INFORMED POSITION BASED WATERMARKING

PAULO VINICIUS KOERICH BORGES[1], JOCELI MAYER[1]

[1]LPDS–Digital Signal Processing Research Laboratory - Department of Electrical Engineering
Federal University of Santa Catarina - SC, Brazil
{paulo,mayer}@eel.ufsc.br

Abstract. In this work we propose improvements to the preliminary investigation on position based watermarking [7] by proposing an informed insertion approach. In addition, we see how these modifications bring even higher fidelity in comparison to the original work, and how the system may become reasonably robust to some common image processing operations. Regarding robustness, we also show how the proposed system may have an unique approach when dealing with collusion attacks. Usually in watermarking systems, the information to be transmitted is related to the watermark sequence itself. In contrast, in position based watermarking, the information is given by the watermark *position* in the image. In the informed embedding method for position based watermarking introduced here, an optimization criteria to choose the best among the available positions is suggested, improving considerably the system's performance. Moreover, we compare the improved system with the traditional spread spectrum method and obtain satisfactory results regarding both fidelity and robustness to different attacks.

1 Introduction

In general, watermarking systems aim to have good performance regarding all the important requirements such as perceptual transparency, robustness, good payload, etc [1]. For many applications, fidelity may be the most important, where a very high signal-to-noise ratio (SNR) is desired. This is the main advantage and motivation behind position based watermarking (PBW). Although for many of these applications the watermarked Work does not suffer any kind of processing, users often unmaliciously modify the Work. These robustness issues, not previously dealt with in the original paper, are now faced here. In the case of malicious attacks, PBW can behave in an unique manner when dealing with collusion attacks.

This paper initially presents a brief overview of PBW. In the sequence, in Section 3, we propose several improvements to original work on PBW. First, we decrease the time required for the detection process significantly by suggesting detection in the frequency domain. Afterwards, we deal with an optimization issue, where the ideal position set (among a few) is selected. In Section 3.3, we bring up and exploit one important feature of PBW: its ability to allow a choice of the watermark (ie. the pseudo-random sequence block). This is possible because the information to be transmitted is given only by the watermark position, and not by its content. We focus on which characteristic are best desired for the watermark to be inserted, as well as how many watermarks we should have available to choose from. Section **??** deals with the modifications that can be done to make the method robust to some very common image processing operations. In addition, this sections shows how the system may be suitable to survive malicious collusion attacks. Finally, Section 5 compares and illustrates that the proposed informed embedding system can have better performance than the traditional spread-spectrum method.

2 Overview of PBW

In traditional watermarking schemes, the information to be transmitted is usually related to the watermark sequence itself. In PBW, the embedding procedure is based on the position of pseudo-random watermark blocks. The blocks are inserted in the image and their position correspond to the information to be transmitted. In the detection process, the detector scans the image and finds *where* these blocks are placed, and decodes these positions to a unique bit string.

Let us consider a host image I_0. A a pixel grid of size NxM, where N is the image height and M is the image width, may represent I_0. In this grid, it is possible to insert k watermarks w of size $w_h \times w_w$ (where w_h is the watermark block height and w_w is the watermark block width), made up of 1's and -1's, modulated by a gain K, as shown in Fig. 1. Let Ref be pixel $(0,0)$ of the watermark blocks, as it shown in Fig. 2.

Let us suppose, for example, that we wish to embed the following bit string S_1 to the image:

S_1 = 0010011: one could say, for example, that making use of an appropriate coding scheme, S_1 could be represented by the embedding of a watermark w with its reference Ref placed over pixel $(10,25)$ of the host image and another watermark w with its reference Ref over pixel $(75,120)$ of the host image I_0.

So, assuming traditional additive embedding technique in the spatial domain, the marked image is identical to the original one, except where the watermark blocks are placed.

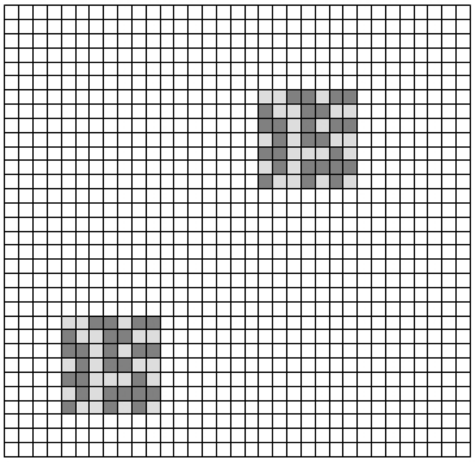


Figure 1: Image grid with two pseudo-random sequences.

