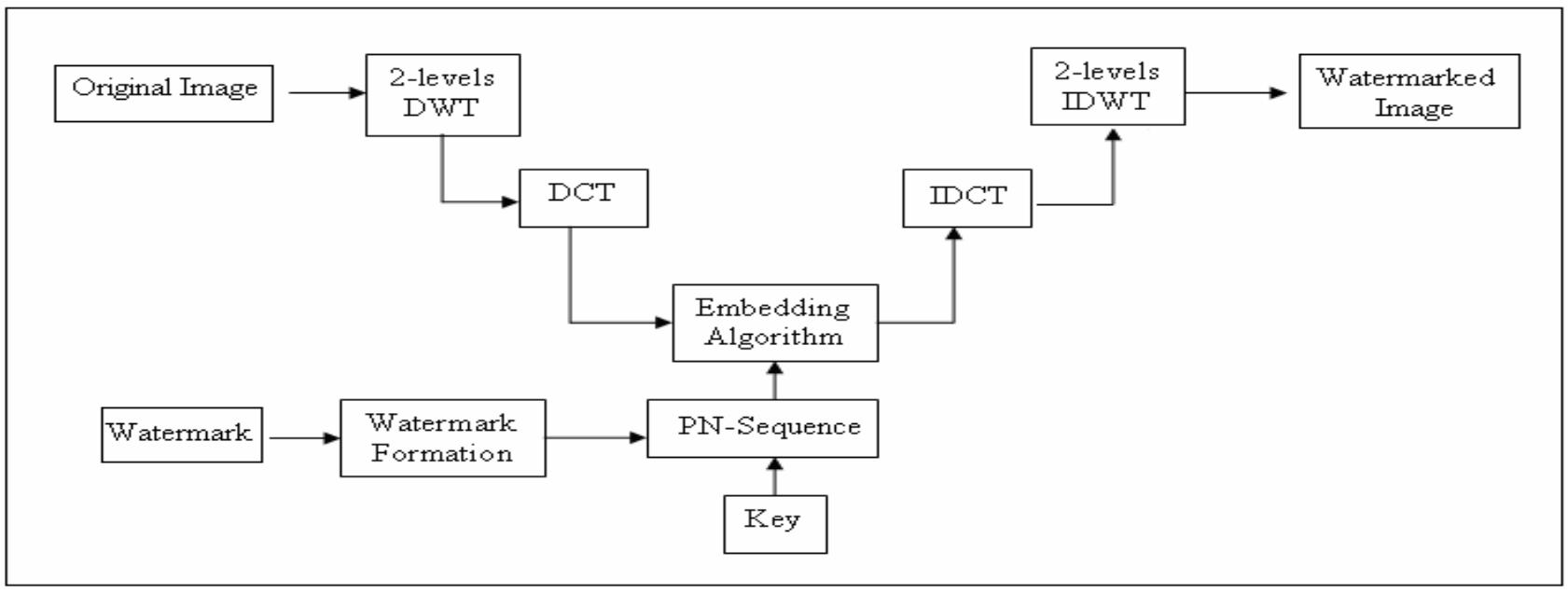
12) Broadcasting Monitoring

To embed the watermark in commercial advertisement, then there must be an automated monitoring system which can verify whether advertisements are broadcasted or not[9].

13) Security

Security is necessary while transferring the data from sender to receiver by using encryption and decryption technique.

The combined DWT-DCT algorithm:

