IBIMA Publishing
Journal of Software & Systems Development
http://www.ibimapublishing.com/journals/JSSD/jssd.html
Vol. 2012 (2012), Article ID 881411, 9 pages
DOI: 10.5171/2012.881411

Robust Image Watermarking Using Genetic Programming

Almas Abbasi[1, 2] and Woo Chaw Seng[3]

[1]Faculty of Computer Science and Information Technology, University of Malaya, Kuala Lumpur Malaysia

[2]Faculty of Computer Science, COMSATS Islamabad, Pakistan

[3]Faculty of Computer Science and Information Technology, University of Malaya, Kuala Lumpur, Malaysia

Abstract

The utilization, sharing and distribution of digital data have been increasing with the wide adoption of internet. This resulted difficulty in protection of copyright and ownership of digital data. Digital watermarking has been proposed as a solution for digital data authentication and copyright protection. We present a genetic programming based watermarking technique for images. Genetic programming is used to structure the watermark by taking into account human visual system characteristics such as luminance sensitivity and contrast masking. A watermark consists of a pseudorandom real number sequence is embedded into perceptually significant blocks of vertical and horizontal sub bands in the wavelet domain. Then, correlation method is applied in watermark detection. Experimental results confirmed that our technique is robust against image processing attack, noise attack, geometric attack and cascading attack. Benchmarking results show that the proposed technique is more robust and more imperceptible compared with other genetic perceptual model-based techniques.

Keywords: Genetic Programming, Wavelet Domain, Digital Watermarking, Human Visual System.

Introduction

With the wide use of internet, and easily copying, transmitting, distributing and editing of digital contents, the copyright protection (Chang et al. 2010) of digital media is becoming a concern for the owners of digital property. There is a need to enforce authentication and intellectual property rights. One way to protect piracy of digital contents is to insert digital watermarks into the data using digital watermarking. Digital watermarking is a process in which we embed data; called watermark into a multimedia object such that watermark is later detected for authorization purpose.

In this paper Genetic Programming (GP) and Watson model for JPEG2000 images is being used to get the optimal level of watermark in Discrete Wavelet Transform (DWT) domain. Khan *et al* (2006) mentioned GP is an evolutionary computation technique which gets its inspiration from natural selection and biological evolution process .We give the desired output to GP. Then, GP takes operands, operators and a fitness function to generate candidate optimal solutions of the given problem. Fitness of candidate solution is measured by the fitness criteria specified by the user. GP works iteratively and stop when it finds an optimal solution or when it reaches a user specified number of generation. The output solution is usually in a form of tree structure.

Related Work

Lots of research has been done in the field of invisible watermarking. There are mainly two working domain in which watermarking can be done, i.e. spatial domain and frequency domain. In spatial domain, intensity values of pixels are changed directly to embed watermark. Most of the researchers now diverted toward DWT because of its excellent spatial localization, frequency spread and multi-resolution characteristics. Wang et.al (2007) proposed a Particle Swarm Organization (PSO) based blind watermarking technique in Discrete Multi-wavelet transformation (DMT) domain.

The drawback of their technique is they have not considered the alteration level of the selected coefficients for watermarking. Qi *et al* (2008) introduced a Quantization Index Modulation (QIM) and Singular Value Decomposition (SVD) based technique in DWT domain. Usman *et al* (2009) proposed a technique based on GP in wavelet domain. GP perform the selection of coefficients for watermark embedding in the Least Significance Bits (LSB) considering payload and imperceptibility. The drawback of these techniques is they do not incorporate the human visual system characteristic while embedding the watermark. In Lai *et al* (2009), they proposed a SVD-based watermarking scheme. The appropriate singular values are taken as an optimization problem and for that micro-genetic algorithm is applied to get the best singular values (SV) by taking into account the scaling factor to embed the watermark image.

Proposed Technique

The proposed algorithm works in two phases, in watermark embedding phase, an image X is transformed to first level discrete wavelet and embedding is performed in horizontal and vertical sub- bands in the wavelet domain as shown in Fig.1. Vertical (LH) and horizontal (HL) bands are divided into independent, non overlapping $m \times n$ blocks where (m,n) is a small integer. In our technique, we set it to 4×4.

