ISSN: 0976-9102(ONLINE)
DOI: 10.21917/ijivp.2015.0165

A BLIND WATERMARKING SCHEME FOR TAMPER DETECTION IN DIGITAL IMAGES

Jobin Abraham
Mahatma Gandhi University, Kottayam, India
E-mail: jnabpc@gmail.com

Abstract

The paper proposes a method for tamper proofing digital images using the technique of digital watermarking. Many a times the published images are subject to tampering to an extent that the facts conveyed in the original image are distorted. The mechanism presented here describes a method for detecting the regions in image that were subject to illegal modifications. The method also can detect the portions in image that were exposed to vector quantization kind of attacks. Two essential requirements of watermarking process for tamper detection, blind and robust, stands fulfilled by the proposed algorithm. The watermarking technique presents an algorithm that employs a frequency domain embedding process using DWT.

Keywords:

Digital Image Watermarking, Embedding, Extraction, DWT, Tamper Proofing

1. INTRODUCTION

Watermarking mechanisms are widely used for copyright protection of digital documents. Digital images are imperceptibly marked using a unique logo of the owner for identification [1],[2]. The use of watermarking techniques for copyright protection of video is presented in [3]-[4]. In addition to copyright protection of digital multimedia resources watermarking can deliver multifarious purposes as fingerprinting, tamper proofing and content labeling [5]. Rajneeshkaur Bedi et al. [6] proposes a method for data authentication of relational databases. Tamper detection makes possible to estimate for the portions in image that are illegally edited or tampered. This has greater relevance as the digital images published or made available for public interest via Internet are subject to unauthorized editing.

P. Meenakshi Devi et al. [7] proposes an extremely complex method using integer Haar wavelet transform. They use a logo binary image as watermark. Size of watermark is to be matched to one-by fourth the size of base image. The base image is decomposed using IWT and the coefficients from the resulting four sub-bands in similar location are selected to form a 2 × 2 coefficient block. All coefficients are so grouped to form a rearranged image (RI). Then to embed the watermark logo bit, traditional odd-even kind of mapping is adopted. If the sum of the four members in 2 × 2 coefficient block add up to an even number, it is then considered to represent a bit 1. And if the sum is an odd number it then represents a 0. Sum of all sub-block are so adjusted to represent the bit to be embedded. After embedding all watermark bits, inverse permutation is performed that rearranges the coefficients into respective frequency sub-bands LL, HL, LH and LL. After these two stages of operations inverse IWT restores the watermarked original image. The two shortcoming of the method are weak robustness to attack and failure in detection of tampering when blocks are swapped internally within the image area. The first limitation is majorly due to fallibility inherent with odd-even modulation methods, as even a minor variation in intensity value can upset the originally encoded values. The second side effect originates from the fact that the portions are marked using a uniform watermark for the entire image regions thus leaving no room for correctly determining the original position whenever the regions are exchanged without altering the values.

In [8] the recovery of a tampered block in a digital image is made possible by hiding that block information in another block which is determined using a one dimensional transform. In the preprocessing stage for watermarking the image is divided into non-overlapping blocks. Then the intensity features of one block is then embedded in the next block and so done for all other blocks in the image. A spatial domain based method is proposed, that hides the intensity value of a block in two LSB bits of pixels in another block. Though limited recovery is possible the method exhibits several shortcomings. Mainly, two LSB bits of all pixels are set to zero for the purpose of hiding recovery information. This leads to substantial loss in finer details. Another shortfall is that if the blocks that are hiding recovery information are also tampered the recovery of block becomes practically impossible. For instance, block A details in B, block B details in C and details of C hidden in block A makes the recovery of tampered block A cumbersome as all the allied blocks are equally affected.

The proposed is a method using DWT. DWT is a preferred choice in several papers as DWT decomposes the image into four non-overlapping multi-resolution sub-bands [9]-[12]. This allows low frequency part to be left unaffected as most of the energy is concentrated and utilize remaining sub-bands to embed the watermark bits.

The remaining sections are organized as follows. Section 2 describes the proposed algorithm. Section 3 is the testing of the algorithm and the results obtained there in. The last section gives the summary of the method and the findings.

2. THE WATERMARKING METHOD

2.1 FEATURES OF THE SUGGESTED METHOD

Two essential requirements of watermarking process for tamper detection are the method must be blind and robust. The proposed method is blind as during the stage of watermark detection the original image is not required.

Hidden watermark bits embedded in most cases are extremely difficult to decode correctly as even a minor variation are critical. Hence here redundant watermarking is enforced to ensure error free bit extraction.

