International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2016): 79.57 | Impact Factor (2017): 7.296

A Spiht Resistant Zero Watermarking Scheme in Wavelet Domain

Keerti Kulkarni[1], Reena Kulkarni[2], Priyadarshini K Desai[3]

[1, 2, 3]BNM Institute of Technology, Bangalore, India

Abstract: ***In this paper, a new method for blind watermarking is used to achieve robustness against SPIHT compression methods as well as some other well known attacks such as Histogram Equalization, Gamma Correction, median noise, salt and pepper noise. The watermark is encoded via singular value decomposition and later embedded. Then we apply discrete wavelet transform (Haar) at one level and the watermark bits are encoded in the coefficients. At the receiver the watermark is obtained after decoding.***

Keywords: digital image watermarking, compression attacks, SPIHT, DWT, Haar Wavelet

1. Introduction

A Digital watermark is a kind of a marker embedded in an audio or an image, to identify the copyright of the signal. It is also used to verify the authenticity or the integrity of the images. It is also used for source tracking and broadcast monitoring. 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 watermarked signal and the cover signal. The signal where the watermark is to be embedded is called the *host* signal. A watermarking system is usually divided into three distinct steps, embedding, attack, and detection. 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. There are many possible modifications, for example, lossy compression of the data (in which resolution is diminished), cropping an image or video, or intentionally adding noise.

Detection (often called extraction) is an algorithm which is applied to the attacked signal to attempt to extract the watermark from it. If the signal was unmodified during transmission, then the watermark still is present and it may be extracted. 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. In this paper we propose a new method for protection against the compression attack using the SPIHT algorithm. The paper is organized as follows. We describe some of the already existing techniques in section 2. Section 3 describes the proposed approach. Section 4 has some of the experimental results, section 5 has comparisons and section 6 concludes the work.

2. Background

Cox, Kilian [1] talk about the spread spectrum approach to watermarking where in marked signal is obtained by an additive modification. Xinyang Huang et, al[2] present a technique to survive geometric attacks by designing a algorithm of scalar costa system based on DWT in the rotation- and scale-and translation-(RST) moment invariant wavelet, i.e. RSTMIW domain. Zheng Xiong-bo et, al [3] blind digital watermarking algorithm based on wavelet transform is proposed. Chih-Chin Lai et, al[4] propose a digital watermarking technique based on singular value decomposition and wavelet transform. Sanaz Shahraeini et. al, [5] propose a robust digital watermarking scheme based on hybrid fractal wavelet against JPEG compression attack. Taherinia et. al, [6] propose a robust spread spectrum technique using 2-level DCT. Balado et. al [7] use Turbo coding in the DCT domain for digital watermarking. Wei-Hung Lin et, al [8] propose a Watermarking Method Based on Significant Difference of Wavelet Coefficient Quantization. Rahimi et. al [9] propose a watermarking scheme in the wavelet domain using turbo codes for robustness against JPEG compression attacks. Depending upon the domain in which the watermark is inserted, these techniques are basically classified into two categories, i.e., spatial-domain and transform-domain methods. Embedding the watermark into the spatial domain component of the original image is an easy technique as watermark is inserted directly onto the pixel level. It has the advantages of low complexity and easy implementation. However, the spatial-domain methods are generally fragile to image processing operations or other attacks. Transform domain techniques are used to embed the watermark by modulating the magnitude of coefficients in a transform domain, such as discrete cosine transform, discrete wavelet transform (DWT), and singular value decomposition (SVD). The transform domain techniques are usually preferred over spatial domain techniques because they are much more resilient in presence of noise.

3. Proposed Approach

a) DWT

Discrete wavelet transform is a multi-resolution decomposition of a signal. The low pass filter applied along

a certain direction extracts the low frequency (approximation) coefficients of a signal. On the other hand, the high pass filter extracts the high frequency (detail) coefficients of a signal. In 2D applications, for each level of decomposition, first perform the DWT in the vertical direction, followed by the DWT in the horizontal direction. After the first level of decomposition, there are 4 sub-bands: LL1, LH1, HL1, and HH1 as shown in fig 1, 2.

Figure 1

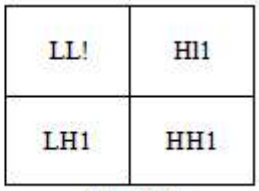

Figure 2

b) SVD

Singular value decomposition is a linear algebra technique used to solve many mathematical problems [4]. Any image can be considered as a square matrix without loss of generality. So SVD technique can be applied to any kind of images. The SVD belongs to orthogonal transform which decompose the given matrix into three matrices of same size [3]. To decompose the matrix using SVD technique it need not be a square matrix. Let us denote the image as matrix A. The SVD decomposition of matrix A is given using equation (1)

$$A=USV^T \quad (1)$$

U and V are unitary matrices such that
U*UT = I
V*VT = I

Where, I is an Identity matrix. S is the diagonal matrix having in its main diagonal all non-negative singular values of A. These positive singular values can be used to embed watermark. The order of singular matrix S is same as original matrix A.