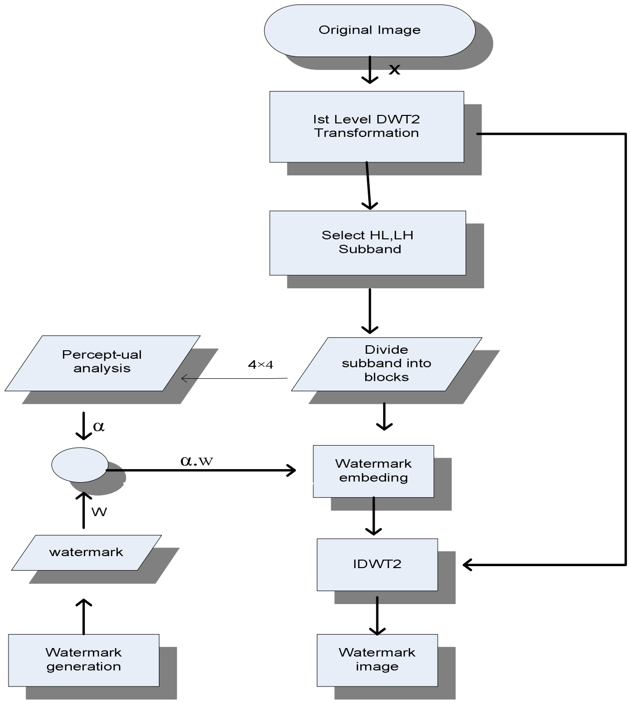


Fig .1 Watermark Embeding Process

Then perceptual significance, S of each m×n block is calculated using the following formula.

$$S = \sum_{i=1,\, j=1}^{i=m,\, j=n} H(i, j)^{2} \tag{1}$$

The sum of square of selected coefficients in a block of *m*×*n* size is represented by *S*. Then, we sort the blocks separately in each sub-band in descending order of the value of *S*. After that, we select the top *b* blocks where *b* is any integer representing the number of blocks of size 4×4 chosen for watermark embedding. The following equation is used to embed the watermark in the selected coefficients:

$$X'[i, j] = X[i, j] + |\propto| * W[i, j] \tag{2}$$

Where $X'[i, j]$ is the watermarked coefficient, $W[i, j]$ is a pseudo-random sequence and $\propto$ is HVS based function. GP is used to embed watermark using Human Visual System (HVS) characteristics. GP takes the luminance and contrast masking value for each of the selected coefficient in the 4×4 block and determine the optimum value of watermark.

Using user specified selection criteria, GP iterates a specified number of times until it gets best strength of watermark for the selected coefficient balancing both the imperceptibility and robustness. GP perform the same set of operations for all the selected coefficient in each block and then for each level. In this way, we get genetic perceptual mask using GP for the whole image.

In watermark detection phase it is assumed the used has in advance, the knowledge of all the steps that is performed while embedding the data. Correlation method is used for the watermark detection. In this phase, a watermarked image *I'* is decomposed into first level DWT. Then its HL and LH sub-bands are divided into *m*×*n* blocks. Sum of the square of coefficients are determined and sorted into descending order similar to the watermark embedding phase. From the sorted blocks, top *b* blocks are selected for watermark detection purpose. The correlation between marked coefficient and the watermark is calculated using the following equation:

$$C = \frac{1}{M}\sum_{i=1}^{M} y_i . t_i . \alpha \qquad (3)$$

Where *M* is the total number of coefficient watermarked, y_i is the watermark, t_i is image coefficient and α is the watermark level calculated through GP. Finally, the correlation value *C* is compared to a predefined threshold which determines whether the watermark exists or not.

A watermark is embedded using a perceptual model which exploits the characteristics of HVS to get good imperceptibility. Contrast masking and luminance masking factors are used in this technique. The strength of watermark which is to be embedded is control by HVS characteristic and is represented as follows.

$$\propto = f\left(a_l(\lambda,\theta,i,j), a_c(\lambda,\theta,i,j)\right) \qquad (4)$$

For each DWT transformed coefficient at location (i, j) within sub-band (λ,θ) where (λ) is the transform level and (θ) is the orientation (Liu et al. 2006).

$$a_l\left(\lambda,\theta,i,j\right) = \left(\upsilon_{LL,i',j'} / \upsilon_{mean}\right)^{\propto T} \qquad (5)$$