Then as the last stage of embedding process measures are adopted to improve the overall robustness. The difference in coefficient values employed to hide the watermark information are subject to a verification process that ensure that a minimal difference exits between them, otherwise the forward and inverse transform operations can erode the hidden markings.

2.2 THE PROPOSED TECHNIQUE

The proposed method uses DWT to transform the spatial intensity values in to frequency domain coefficients. The block diagram of the embedding process is shown in Fig.1. The host image is decomposed into non-overlapping sub-blocks of size 8 × 8 or 16 × 16. Discrete wavelet transform operation in applied to each sub-block and middle frequency bands are used for embedding the watermark bit.

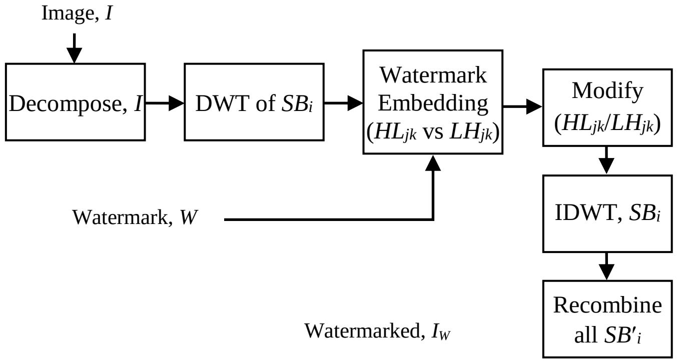

Fig.1. Block Diagram of Watermark Embedding

Two frequency sub-bands HL and LH are used for watermark embedding. Coefficients are then adjusted to represent the watermark bits by comparing them against the watermark bit to be attached. The algorithm spreads embedding over the entire area by dividing the base image into non-overlapping blocks. The watermark used is the dynamically generated sequence number that corresponds to the block mostly by the order they are considered. The final watermark is then generated by substituting each digit with its four bit binary equivalent. Hence if a four digit number is used, a sixteen bit binary pattern meant for a sub-block results. This watermark is redundantly embedded so as to enhance the chances for correctly decoding the embedded bits.

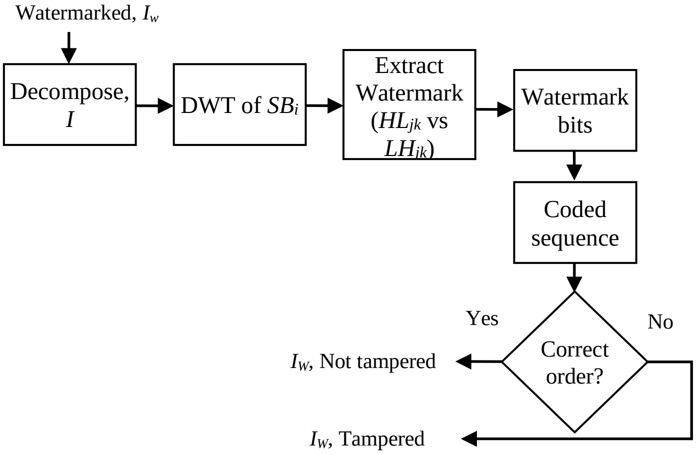

Fig.2. Block Diagram of Watermark Extraction

The Fig.2 shows the block diagram for watermark extraction. Being a blind method for watermarking, the extraction stage does not use the original image for comparison. At the final stage of the extraction if all the embedded codes are detected in correct order it can be inferred that the particular image is not tampered. Failure in extraction either from a sub-block or error in sequence order can be linked to the probability of image being tampered.

The watermark is spread in the entire image area during the process of watermarking. Hence sufficient care is taken not to degrade the image quality significantly. The coefficients should be varied to an extent that is large enough that they remain inert to the changes that may be incurred during the forward transform and inverse transform operations. Moreover there can be zero magnitude coefficients, adjusting these are also taken care of.

2.2.1 *Embedding Algorithm:*

1. Input the image, i of size $N \times N$.
2. Divide the image I into non-overlapping sub-blocks (SBj) of size $S \times S$. Here $j = 1, 2...P = S \times S$.
3. Select an appropriate range for block numbers (BN) based on the number i of sub-blocks. $BN_q = 1, 2\ldots(N \times N/S \times S)$.
4. Convert the digits in block sequence number BN_q to binary.
5. Denote the watermark bit array for a BN_q as W_i, where $i = 1, 2...M$. $M = 16$, assuming BN has four digits.
6. Compute DWT for the sub-block SB_j.
7. Embed the watermark bits considering corresponding coefficients from HL and LH band.

   if ($W_{ji} = 1$), set $HL_j(x, y) > LH_j(x, y)$

   else

   set $LH_j(x, y) > HL_j(x, y)$. Here, W_{ji} is the watermark pattern for j^{th} SB.
8. Ensure that a minimal difference, α, exists between corresponding coefficients.