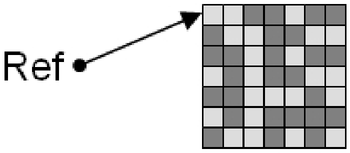


Figure 2: Representation of the reference pixel.

If the insertion is applied on the DCT domain, for example, the distortion is spread all over the image.

In the detection process, the detector scans the image and finds the exact positions in the image with the highest correlation to the watermark blocks, as illustrated in Fig. 3. These positions are finally decoded to the bit string they represent.

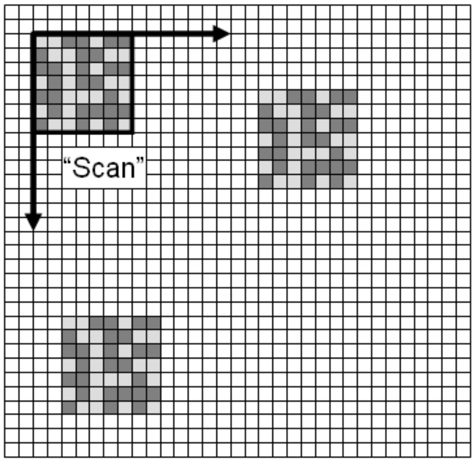


Figure 3: The process of searching for watermarking blocks.

The capacity for the method clearly depends on the image size and on the number and size of watermark blocks. Considering no superposition of one watermark over another, and considering that splitting of the watermark is not permitted, the capacity is given by:

$$Cap = \frac{\log[C(p,k)]}{\log 2} = \log_2[C(p,k)] \tag{1}$$

where

$$C(p,k) = \frac{p!}{(p-k)! \cdot k!} \tag{2}$$

is the combination formula, and p

$$\begin{aligned} p = {} & (N - w_h + 1) \cdot (M - w_w + 1) \\ & - (k-1) \cdot [(2 \cdot w_w - 1) \cdot (2 \cdot w_h - 1) - 1] \end{aligned} \tag{3}$$

is the number of available positions for the insertion of k watermarks.

An illustration of the above equation (1) can be seen in Fig. 5

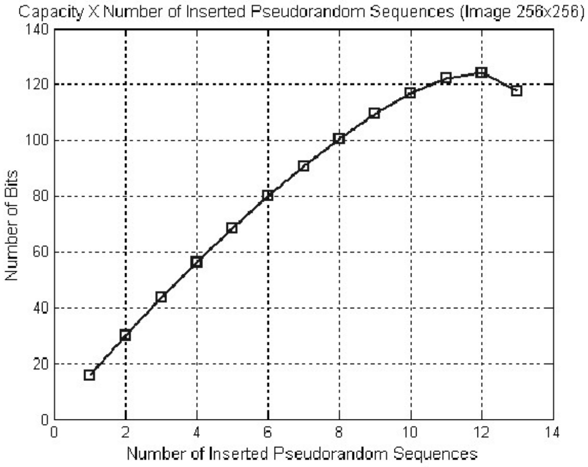


Figure 4: Capacity for a 256×256 image with watermark blocks of size 32×32.

3 Proposed Improvements

3.1 The detection procedure

One major disadvantage of the initially proposed PBW is the computationally inefficient detection process. The operation of scanning the image and calculating the correlation for each position can be quite time consuming for large images. As a simple alternative to overcome this inefficiency, we make use of the *correlation theorem* [9]. The correlation can then be carried out in the frequency domain via the FFT (Fast Fourier Transform), by simply multiplying the Fourier

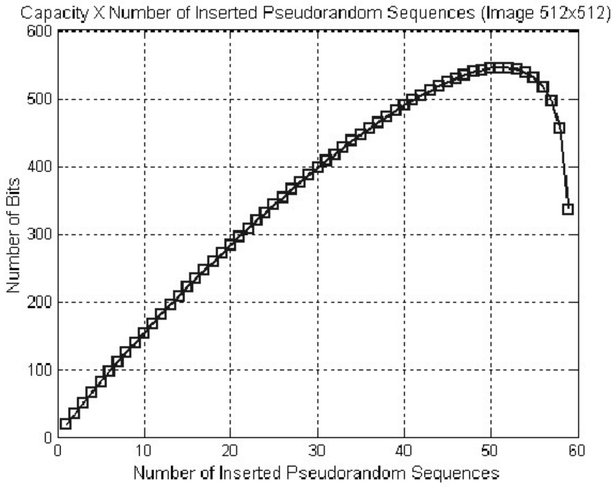


Figure 5: Capacity for a 512×512 image with watermark blocks of size 32×32.

transforms of both the image and watermark block. As an example, suppose we are inserting information in the spatial domain of the Lena image. The distortion occurs only inside the indicated square regions in the input image I_W of Fig. 6, which shows the block diagram for the proposed detector (operations like padding with zeros, rounding, etc, are omitted from the diagram).