In Eq. (5), we perform luminance masking where $\upsilon_{LL,i',j'}$ is the coefficient value in LL sub-band. υ_{mean} is the LL sub-band constant corresponding to the mean luminance of display. $\propto T$ has the value 0.649. Details can be read in (Liu et al. 2006).

$$ac\left(\lambda,\theta,i,j\right) = \max\left\{1, \left(\frac{|\upsilon(\lambda,\theta,i,j)}{JND_{\lambda,\theta} a_l(\lambda,\theta,i,j)}\right)^{\varepsilon}\right\} \qquad (6)$$

Eq. 6 performs the contrast masking. JND threshold is formulated as follows. For detail read (Liu et al. 2006).

$$JND_{\lambda,\theta}(r) = \frac{1}{A_{\lambda,\theta}} a.10^{k\left\{\log_{10}\left(g_\theta f_0 2^\lambda / r\right)\right\}^2} \quad (7)$$

Where $a.$, g_θ, k , f_0 are constants, for the amplitude of the DWT 9/7 basis function corresponding to level λ and orientation θ. Parameter r is the visual resolution of the display in pixels/degree.

Details of the parameters, for DWT threshold model and amplitude for the first level of a 9/7 DWT applied in the experiment, can be found in (Liu et al. 2006).

Firstly, an initial random population p is created. If I is the individual of this population and X is the image then; for each individual in the population perform the following steps using GP.

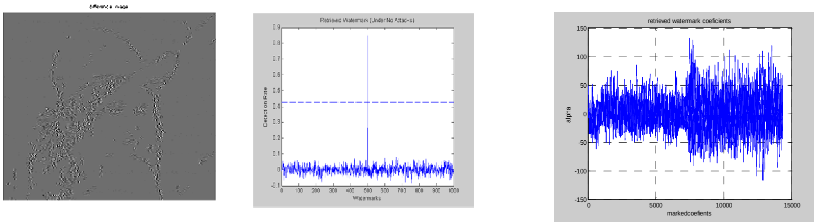
Step 1. Convert the image *X* into first level dwt2 Step2. Take the LH, HL sub band and perform the steps 3-8 for each sub band Step3. Compute $m \times n$ block. Step4. Compute sum of square of each coefficient in the $m \times n$ block using Equation 1. Step5. Sort all blocks in descending order; select top *b* blocks for embedding. Step6. Compute perceptual mask using Equation 4. Step7. Embed the watermark using Equation 2. Step8. Compute fitness using equation fitness=Structure Similarity Index Measure (SSIM).

Implementation Details

Matlab software is used to carry out simulations. To apply GP, GPLAB toolbox is used. Images such as Baboon, Boat, Lena, Couple, Cameramen, Peppers, etc. of size 512×512 are used as cover images. Ramped half and half method, defined in GPLAB, is used to create initial population in GP. GP function include *sin*, *cos*, *mylog*, *mydivide*, ×, —, + are used to perform operation on variables and constants. Variable terminals include luminance, contrast masking, and DWT coefficients.

Imperceptibility Measure

Imperceptibility of watermarked image is calculated using Peak Signal-to-Noise Ratio (PSNR) and Mean Square Error (MSE). Fig.2 shows our proposed technique has the ability to intelligently structure and embed the watermark and also introduce distortion using perceptual significance of pixels in a block, perceptual model and GP.



(a) (b) (c)

Fig.2 (a) Difference Image of *Lena*, and Detector Response for (b) Watermark Exist and (c) Watermark Absence

Robustness

The robustness of this technique is checked by applying different types of attacks on the watermarked images. Results show that our technique is robust against most of the attacks because watermark can still be detected after applying different types of attacks.

Filtering Attacks:

For testing purpose the watermark image is attacked with a low pass filter and median filter, each with window sizes from 2×2 to 6×6, and Wiener filter. Watermark is detected after each attack which shows the technique is robust to these types of attacks.

Noise Attack:

The other type of attack carried out is Gaussian noise addition with window size 3×3 and STD of 0.2, also noise with power of 500,1000,5000,10000, and 15000 was added and original watermark is detected from the corrupted images.

JPEG Compression Attack:

Compression of watermark images are performed with different JPEG quality factor (QF) values. The quality factor down to 5% is applied and watermark can be detected by the detector.

***Cascading Attacks**:*

The watermarked images are also tested against cascading attacks. Firstly, the image is subjected to Weiner filter, then the images were compressed with different JPEG QF 75%,50%,25% etc, and finally noise with different power of 500,1000,50000,10000, and 15000 was added to the same corrupted image. The detector still can detect watermark after each set of attacks.

