

FULLY ROBUST SPREAD SPECTRUM WAVELET WATERMARKING SYSTEM

M. Osadebey and A. Georgakis

Digital Media Laboratory (DML),
Department of Applied Physics and Electronics,
Umeå University, SE-90187 Umeå Sweden
apostolos.georgakis@tfe.umu.se

ABSTRACT

Existing spread spectrum based watermarking techniques can not despread the encoded signal as expected in a typical spread spectrum communication system. Also the change in the statistics of the watermarked image as a result of attacks are not adequately compensated. It is therefore expected that these systems have not yielded the desired fully robust characteristics. This paper presents a spread spectrum technique for digital image watermarking. During the detection phase the spatial-frequency localization property of wavelet transform is explored and compensated for attack-induced changes in the statistics of the watermarked images. Experimental results from the system exhibit excellent anti-jamming features similar to spread spectrum communication techniques. Furthermore they confirm the superior performance over existing correlation-based spread spectrum wavelet watermarking system.

Index Terms— Spread spectrum, watermark, correlation, wavelet transform

1. INTRODUCTION

The major criteria for assessment of watermarking systems are security, imperceptibility and robustness to attacks. The most lethal malicious attack is geometric distortion rotation, scaling and translation. In the literature researchers have proposed methods to increase the robustness of watermarks to geometric attacks [1, 2, 3, 4, 5]. A close look at the proposal in [5] showed that a new system is created within the watermarking system. The system in [1] had been reported in [4] to be theoretically sound but impractical. The template used in [3] is vulnerable to attacks. The system in [4] restricts the watermark to one with periodic pattern hence restricting the applicability of the system. The authors in [6] proposed a robust spread spectrum watermarking system by embedding data in specific sub-bands and channels and increasing orthogonality of the modulating pseudo-random codes. However the acclaimed excellent performance of the system over

other systems did not include malicious attacks such as geometric distortion. Performance factors analysis of wavelet-based watermarking methods as carried out in [7] revealed their vulnerability to severe levels of JPEG compression, median filtering and geometrical attacks.

Study of a spread spectrum technique applied to wireless communication show that the despreading process in the decoder unit of the receiver plays a key role in conferring the system with its excellent anti-jamming feature. The novel feature of our watermarking system design is its model as a communication system [8] with the original (host) image representing the communication channel, the watermark represent the message (base band) signal and the legal and malicious attacks represent the noise, interference or jamming of the message signal. In the embedding section the frequency of the message signal is spread using a *pseudo-random noise* (PRN) signal defined by a secret key. An exact replica and perfectly synchronized PRN signal is generated at the decoding section that consists of a tuner (dspreader), a correlator and a comparator units.

2. ENCODING UNIT

The watermark has black pixels as foreground and white pixel as background. The state of the PRN generator is set to that of a predefined secret key. This will set the PRN generator to the same fixed state and enables repetition of same random numbers. During scanning for the watermark, for every foreground pixel a different and independent PRN z of same dimension as the wavelet transform of the host image is generated and added to the horizontal and vertical detail coefficients of the wavelet transform of the host image $W(I)$ scaled by a defined distortion factor K according to the equation

$$WQ = W(I) + K \sum_{z=1}^p PRN_z \quad (1)$$

where p is the number of foreground bits. PRN signal is generated for every background pixels but is not added to the host image.

The work was supported by a research grand from the Faculty of Science, Umeå University.

3. CORRELATOR UNIT

For each foreground bit i and background bit j of the watermark, let H_i, V_i, H_j, V_j , be correlation value between the horizontal H and vertical V details component of the wavelet decomposed host image and the PRN signal. The average correlation is:

$$C_H = \frac{1}{N} \left(\sum_{i=1}^p H_i + \sum_{j=1}^q H_j \right) \quad (2)$$

$$C_V = \frac{1}{N} \left(\sum_{i=1}^p V_i + \sum_{j=1}^q V_j \right). \quad (3)$$

In the absence of attack, the correlation between the PRN signal generated at the correlator unit (corresponding to the foreground of the watermark) and the watermarked image will be high because corresponding PRN signals were embedded and localized in frequency and space of the wavelet decomposed watermarked image. On the contrary, the correlation between the PRN signal generated at the correlator unit and the wavelet decomposed watermarked image will be very low (close to zero) because the corresponding PRN signals are not constituent of the wavelet decomposed watermarked image.