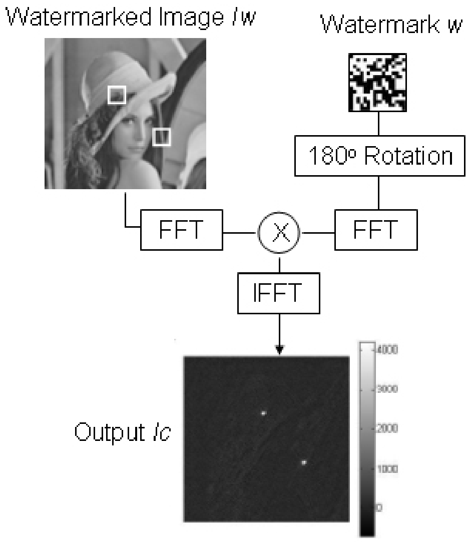


Figure 6: Block watermarked Lena.

So, the bright spots in the output image I_C represent the positions where the watermark blocks were placed, becoming clear the relationship between I_C and the squares positions in I_W. An analysis of computational complexity of both the spatial and frequency domain detection method is given next. This comparison presents the advantage of using the correlation theorem to speed up the process. Equation (4) presents the correlation operation in its basic form, for a block w of dimensions $w_h \cdot w_w$:

$$R_{I_w w} = \frac{1}{w_h \cdot w_w} \sum_{i=1}^{w_h} \sum_{j=1}^{w_w} I_{W_{i,j}} w_{i,j}, \tag{4}$$

For this equation we may consider, approximately, a computational complexity of $\mathcal{O} \approx 2(w_h \cdot w_w)$ operations. Desconsidering borders and making an approximation, the whole process does the correlation operation over the whole image (Figure 3), that is, $M \times N$ times. Hence, the number of operations raise, and we can write the equation of computational complexity $\mathcal{O}_{CC}$ of the detection process using correlation as:

$$\mathcal{O}_{CC} = M \cdot N(w_h \cdot w_w) \cdot 2 \tag{5}$$

Regarding the FFT, it is known [9] that this transform has a computational complexity of

$$\mathcal{O}_{FFT} = M \cdot N \log_2(M \cdot N) \tag{6}$$

operations. Considering that the block diagram of Figure 6 contains two FFT's e one IFFT (which has the same computational complexity of the FFT), we may determine the computational complexity $\mathcal{O}_{Freq}$ of the whole process as:

$$\mathcal{O}_{Freq} = 3 \cdot M \cdot N \log_2(M \cdot N) \tag{7}$$

From equations (5) and (7) the graph in Figure 7 may be built. In this figure, the upper line represents the $\frac{\mathcal{O}_{CC}}{\mathcal{O}_{Freq}}$ ratio, with fixed block dimensions. The lower line represents the $\frac{t_{CC}}{t_{Freq}}$ ratio, obtained from experimental results, where t_{CC} is the processing time of the spatial domain search, and t_{Freq} is the processing time of frequency domain search. Although there is a scale difference, a similar behavior from the two curves is noted, decreasing as the image size increases. Equaling equations (5) and (7), image dimensions for which both techniques have the same performance (that is, $\frac{\mathcal{O}_{CC}}{\mathcal{O}_{Freq}} = 1$) can be estimated, as a function of w_h e w_w:

$$M \cdot N = 2^{\frac{2(w_h \cdot w_w)}{3}} \tag{8}$$

3.2 Optimization Process

The coding scheme proposed in [7] consists of an one-to-many mapping to code a string S to k positions p_j $(j = 1, 2, ..., k)$ in the image. It is suggested that instead of having only one single set Q of positions representing S, we

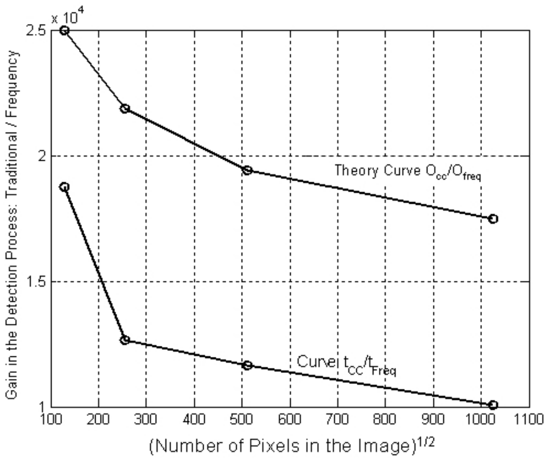


Figure 7: Computational complexity ratio $\frac{\mathcal{O}_{CC}}{\mathcal{O}_{Freq}}$ and processing times ratio $\frac{t_{CC}}{t_{Freq}}$, as a function of image size.