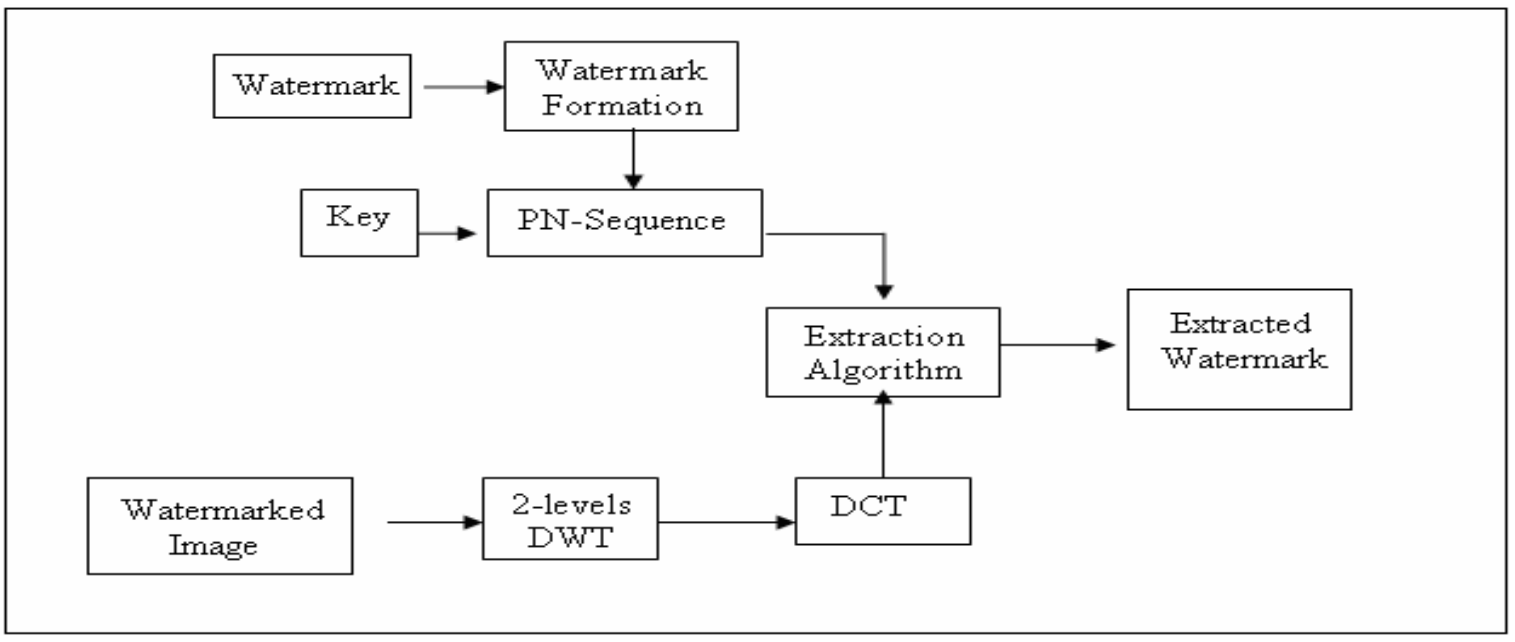


A) The DCT and DWT Watermark embedding Procedure

step1: Apply DWT to decompose the cover host image into four non-overlapping
Multi-resolution sub-bands. LL1, HL1, LH1, and HH1.
step2: Apply DWT again to sub-bands HL1 to get four sub-bands and choose the HL2 sub-bands as shown in fig (a) or DWT to sub-bands HH1 to get four smaller sub-bands and choose the HH2 sub-bands as shown in fig (b).
step3: Divide the sub-bands HL2 (or HH2) into 4*4 blocks.
Step4: Apply DCT to each block in the chosen sub-bands (HL2 or HH2)
Step5: Re-formulate the gray-scale watermark image into a vector of zeros and Ones.
Step6: Generated two uncorrelated pseudo-random sequences. One sequence is used to embed watermark bit 0.
(PN-0) and other sequence is used to embed the watermark bit 1 (PN-1). Number of elements in each of the two Pseudo-random sequences must be equal to the number of mid-band element of DCT-transformed DWT sub-bands.
Step7: Embed the two pseudo-random sequences, PN-0 and PN-1 with a gain factor α, in the DCT transformed 4*4 block of the selected DWT sub-bands of the host image.
Embedding is not applied to all the coefficient of the DCT blocks but only to the mid band DCT coefficients. If we denote x as the matrix of the mid band coefficient of the DCT transformed block, then embedding is done as follows:

If the watermark bit is 0 then1
$x' = x + \alpha * PN\text{-}0$
Otherwise,
If the watermark bit is 1 then,
$x' = x + \alpha * PN\text{-}1$
step8: Apply inverse DCT(IDCT) to each block after its mid-band coefficient have been modified to embed the watermark bits as described in the previous step.
Step9: Apply the inverse DWT(IDWT) on the DWT transformed image, including the modified sub-bands, to produce the watermarked host image.