4. COMPARATOR UNIT

In the comparator unit every correlation values in the correlation function is scanned and compared to a predefined scalar number called decision threshold value τ . If any of the correlation function value is greater than the decision threshold value one bit is entered into the corresponding point in an initially created null vector space of same dimension as the watermark. Otherwise a zero bit is entered. In the absence of attack we have $\tau = C_H + C_V$.

An attack changes the spatial and frequency domain statistics of the watermarked image. Assume that the net increase in correlation values, resulting from attack, for the horizontal and vertical components are $\Delta H_i, \Delta H_j, \Delta V_i, \Delta V_j$ respectively, the new correlation decision threshold value becomes

$$\begin{aligned} \tau_D &= \frac{1}{N} \left(\sum_{i=1}^p (H_i \pm \Delta H_i) + \sum_{j=1}^q (H_j \pm \Delta H_j) \right) \\ &+ \frac{1}{N} \left(\sum_{i=1}^p (V_i \pm \Delta V_i) + \sum_{j=1}^q (V_j \pm \Delta V_j) \right) \quad (4) \end{aligned}$$

The above equation indicates that attacks cause an upward or downward shift in the original threshold decision values of the comparator. The shift in correlation values if not compensated for will result in error of judgment regarding the presence of watermark. The severity of attacks on a watermarked

image cannot be precisely measured by a watermarking system; hence the recovery decision threshold value resulting from this attack cannot be precisely determined. The best we have done so far is to determine that there is either an upward or downward shift in the threshold decision value. This issue was addressed in [9, 10] using probabilistic approach. The design principle of the comparator unit of our watermarking system is a departure from existing probabilistic technique. In line with Eq. 4 the recovery decision threshold of the comparator unit is discretized upwards and downwards in steps T of the mean correlation function τ using step size ρ so that the extracted watermark W_E is according to the equation

$$W_E = C_\tau = \begin{cases} 1 & c \geq T\rho\tau \\ 0 & c \leq T\rho\tau \end{cases} \quad (5)$$

The step size ρ gives the comparator unit the resolution power to search the decision threshold space for values that gives correct judgment on recovery of the watermark, and compensate for the shift in the statistics of correlation values. By doing so the watermarking system is robust, sensitive and adaptive to all known forms and severities of attacks that cause a shift of the decision threshold during decoding in correlation-based technique. We adopted heuristic approach to determine the step size used for discretizing the mean threshold value.

4.1. Simulation of watermarking system

Values of distortion factors ranging from the lower limit of 0.02 to upper limit of 20 in steps of 0.02 were inputted into the watermarking system. Each distortion factor value gives ten peak signal to noise ratio because the decision threshold of the comparator is discretized upwards in ten steps of the mean correlation function. However, in this simulation, the maximum of the ten peak signal to noise ratios corresponding to each distortion factor is the output (maximum PSNR). Simulation result showing the first, second and third sub-band for a 3-level wavelet decomposition of the host image is shown in Fig. 1.

4.2. Analysis of simulation result

As shown in Fig. 1, the peak signal to noise ratio (PSNR) of the recovered watermark increases at different rates for each sub-band from its lowest level until it attains a threshold value where it remains constant no matter the increase in distortion factor. The quality of recovered watermark decreases with increasing sub band. Though the third sub band offered the lowest visual quality of about 11 dB, the output is quite visible to the human visual system.

4.3. The need for a despreader unit

The objective of our watermarking system design is to embed a watermark that is imperceptible and that can also be unambiguously detected. In the previous section we have seen that

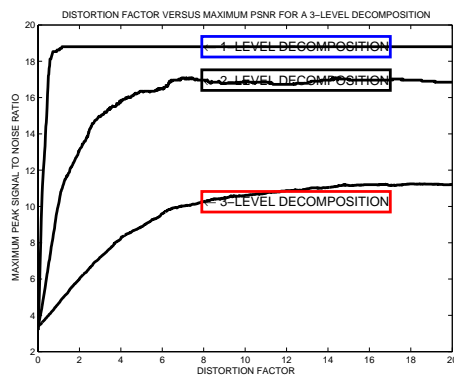


Fig. 1. Variation of maximum PSNR of recovered watermarks with distortion factor in each sub band for a 3-level decomposition

from the simulation result if we choose to have an imperceptible watermark we need to trade off unambiguous detection and if we choose to have a watermark that can be unambiguously detected in an image we will have to trade off imperceptibility of the watermark.