have q sets, where $\{q \in \mathbb{Z} \mid q > 1\}$. As an clarifying example, one could have the following options Q_i $(i = 1, 2, ..., q)$ as where to insert the watermarks when embedding S, for $k = 2$ and $q = 5$. (Fig. 8)

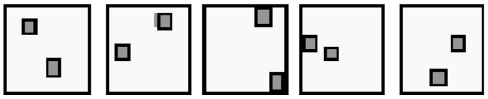
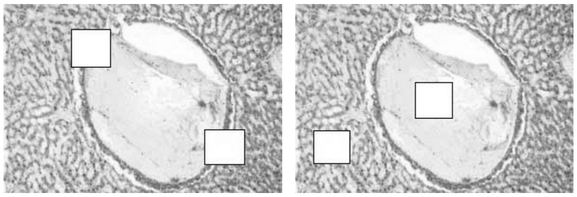


Figure 8: Illustration of different watermark sets representing the same bit string for $q = 5$ and $k = 2$.

Having these q options allows the choice of the best Q_i to be made in terms of fidelity and detection performance of the watermark. Also, for various reasons, it may be interesting to keep some regions of the image totally distortion free, as for example, the membrane of the cell in Fig. 9. One will choose the set depending on the watermark requirements, and we propose here the use of Pareto optimization method [8] to make this choice. Usually, there exists a trade-off among the different properties of watermarking. Using Pareto optimization, the trade-off is represented by the angle α in Fig. 10. In this figure, an example of set selection is given, with set 1 or set 4 being selected (depending on the angle α). A fidelity measure for each of the sets can be obtained using Watson's perceptual model [3], for example. For robustness, the result of the correlation can be used, as a higher correlation means more robustness to the watermark, regarding additive white Gaussian noise (AWGN).



(a) (b)

Figure 9: Example of how a set 9(a) can be more suitable than the other 9(b), where both represent the same bit string to be embedded.

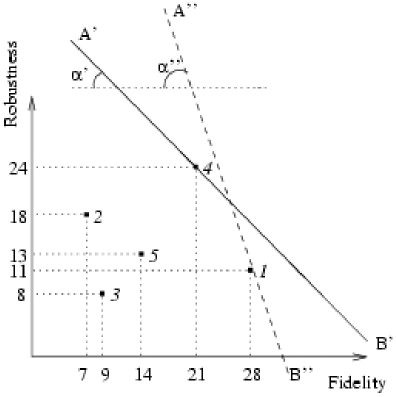


Figure 10: Selection of the best set (among five) using Pareto method.

3.3 Choosing the watermark

As mentioned before, PBW allows a choice of the watermark, so the best alternative regarding detection (and consequently robustness to AWGN, for example) can be selected. To do so, it can be created a set of watermark candidates, and due to the informed insertion, the best performance watermark can be embedded.

Let W be a set of t watermarks w_i $(i = 1, 2, ..., t)$, where t is the number of available watermarks and $\{t \in \mathbb{Z} \mid t > 1\}$. It is desired that if a given watermark w_i does not have an acceptable detection (correlation value), another w_j $(j \neq i)$ may have. In order to maximize the probability this will occur, these watermarks should be orthogonal to each other. It is known that randomly generated sequences usually tend to be close to orthogonal [10], so a good set W can be formed by pseudo-randomly generated watermarks w_i. Additionally, the more available watermarks to choose from, the greater the probability of having higher correlation at detection, that is

$$\begin{aligned} Prob(\max\{\langle I_w, w_i\rangle\} > T) \quad &> \\ Prob(\max\{\langle I_w, w_j\rangle\} > T) & \end{aligned} \tag{9}$$

for $i = 1, 2, ..., t$ and $j = 1, 2, ..., t'$ with $t > t'$. $\langle I_w, w_i \rangle$ represents the correlation between image I_w and watermark w_i. On the other hand, having a very large number t of usable watermarks may become computationally inefficient, since many correlations have to be calculated and compared prior to the final choice and embedding. Fig. 11 illustrates that as the number t of available watermarks grows, on average, the detection measure does increase as well (in accordance to (9)), but tends to stabilize after a given point. For this reason, a good set W could have $t = 20$, for example. That is, it could be formed by 20 sequences pseudorandomly generated, allowing good detection and robustness.