   Else vary the largest in (HL, LH) pair by an amplification of v, $v = 1.1 < v < 2$.
9. Reset i to 1 and repeat the embedding process to embed two additional copies of watermark bits.
10. Perform inverse DWT for modified SB_j.
11. Increment j to next SB_j and repeat the steps from 5 for embedding with next number j from the sequence.
12. Combine all the embedded blocks and output the watermarked image I_w.

2.2.2 *Watermarked Extraction:*

1. Input the watermarked image I_w.
2. Divide the image I_w into sub-blocks (SB) of size S × S.
3. Compute DWT for the block SB_j.
4. Extract the embedded bits for block j

   If ($HL_j(x, y) > LH_j(x, y)$)

   $WE_jk = 1$;

   else

   $WE_jk = 0$;

   Here $k = 1, 2...3*\mathrm{M}$. WE_{ji} is the extracted code pattern for j^{th} sub-block.

5. Estimate the final set comparing the three set of extracted bits.

   If $((WE_jk + WE_jk + 16 + WE_jk + 32) > = 2)$

   $WE_{ji} = 1$;

   else

   $WE_{ji} = 0$;

6. Output the decimal equivalent for the block.
7. Decode the hidden sequence markings for all the subsequent blocks by repeating from step 3.
8. Output the status on tampering based on the correctness of sequence numbers found.
9. Set the intensity value as 0 for all tampered sub-blocks (SB_j) or regions in result image.

The extraction algorithm improves upon the final watermark outputted by selecting the best two from the three instances of extracts corresponding to each sequence code.

3. TESTING THE ALGORITHM

The proposed algorithm is implemented using MATLAB and tested on various images. The output image for two test cases is shown in the Fig.3.

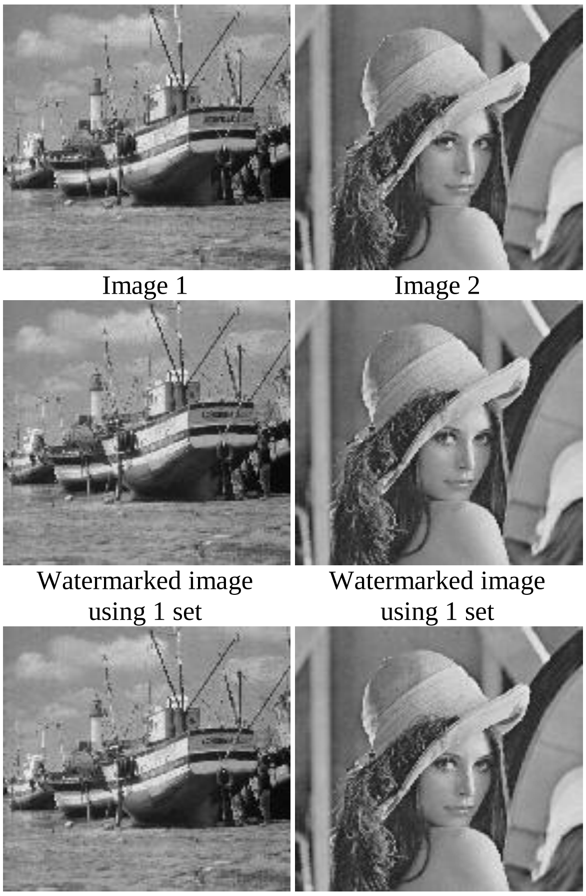

Image 1 Image 2

Watermarked image using 1 set Watermarked image using 1 set

Watermarked image 1 Watermarked image 2

Fig.3. Testing Image using Proposed Watermarking Algorithm

If four digit numbers are used, the range extends from 0 to 9999. However the range of values used for embedding depends on how the blocks are sized and the number of blocks to be marked. A block size of 16 × 16 is used for the above images of actual size 512 × 512. Hence there will be 1024 blocks. Selected range for indexing as used here is 0 to 1023. Thus a binary patter comprising 16 bits per digit is used for embedding into each of the block.

Also experimented is the redundant embedding and embedding the sequence code just once in the image sub-blocks. The resulting images are also included in Fig.3.