To achieve our goal of both imperceptibility and unambiguous detection of the watermark our design strategy is break the simulation curve (distortion factor versus maximum PSNR of recovered watermark) into two sections to derive two independent units the encoding (spreading) and despreding units. The encoder unit will then be fed into the despreding unit. The despreding unit will despread the output of the encoding unit (watermarked image). Sectioning of the simulation curve to obtain the encoding and despreding units for a 1-level decomposition is shown in Fig. 2. Based on our simulation result the distortion factor of the encoder is set at $K \ll 1.2$ and the minimum distortion factor of the despreding is set at $K \geq 1.2$. This is the minimum value at which the despreding and of course the watermarking system can operate to encode watermark imperceptibly and detect unambiguously. The operation of the despreding unit is described below.

During the encoding phase there is a spreading of the spectrum of the watermark. Hence it is expected that despreding of the watermarked image will take place before watermark detection as in a typical spread spectrum communication technique. The despreding unit generates PRN signals synchronized with that at the embedding stage and successively add a scaled version of the signal to the horizontal and vertical components of the wavelet decomposed watermarked image. The scale of weight is variable but fixed above a threshold value $K \geq 1.2$. The despreding performs two functions. It despreads the high frequency watermark back to its original base band watermark signal before been made available to the correlator stage of the watermarking system. At same time it spreads the frequency of any form of attacking signal reducing its effect to insignificant level in the wa-

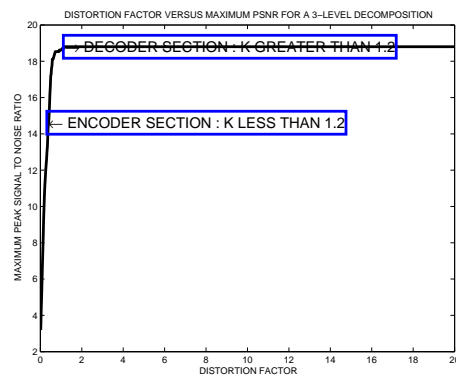


Fig. 2. Break up of the simulation curve into two sections to form the encoder and despreding units

termarked image thereby reversing the effect of any attack on the watermarked image. By varying (tuning) the scales of weight of the PRN signal the system adaptively adjust itself to reverse the effect of all forms and severities of attacks.

5. EXPERIMENTAL RESULTS

The universality and applicability of our algorithm to any kind of host image and watermark pattern is demonstrated using the standard Lena image as host image and the popular Coca-Cola logo as watermark. Figures 3(a)-(f) show the PSNR curves for all the recovered watermarks under various attacks. As it can be seen from the graphs the proposed watermarking system is fully immune to all forms and severities of attacks.

6. CONCLUSIONS

This paper proposes a fully robust, secure and tunable spread spectrum correlation-based wavelet watermarking system. Experimental results obtained confirm its superior performance over existing wavelet based spread spectrum watermarking schemes.

7. REFERENCES

- [1] J. Ó. Ruanaidh and T. Pun, "Rotation, scale and translation invariant digital image watermarking," in *Proc. IEEE Int. Conf. on Image Processing (ICIP'97)*, 1997, vol. 1, pp. 536–539.
- [2] M. Kutter, S. Bhattacharjee, and T. Ebrahimi, "Towards second generation watermarking schemes," in *In Proc. of IEEE Int. Conf. on Image Processing (ICIP'99)*, 1999, vol. 1, pp. 320–323.
- [3] S. Pereira and T. Pun, "Fast robust template matching for affine resistant image watermarking," in *In Proc. of*