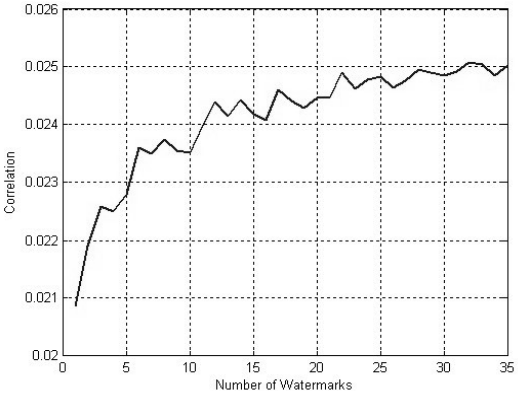


Figure 11: Influence of the number of available watermarks in the detection value

4 Fingerprinting and Robustness to Collusion Attacks

Fingerprinting is considered one importante application of watermarking systems [2], in which illegal copies of a Work can be traced. In this application, the owner embeds different watermarks in the copies of the same data supplied to different customers. Fingerprinting can be considered similar to embedding a different serial number to each customer, in order to identify customers who have broken their license agreement. In the case of image data, each user U_i receives a watermarked image I_{W_i}.

Collusion attacks have recently been of great concern when dealing with watermarking security [4] in fingerprinting applications. In this attack, C different users average their C watermarked images (Figure 12), resulting in the reduction of the watermark energy. As a result, the signature watermark may become undetectable, depending on how many images C were in the attack. Detailed information about collusion attacks is present in [4].

In this context, we show that PBW, due to its distinguished approach, can be set to be more resilient collusion attacks in fingerprinting applications, when compared

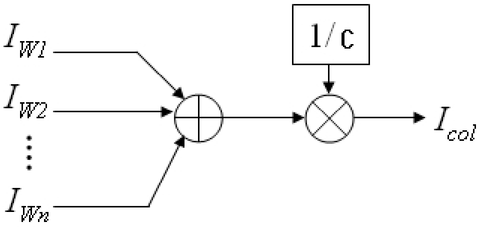


Figure 12: Block diagram of linear collusion attack by averaging.

with spread spectrum techniques (basic model presented in [1]). As it has already been extensively discussed in this paper, PBW does not modify the whole image, but only small parts of it. Furthermore, for the same image, different users tend to have signatures watermarked in different regions of the image with high probability, considering that $w_h \cdot w_w \ll M \cdot N$.

Considering $\bar{I_0}$ a vector of length $M \cdot N$ containing the elements of the host image. A multi-bit message $\bar{B}$ of length L is to be embedded into I_0.

$$\bar{B} = [B_1, B_2, \ldots, B_L], B_j \in \{-1, +1\} \qquad (10)$$

As a review, in the case of CDMA watermarking, to obtain a watermark vector $\bar{W}$ of length $M \cdot N$ carrying the L-bit message, a set $\mathcal{P}$ of L reference marks is created. Each reference mark $\bar{P_j}$ is a pseudo-random sequence of length $M \cdot N$.

$$\mathcal{P} = \{\bar{P_1}, \bar{P_2}, \ldots, \bar{P_L}\} \qquad (11)$$

$$\bar{P_j} = [P_{j1}, P_{j2}, \ldots, P_{jM \cdot N}], P_{ji} \in \{-1, +1\} \qquad (12)$$

The pseudo-random sequence elements P_{ji} are random numbers assuming -1 or +1 with equal probability. Ideally, for CDMA, the pseudo-random sequences of the set $\mathcal{P}$ should be orthogonal to each other. These pseudo-random sequence are generated from a key κ that should be known by both the embedder and the detector, such that they can generate the same set $\mathcal{P}$.

By equation (13) the L-bit message $\bar{B}$ is spread into a $M \cdot N$-dimensional sequence $\bar{W}$ corresponding to the watermark vector. The gain factor K determines the watermark magnitude.

$$\bar{W} = K \cdot \sum_{j=1}^{L} B_j \cdot \bar{P_j} \qquad (13)$$

The watermarked image vector $\bar{I_W}$ is finally obtained with equation (14):

$$\bar{I_W} = \bar{I}_0 + \bar{W} \tag{14}$$

Let $\langle \bar{a}, \bar{b} \rangle$ be the correlation between vectors $\bar{a}$ and $\bar{b}$. Considering the use of correlation to detect the watermark, a decision variable D_j is given by:

$$D_j = \langle \bar{I}_W, \bar{P}_j \rangle = \frac{1}{M \cdot N} \sum_{i=1}^{M \cdot N} I_{W_{(i)}} \cdot P_{j(i)} \tag{15}$$

in which j represents the pseudo-random sequence index and i represents the vector element index.