B) The DCT and DWT Watermark extraction Procedure:



step1: Apply DWT to decompose the watermarked Image into four non overlapping multi resolution sub-bands: LL1, HH,LH1 and HL1.
step2: Apply DWT to HL1 to get four smaller sub-bands and choose the sub-bands HL2 as shown in fig (a) or apply DWT to HH1 sub-bands and choose HH2 sub-bands as shown in fig 2(b)
step3: Divide the sub-band HL2 (or HH2 into 4*4 blocks)
step4: Apply DCT to each block in the chosen sub-bands (HL2 or HH2) and extract the mid band coefficients of each DCT transformed block.
step5: Regenerate the two pseudo-random sequences(PN-0 and PN-1) using the same speed used in the watermark embedding procedure.
step6: For each block in the sub-bands HL2 (or HH2) calculate the correlation between mid-band coefficient and the two generate pseudo-random sequences (PN-0 and PN-1). If the correlation with the PN-0 was higher than the correlation with PN-1 then the extracted watermark bit is considered 0, otherwise the extracted watermark is considered 1.
step7: Reconstruct the watermark using the extracted watermark bits and compute the similarity between the original and the extracted watermark.[9],[10],[11]

Conclusion:

In this paper, we described a combined DWT-DCT digital image watermarking algorithm. The watermark is added in select coefficients with significant image energy in the discrete wavelet transform domain in order to ensure non- erasability of the watermark.
Watermarking was done by embedding the watermark in the first and second level DWT sub-bands of the host image, followed by the application of DCT on the selected DWT sub-bands.

The simulation results suggest that this watermarking system can keep the image quality as well as it is robust against many common image processing operations of filer, sharp enhancing, adding salt noise, image compression, image segmentation and so on. This algorithm has strong capability of embedding single and anti-attack.

References:

[1] Preeti Parashar and Rajeev Kumar Singh *"A Survey: Digital Image Watermarking Techniques "* International Journal of Signal Processing, Image Processing and Pattern Recognition Vol. 7, No. 6 (2014), pp. 111-124 http://dx.doi.org/10.14257/ijsip.2014.7.6.10 ISSN: 2005-4254 IJSIP Copyright ⓒ2014 SERSC
[2] James Greenfield "Digital watermarking" www.cs.uct.ac.za/courses/CS400W/NIS/papers99/jgreenfi/watermarking.htm
[3] SarajuP.Mohanty, "Digital Watermarking: A Tutorial Review", http://www.csee.usf.edu/~smohanty/research/Reports/WMSurvey1999Mohant y.p-df
[4] Bhupendra Ram, Digital Image Watermarking Technique using Discrete Wavelet Transform and Discrete Cosine Transform, Issue4, April 2013 ISSN 2278-7763.
[5] Ante Poljicak, Lidija Mandic, Darko Agic**,** Discrete Fourier transform–based watermarking method with an optimal implementation radius, Journal of Electronic Imaging 20(3), 033008 (Jul–Sep 2011)
[6] Ruby Shukla, Manish, Prof. A.K. Arora *"Image Watermarking Analysis: Using Discrete Cosine Transform and LSB Substitution"* ISSN: 2277 – 9043 International Journal of Advanced Research in Computer Science and Electronics Engineering Volume 1, Issue 5, July 2012
[7] I.J.Cox, M.L. Miller and A.L. Mckellips,*" Watermarking as communications with side information"*, Proc. of IEEE, vol 87, no. 7, pp 1127-1141, 1999.
[8] F. Bartolini, M. Barni, V. Cappellini, and A. Piva*, "Mask building for perceptually hiding frequency embedded watermarks,"* in Proc. 5th IEEE Int.Conf. Image Processing ICIP'98, vol. I, Chicago, IL, Oct. 4-7, 1998, pp.450-454.
[9] *"Watermarking digital image and video data"* IEEE SIGNAL PROCESSING MAGAZINE 1053-5888/00/$10.00©2000IEEE
[10] Ali Al-Haj *"Combined DWT-DCT Digital Image Watermarking"*, Journal of Computer Science 3 (9): 740-746, 2007 ISSN 1549-3636 © 2007 Science Publications
[11] Mei Jianshen1, Li Sukang1 and Tan Xiaomei *"A Digital Watermarking Algorithm Based On DCT and DWT"* ISBN 978-952-5726-00-8 (Print), 978-952-5726-01-5 (CD-ROM) Proceedings of the 2009 International Symposium on Web Information Systems and Applications (WISA'09) Nanchang, P. R. China, May 22-24, 2009, pp. 104-107