Geometric Attacks:

In order to show the robustness against geometric attacks, cropping are used. Cropping with different rates like 75%, 50%, 15% are applied. The watermark is robust to cropping attack as watermark is still detected after the said attack.

Watermark Lena image is tested against the resize attack. A 512 ×512 image is resized to ½ and ¾ of its original size and watermark detector response is well above the threshold .Which shows that our technique is robust against the resize attack.

Watermark is also tested against rotation attack of degrees +45 and -45. After performing rotation attack, the detector still detects the watermark.

Matlab functions of **im2single**, **im2double** and zeropading rescaling attacks are also performed on the watermarked images and our technique is robust to these attacks.

Several GP simulations are carried out to get the best expression, through which optimal strength watermark was embedded in the images.

Formula: '–(–(–(–(*coef*, 0.16554), *sin*(*X1*)), *contrast*), *coef*)'

Where *contrast* is the contrast sensitivity, *coef* is the DWT coefficient and *X1* is the luminance value of a pixel in an image.

Experimental Results

The watermark embedding and watermark detection are performed on standard images as mentioned in section 4 above. The images are selected with different characteristic such as texture, flat, curves, contrast, smooth, light reflecting surfaces etc. They all are gray images of size 512×512. Fig.3 summarizes the measured values of PSNR, MSE and Structure Similarity Index Measure (SSIM) after attacks. PSNR and SSIM are the imperceptibility measures. The greater the value of PSNR, and the lesser the value of MSE, the better the imperceptibility of the watermarked image. Fig.3 also demonstrates the imperceptibility comparison of the proposed technique with Khan *et al* (2006), in terms of quality of watermarked image measured in PSNR, MSE, SSIM for different training images. The WPM represents Watson Perceptual Model and GPM is Genetic Perceptual Model proposed by Khan *et al* (2006).

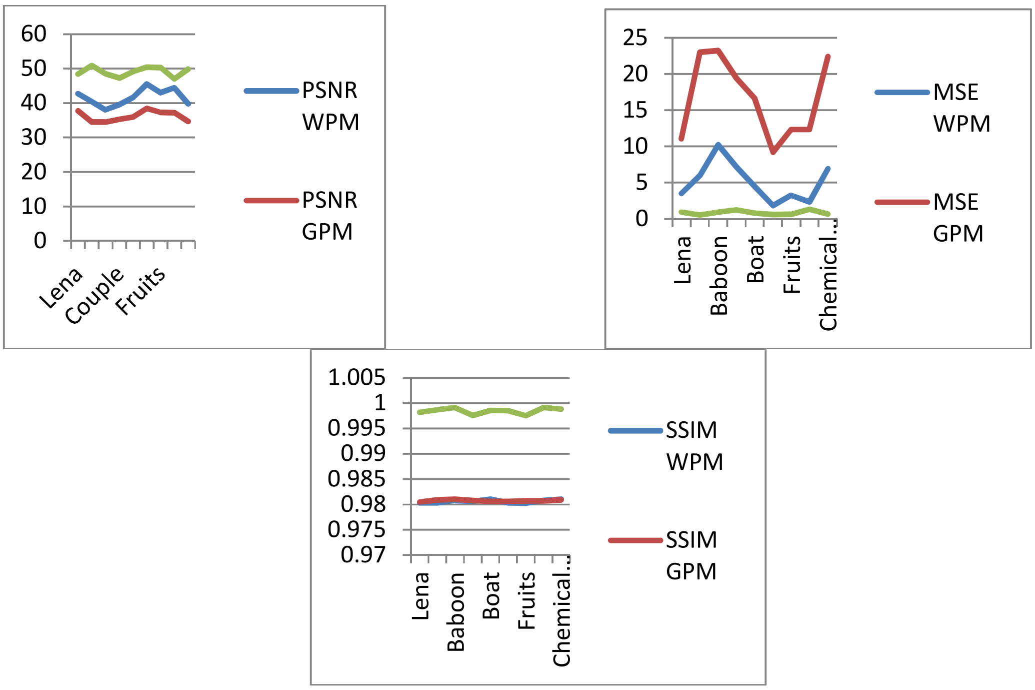


Fig.3. Imperceptibility Comparison of the Proposed Technique with Other Techniques

Fig.4 summarizes the average performance of different attacks on watermarked image and its comparison with other techniques. It is noticeable that the proposed technique outperforms the technique of Khan *et al* (2006). The improvement in terms of higher PSNR and SSIM values, and lower values for MSE.