Let $\bar{I}_{Col}$ be an attacked (by collusion) version of $\bar{I}_W$:

$$\bar{I}_{Col} = \frac{1}{C} \sum_{k=1}^{C} \bar{I}_0 + \frac{1}{C} \sum_{k=1}^{C} \bar{W}_k \tag{16}$$

Considering a collusion attack, from equation (15):

$$\begin{aligned} D_j &= \langle \bar{P}_j, \bar{I}_{Col} \rangle \\ &= \langle \bar{P}_j, \frac{1}{C} \left(\sum_{k=1}^{C} \bar{I}_0 + \sum_{k=1}^{C} \bar{W}_k \right) \rangle \\ &= \langle \bar{P}_j, \left[\bar{I}_0 + \frac{1}{C} \sum_{k=1, k \neq \alpha}^{C} \bar{W}_k + \frac{1}{C} \cdot \bar{W}_\alpha \right] \rangle \end{aligned} \tag{17}$$

in which α is a constant and $\bar{P}_j \in \bar{W}_\alpha$. Appropriately using the distributive property of $\langle , \rangle$:

$$\begin{aligned} D_j \;=\; & \langle \bar{P}_j, \bar{I}_0 \rangle + && \text{(A)} \\ \langle \;\; & \bar{P}_j, \frac{1}{n} \sum_{k=1, k \neq \alpha}^{n} \bar{W}_k) \rangle + && \text{(B)} \\ \langle \;\; & \bar{P}_j, \frac{1}{n} \bar{W}_\alpha \rangle && \text{(C)} \end{aligned} \tag{18}$$

Regarding (A):

For CDMA, A = τ (constant).

For PBW, A = min$\{\langle \bar{P}_i, \bar{I}_0 \rangle\}$, $i = 1, 2, \ldots, t$, where $\bar{P}_i$ is chosen from the watermark set W.

Regarding (B):

For PBW, B = 0 with probability p_n (defined later).

For CDMA, B>0, due to the interference among the L $\bar{P}_j$ sequences.

Regarding (C):

Normalizing, C = 1 for PBW, since $\bar{W}_\alpha = \bar{P}_j$.

Normalizing, C ≈ 1 for CDMA, due to equation (14).

In order to achieve B = 0 in equation (18) using PBW, when adding two or more images together in a collusion attack, superposition of the watermark blocks of one image over the watermark blocks of another image is not allowed, as this superposition may act as interference (as occurs in spread spectrum watermarking). It is shown next that PBW can indeed have a very low probability of mixing different watermarks from different users.

Consider the grid shown in Figure 1 with two blocks inserted in it. As mentioned, the grid itself represents a digital image and the blocks represent watermarks inserted in this image. Let block A_1 be one of the marked blocks of the grid shown in Figure 1. Let the grid have dimensions $M \times N$ and let the marked block A_1 have dimensions $w_h \times w_w$. Consider that the Ref of an additional block B_1 may be located at any of the $M \cdot N$ image pixels with equal probability. In an geometric analysis, we find that the probability p_n $\{0 \leq p_n \leq 1\}$ of absence of watermark blocks superposition is given by

$$p_n \geq 1 - k^2 \cdot \frac{(2 \cdot w_h - 1) \cdot (2 \cdot w_w - 1)}{M \times N} \cdot (C - 1) \tag{19}$$

The symbol $\geq$ is used because p_n depends on the positions of the blocks, so equation (19) represents the worst case situation, considering no interference. On the other hand, the probability of occurring complete block superposition is given by

$$p_y = \left(\frac{k^k}{(M \cdot N)^k} \right)^{C-1} \tag{20}$$

representing the probability p_y $\{0 \leq p_y \leq 1\}$ of occurring the complete superposition of the k watermark blocks of C images. This would be the case in which, similarly to CDMA watermarking, full superposition (and consequently maximum interference) of the watermarks occurs.

5 Experiments

Although PBW can be applied in any domain (spatial, frequency, wavelet), we present here a comparison with the existing CDMA [1] method in the spatial domain. It should be noted that many of the tools (pre-filtering, masking, etc) that can be used in CDMA watermarking may be used for PBW as well.