The quality of the watermarked image is analyzed using PSNR ratio. PSNR is the signal to noise ratio. Higher the values of PSNR lower the impact of distortion due to embedding. Embedding an external watermark is treated as noise addition.

Table.1. Shows the PSNR Values Measured for the Two Cases of Watermark Experimented

Image	Redundant embedding	Non-redundant embedding
Lena	33.46	38.59
Boat	30.44	35.22
Aero plane	37.99	43.02

The PSNR values in above table shows that the though every block is marked using a unique sequence code the net degradation is kept to minimal. Two sets of results in Table.1 shows the case when sub-blocks are marked just once vs. the case where three redundant set are marked per block. Obviously, when a sub-block is embedded thrice using an external data the quality suffers to certain extent. However, at the time of extraction redundant marking is more robust and infallible compared to the other.

4. CONCLUSION

A frequency domain watermarking method to detect image tampering is discussed. When conventional watermarking schemes for the sole purpose of copyright protection is used there is immense flexibility in selecting the watermark size and safe regions from the base image for hiding the watermark. But while tamper proofing image the watermark must cover the entire image area and the mark has to be unique in each of the portion so that their exact identification is possible. Another challenge is to ensure sound watermark extraction. To ensure this minimal difference, α is forced between corresponding coefficients set of watermark bits for better recovery. Two important requirements of watermarking process for tamper detection are met. The method presented is blind and robust. The use of redundant watermarking significantly improves the overall robustness to watermark removal attacks.

REFERENCES

[1] Kamran Hameed, Adeel Mumtaz and S.A.M Gilani, "Digital Image Watermarking in the Wavelet Transform Domain", *World Academy of Science, Engineering and Technology*, Vol. 13, pp. 86-89, 2006.

[2] Shiguo Lian, Dimitris Kanellopoulos and Giancarlo Ruffo, "Recent Advances in Multimedia Information System Security", *Informatica*, Vol. 33, No. 1, pp. 3-24, 2009.

[3] S.S. Bedi, Rakesh Ahuja and Himanshu Agarwal, "Copyright Protection using Video Watermarking based on Wavelet Transformation in Multiband", *International Journal of Computer Applications*, Vol. 66, No. 8, pp. 1-5, 2013.

[4] Ding Hai Yang, Zohu Ya Jain, Yang Yi-xian and Zhang Ru, "Robust Blind Watermarking Algorithm in Transform Domain Combining with 3D Video Correlation", *Journal of Multimedia*, Vol. 8, No. 2, pp. 161-167, 2013.

[5] Vidyasagar M. Potdar, Song Yan and E Chang, "A Survey of Digital Watermarking Techniques", *Proceedings of 3rd IEEE Conference on Industrial Information*, pp. 709-716, 2005.

[6] Rajneeshkaur Bedi, Anita Thengade and Vijay M. Wadhai, "A New Watermarking Approach for Non-numeric Relational Database", *International Journal of Computer Applications*, Vol. 13, No. 7, pp. 37-40, 2011.

[7] P. Meenakshi Devi, M. Venkatesan and K. Duraiswamy, "A Fragile Watermarking Scheme for Image Authentication with Tamper Localization Using Integer Wavelet Transform", *Journal of Computer Science*, Vol. 5, No. 11, pp. 831-837, 2009.

[8] Phen Lan Lin, Chung Kai Hsieh and Po-Whei Huang, "A hierarchical digital watermarking method for image tamper detection and recovery", *Pattern Recognition*, Vol. 38, No. 12, pp. 2519-2529, 2005.

[9] Qing Liu and Jun Ying, "Grayscale Image Digital Watermarking Technology Based on Wavelet Analysis", *Proceedings of IEEE Symposium on Electrical & Electronics Engineering*, pp. 618-621, 2012.

[10] Jobin Abraham and Varghese Paul, "Image Watermarking using Bit-planes from Grayscale Watermark", *Proceedings of International Conference on Information Science*, pp. 76-79, 2014.

[11] B. Sureka and G. N. Swamy, "Sensitive Digital Image Watermarking for Copyright Protection", *International Journal of Network Security*, Vol. 15, No. 1, pp. 95-103, 2013.

[12] Maha Sharkas, Dahlia R Elshafie and Nadder Hamdy, "A Novel Dual-purpose Image Watermarking technique", *International Journal of Computer, Electrical, Automation, Control and Information Engineering*, Vol. 1, No. 7, pp. 2022-2026, 2007.