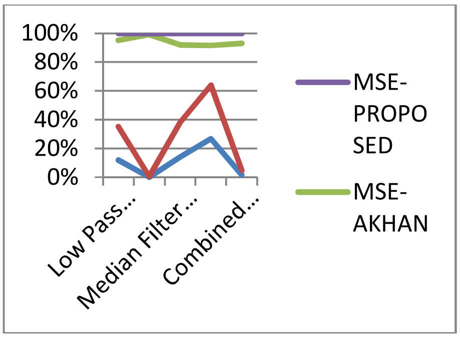


Fig.4. Robust Comparison of After Attacks Average Values of the PSNR and MSE of Proposed Technique with Other Techniques

Conclusion

In this paper a blind, still image, GP based watermarking algorithms is presented. To get the perceptually significant coefficient, the sum of square of coefficient in each block of size 4×4 is calculated and then sorted in descending order. The top *b* blocks are selected for embedding watermark. GP is used to structure the watermark according to HVS characteristics such as contrast masking and luminance sensitivity. Robustness of the proposed algorithm is tested against several attacks. Results of these attacks show that the proposed technique is resistant to most of the attacks. In the future, we will explore other fast machine learning techniques to get optimal DWT level and optimal block size for watermark embedding.

Acknowledgement

The authors thank University of Malaya Bright Sparks Program for the postgraduate scholarship awarded.

References

Chang, C. C., Chen, Y. H. & Kieu, D. (2010). 'A Watermarking Technique Using Synonym Substitution for Integrity Protection of XML Documents,' *ICIC Express Letters*, 4(1), 89-94.

Cox, I. J., Kilian, J ., Leighton, F. T. & Shamoon, T. (1997). "Secure Spread Spectrum Watermarking for Multimedia," *IEEE Trans. on Image Processing*, 6(12), 1673-1687.

Huang, H.- C., Chu, C.- M. & Pan, J.- S. (2008). "The Optimized Copyright Protection System with Genetic Watermarking," *.Soft Computing, A Fusion of Foundations, Methodologies and Applications - Special Issue on Bio-Inspired Information Hiding.*13(4).

Khan, A., Mirza, A. M. & Majid, A. (2006). "Intelligent Perceptual Shaping of a Digital Watermark: Exploiting Characteristics of Human Visual System," *KES Journal* 10(3): 213-223.

Lai, C.- C., Huang, H.- C. & Tsai, C.- C. (2009). "A Digital Watermarking Scheme Based on Singular Value Decomposition and Micro-genetic Algorithm," *International Journal of Innovative Computing, Information and Control*, 5(7),1867-1874.

Liu, Z., Karam, L. J. & Watson, A. B. (2006). "JPEG2000 Encoding with Perceptual Distortion Control," *IEEE Transactions on Image Processing* 15(7),1763-1778.

Qi, X., Bialkowski, S. & Brimley, G. (2008). "An Adaptive Qim and SVD Based Digital Image Watermarking Scheme In The Wavelet Domain," *Image Processing, 2008. ICIP 2008*. 15th IEEE International Conference on , ISBN: 978-1-4244-1765-0, 12-15 Oct. 2008, San Diego, CA.

Usman, I., Khan, A. (2009). "BCH Coding and Intelligent Watermark Embedding: Employing Both Frequency and Strength Selection," *Applied. Soft Computing,*10(1),332-343.

Usman, I., Khan, A. , Ali, A. & Choi, T.- S. (2009). "Reversible Watermarking Based On Intelligent Coefficient Selection And Integer Wavelet Transform," *IJICIC International Journal of Innovative Computing Information and Control*, 5(12),4675-4682.

Wang, Z., Sun, X. & Zhang, D. (2007). "A Novel Watermarking Scheme Based On PSO Algorithm," *LNCS* 4688, 307-314.

Zheng, Y., Wu, C. H., Lus, Z. M. & Ip, W. H. (2008).'Optimal Robust Image Watermarking Based On PSO and HVS In Integer DCT Domain,' *IJCSES International Journal of Computer Science and Engineering System*, 2(4).