5.1 Fidelity

In the experiment, for a fair comparison, we tune both techniques (PBW and CDMA) to the same capacity (28 bits) and fix an unique gain K just strong enough to assure successful detection in the 250 test images. The other parameters were:

- Dimensions of watermarked images: 256×256
- Dimensions of watermark blocks used: 32×32
- Number k of blocks used: $k = 2$

Table 1: Fidelity Comparison: Watson Perceptual Model$^\diamondsuit$ SNR$^\bigstar$

Amount of Distortion		
Image	Proposed Method	Spread Spectrum
Lena	0.0040$^\diamondsuit$ 42.03$^\bigstar$	0.0746$^\diamondsuit$ 29.52$^\bigstar$
Barbara	0.0037$^\diamondsuit$ 43.32$^\bigstar$	0.0722$^\diamondsuit$ 30.81$^\bigstar$
Peppers	0.0042$^\diamondsuit$ 43.97$^\bigstar$	0.0726$^\diamondsuit$ 31.41$^\bigstar$
F-16	0.0030$^\diamondsuit$ 46.38$^\bigstar$	0.0610$^\diamondsuit$ 33.87$^\bigstar$
Sailboat	0.0031$^\diamondsuit$ 44.23$^\bigstar$	0.0632$^\diamondsuit$ 31.74$^\bigstar$
AVERAGE	0.00391$^\diamondsuit$ 43.50$^\bigstar$	0.0720$^\diamondsuit$ 32.14$^\bigstar$

Table 2: Fidelity Comparison: Watson Perceptual Model$^\diamondsuit$ SNR$^\bigstar$

Amount of Distortion		
Image	Informed PBW	Blind PBW
Lena	0.0040$^\diamondsuit$ 42.03$^\bigstar$	0.0063$^\diamondsuit$ 37.95$^\bigstar$
Barbara	0.0037$^\diamondsuit$ 43.32$^\bigstar$	0.0057$^\diamondsuit$ 39.24$^\bigstar$
Peppers	0.0042$^\diamondsuit$ 43.97$^\bigstar$	0.0068$^\diamondsuit$ 39.89$^\bigstar$
F-16	0.0030$^\diamondsuit$ 46.38$^\bigstar$	0.0048$^\diamondsuit$ 42.30$^\bigstar$
Sailboat	0.0031$^\diamondsuit$ 44.23$^\bigstar$	0.0049$^\diamondsuit$ 40.15$^\bigstar$
AVERAGE	0.00391$^\diamondsuit$ 43.50$^\bigstar$	0.0054$^\diamondsuit$ 40.33$^\bigstar$

- Number q of option sets, for the informed insertion: $q = 4$

- Number t of watermarks in the set W, for the informed insertion: $t = 20$

Having assigned these parameters, we compare both systems regarding fidelity. Results of Table 1 illustrate that informed PBW does offer both a higher SNR and a higher measure according to Watson's perceptual model, illustrating that fidelity can be one of its main advantages. The AVERAGE field represents the average of results for 250 test images.

Table 2 shows results of another experiment, in which informed insertion PBW is compared with the previously proposed [7] blind insertion PBW.

5.2 Robustness

In another experiment, both the CDMA and PBW methods were tuned to the same capacity and fidelity. The methods are now compared regarding robustness to non-malicious attacks. Often, non-malicious attacks can be approximated by the addition of additive white Gaussian noise (AWGN) to an image [1], justifying its use in the experiment. For each of the 250 test images, AWGN was added, with increasing variances (steps of 0.002). Results presented in Figures 13 and 14 illustrate that for the same noise energy, PBW has a better detection performance than CDMA watermarking. In these figures, the horizontal axis indicate the noise variance, and the vertical axis indicate how many, out of the 250 test image, had their watermarks successfully detected.

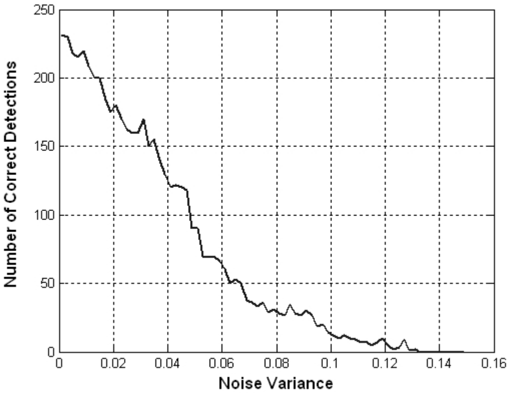


Figure 13: Number of images with correct detection as a function of noise variance, for the PBW method.

For an image severely damaged (AWGN with variance 0.04), in PBW about 50% (125 out of 250) of the watermarks were sucessfully detected. In CDMA, for the same noise energy, less than 10% of the images had their respective watermarks correctly detected.