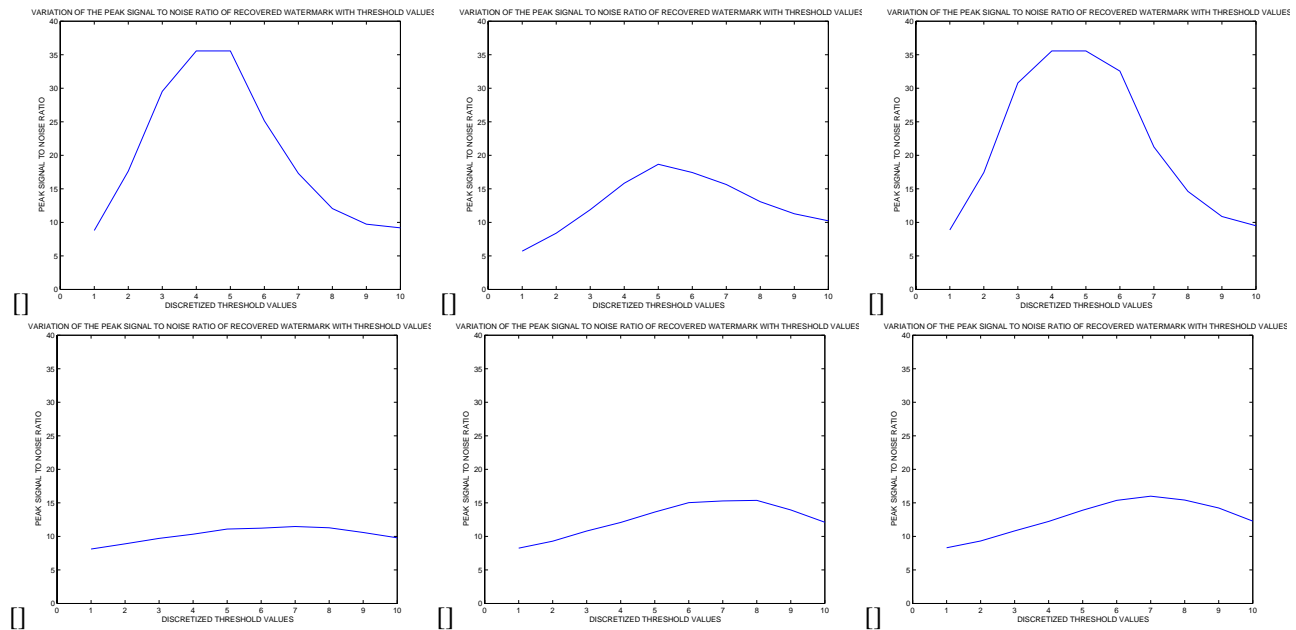


Fig. 3. The variations of PSNR for all the recovered watermarks with discrete decision threshold values for a 1-level wavelet decomposition for the following attack schemes: (a) 5% JPEG compression, (b) Resizing to 128×128 , (c) Laplacian filtering, (d) Cropping attack, (e) Gaussian filtering attack, (f) 120-degree rotation attack.

Intl. Workshop on Information Hiding, 1999, vol. LNCS 1768, pp. 200–210.

detection,” in *In Proc. of COST254 Workshop on Intelligent Communications*, 1998.

- [4] C.-H. Lee and H.-K. Lee, “Geometric attack resistant watermarking in wavelettransform domain,” *Optic express*, vol. 13, pp. 4, 2005.
- [5] N. Kaewkamnerd and K.R Rao, “Wavelet based watermarking detection using multiresolution image registration,” in *In Proc. of TENCON’00*, 2000, vol. 2, pp. 171–175.
- [6] S. P. Maity, M. K. Kundu, and T. S. Das, “Design of a robust spread spectrum image watermarking,” in *4th ICVGIP*, 2004, pp. 145–150.
- [7] C.-S. Woo, J. Du, and B. Pham, “Performance factors analysis of a wavelet-based watermarking method,” in *In Proc. of the Australian Workshop on Grid computing and research*, 2005, vol. 44, pp. 89–97.
- [8] S. D. Wolthusen, M. Arnold, and M. Schmucker, *Techniques and application of digital watermarking and content protection*, Artech house Inc, 2003.
- [9] E. Masataka and M. Akio, “An analysis of correlation-based watermarking systems,” *Electronics and communications in Japan, Part 3*, vol. 86, no. 11, 2003.
- [10] A. Piva, M. Barni, F. Bartolini, and V. Cappellini, “Threshold selection for correlation based watermark