4. Experimental Results

The images used are all 256 x 256 images. Fig(a) represents the watermarked image. Fig(b) represents the extracted watermark in the absence of any attack. Fig(c) shows the compressed image and Fig(d) the corresponding extracted watermark. Fig(e) shows Histogram equalized image and Fig(f) the corresponding extracted watermark. Fig(f) shows the median filtered image and Fig(g) the corresponding extracted watermark. Fig(h) shows the image corrupted by salt and pepper noise and Fig(i) the corresponding extracted watemark.

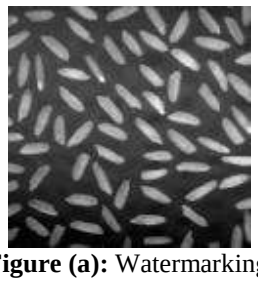

Figure (a): Watermarking

Figure (b): extracted watermark image

Figure (c): Compressed image

Figure (d): Extracted watermark image

Figure (e): Watermarked image

Figure (f): extracted watermark image

Figure (g): Watermarked image

Figure (h): Extracted watermark image

Figure (i)

Figure (j)

5. Comparisons

The quality of the watermarked image be measured in the form of PSNR is the main criteria used to measure the quality of the watermarked image. The peak signal to noise ratio (PSNR) and Mean Square Error (MSE) are defined as follows.Given a noise-free $m \times n$ monochrome image I and its noisy approximation K, MSE is defined as:

$$MSE = \frac{1}{m\,n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i,j) - K(i,j)]^2 \quad (2)$$

The PSNR is defined as:

$$\begin{aligned} PSNR &= 10 \cdot \log_{10}\left(\frac{MAX_I^2}{MSE}\right) \\ &= 20 \cdot \log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right) \\ &= 20 \cdot \log_{10}(MAX_I) - 10 \cdot \log_{10}(MSE) \end{aligned} \quad (3)$$

Here, MAX_I is the maximum possible pixel value of the image. When the pixels are represented using 8 bits per sample, this is 255.

Table 1: MSE and PSNR of the watermarked images for various attacks

	MSE	PSNR
Original Image	244.9738	24.2396
Watermarked Image	3.7242	42.4205
SPIHT Compressed	3.3657	42.86
Histogram Equalization	54.3064	30.7823
Median Noise	3.7242	42.4205
Salt and Pepper Noise	6.9505	39.7106

6. Conclusion and Future Work

In this paper, a robust image-watermarking technique based on single level DWT and SVD has been presented. The Experimental results of the proposed technique have shown both the significant improvement in perceptibility and the robustness under possible attacks. Further work of integrating the performance measured against Rotation, Scaling, contrast adjustment (CA), cropping, and gamma correction (GC) against various attacks is being done.

References

[1] I. Cox, J. Kilian, F. Leighton, and T. Shamoon, “Secure Spread Spectrum Watermarking for Multimedia,” IEEE Transactions on Image Processing, vol. 6, no. 12, pp. 1673-1687, Dec. 1997.

[2] Xinyang Huang, Hengyang Yang Luo ; Minsheng Tan ; Dazheng Lin “A Image Digital Watermarking based on DWT in Invariant Wavelet Domain” in fourth international conference on Image and graphics 2007 , Aug 2007, pgs 329-336

[3] Zheng Xiong-bo ,Zhang Xiao-wei ; Sun Ming-jian “A blind digital watermarking algorithm based on wavelet transform”, IEEE International Conference on Computer Science and Automation Engineering, 2011, Vol 4, page 679-682.

[4] Chih-Chin Lai “Digital Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition”, in IEEE Transactions on Instrument and measurement Nov. 2010 Volume: 59, Issue: 11, Page(s): 3060 – 3063

[5] Sanaz Shahraeini 1 and Mahdi Yaghoobi “A Robust Digital Image Watermarking Approach against JPEG Compression Attack Based on Hybrid Fractal-Wavelet” in 2011 International Conference on Computer Communication and Management Proc .of CSIT vol.5 (2011)

[6] H. Taherinia and M. Jamzad, .A robust spread spectrum watermarking method using two levels dct,. Int. J. Electron. Secur. Digit. Forensic, vol. 2, no. 3, pp. 280.305, 2009.

[7] G. F. Balado F. and S. S., .Turbo coding for sample-level watermarking in the dct domain,. in Proceedings of International Conference on Image Processing, vol. 3, Thessaloniki, 2001, pp. 1003.1006.

[8] Wei-Hung Lin; Shi-Jinn Horng; Tzong-Wann Kao; Pingzhi Fan; Cheng-Ling Lee; Yi Pan; , "An Efficient Watermarking Method Based on Significant Difference of Wavelet Coefficient Quantization," Multimedia, IEEE Transactions on , vol.10, no.5, pp.746-757, Aug. 2008.

[9] Rahimi, Arabzadeh, M. Danyali, H. ; Kazemi, K. “A JPEG resistance watermarking technique in wavelet domain based on Turbo codes”, 19th Iranian Conference on Electrical Engineering, May 2011, pg 1-3