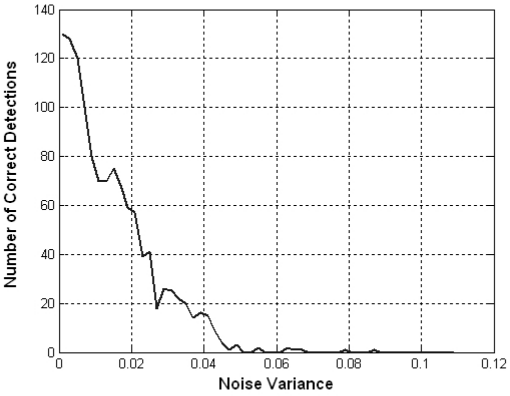


Figure 14: Number of images with correct detection as a function of noise variance, for the CDMA method.

5.3 Collusion Attacks

Results of an experiment comparing CDMA and PBW regarding robustness to collusion attacks are shown in Figure 15. In this figure, the horizontal axis indicates the tested image. The vertical represents the number C of images included in the attack. The marks indicate the maximum value of C for which the systems present a perfect detection.

A superior performance of the PBW method is noted, in agreement with the analysis of Section 4.

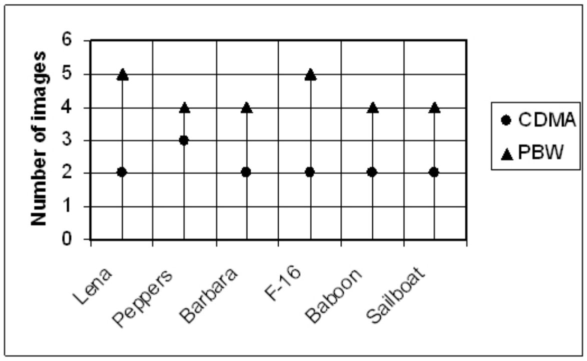


Figure 15: Comparison between CDMA and PBW, regarding robustness to collusion attacks.

6 Conclusions

In this paper, we have proposed an informed insertion method for the innovative PBW technique. We have introduced an optimization issue involving the choice of the best positions to make an insertion. Results have shown that under circumstances where complete fidelity of specific regions of the image is a major issue, PBW has better performance in comparison to standard CDMA. We also argue that PBW may be more robust to AWGN and collusion attacks, as illustrated by the experimental results. Future study includes a metric to determine the ideal number of sets to have available in the optimization process, as the greater the number of sets, the lower the capacity. In addition, future work may extend the PBW method to audio or video watermarking.

Acknowledgments

This work was supported by CNPq, Grants Nos. 55164/01-1 and 550658/02-5.

References

[1] Ingemar J. Cox, Matthew L. Miller and Jeffrey A. Bloom, *Digital Watermarking*, Morgan Kaufmann, 2002.

[2] Gerhard C.Langelaar, Iwan Setyawan and Reginald L. Lagendijk, “Watermarking digital image and video data”, *IEEE Signal Processing Magazine*, vol. 17, no. 5, pp. 20-46, 2000.

[3] A. B. Watson, “DCT quantization matrices optimized for individual images,” *Human Vision, Visual Processing, and Digital Display IV*, SPIE 1913:202-216, 1993.

[4] M.Wu, W. Trqappe, Z. Wang, and K.J. Ray Liu, “Collusion-resistant fingerprinting for multimedia,” *IEEE Signal Processing Magazine*, vol. 21, no. 2, pp. 15-27, March 2004.

[5] J.Mayer, A.V.Silverio and J.C.M.Bermudez, “On the Design of pattern sequences for spread spectrum image watermarking”, *International Telecommunications Symposium* (ITS2002), 2002.

[6] R.B. Wolfgang, C.I. Podilchuk and E.J. Delp, “Perceptual watermarks for digital images and video,” *Proc. IEEE*, vol. 87, pp. 1108-1126, July 1999.

[7] P. V. K. Borges and J. Mayer, “Position Based Watermarking” *IEEE Proc. of 3rd International Symposium on Image and Signal Processing and Analysis - 2003 ISPA Conference*, 2003.

[8] Winston, Wayne L., *Introduction to Mathematical Programming: applications and algorithms*, Duxbury Press, 1995.

[9] R.C.Gonzalez and R.E.Woods. *Digital Image Processing*. Addison-Wesley, 1992.

[10] T. M. Cover, J. A. Thomas. *Elements of Information Theory*. New York: John Wiley & Sons, 1991.