A ROBUST IMAGE WATERMARKING TECHNIQUE BASED ON SPECTRUM ANALYSIS AND PSEUDORANDOM SEQUENCES

Anastasios L. Kesidis and Basilios Gatos
Computational Intelligence Laboratory, Institute of Informatics and Telecomunications
National Center for Scientific Research "Demokritos", GR-153 10 Agia Paraskevi, Athens, Greece
akesidis@iit.demokritos.gr, bgat@iit.demokritos.gr

Keywords: Image watermarking, invisible watermark, blind watermarking, pseudorandom noise sequences, geometric distortions, attacks, data hiding, information embedding.

Abstract: In this paper a watermarking scheme is presented that embeds the watermark message in randomly chosen coefficients along a ring in the frequency domain using non maximal pseudorandom sequences. The proposed method determines the longest possible sequence that corresponds to each watermark bit for a given number of available coefficients. Furthermore, an extra parameter is introduced that controls the robustness versus security performance of the encoding process. This parameter defines the size of a subset of available coefficients in the transform domain which are used for watermark embedding. Experimental results show that the method is robust to a variety of image processing operations and geometric transformations.

1 INTRODUCTION

Nowadays the size of the available digital media is increasing rapidly. This fact leads to an urgent need for an efficient copyright protection of the digital content. Digital image watermarking can offer copyright protection of image data by hiding copyright information in the original image. Image watermarks may be visible or invisible, where a visible watermark is easily detected by observation while an invisible watermark is designed to be transparent to the observer and detected using signal processing techniques. In the literature, there are two main invisible watermarking categories: (i) spatial domain watermarking and (ii) spectrum domain watermarking. In the spatial domain watermarking, the watermark is embedded by directly modifying the pixels of an image (Kimpan, 2004, Hyung, 2003). Spectrum domain techniques are applied to transform domains such as the Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT) and Discrete Wavelet Transform (DWT). Cox et al. (Cox, 1997) have proposed a watermarking technique based on embedding a watermark in the DCT domain using the concept of spread spectrum communication. In order to obtain a robust watermark, the watermark is embedded in the low-frequency components of the image. The technique proposed in (Alturki, 2000) is based on modifying the sign of a subset of low frequency, image transform coefficients (DCT, DFT and Hadamard transforms) with high to moderate magnitudes. In (Dugad, 1998), the spread spectrum image watermarking technique in the DWT domain is proposed. A watermark with a constant weighting factor is embedded into the perceptually significant coefficients in the high frequency sub bands in order to preserve invisibility. In (Kumsawat, 2005), the spread spectrum image watermarking algorithm using the discrete multi wavelet transform is proposed. In this approach, performance improvement with respect to existing algorithms is obtained by genetic algorithms optimization.

In this paper a watermarking scheme is presented that uses the frequency domain in order to embed a watermark that is previously encoded using pseudorandom noise sequences. In order to increase the security of the watermarking process a parameter of the algorithm defines a subset of randomly selected frequency coefficients where the watermark will be embedded. Furthermore, the proposed method determines the longest possible pseudorandom sequence that corresponds to each watermark bit for a given number of candidate coefficients in order to increase the method's robustness. The parameter of the algorithm that defines the number of watermarked coefficients also controls the robustness versus security performance of the encoding process. Several experimental results show that the watermarked images are robust to a variety of image processing operations and geometric transformations. The rest of the paper is organized as follows: section 2 provides a brief introduction to pseudorandom noise sequences and section 3 determines the coefficients of the frequency domain where the method is applied as well as the parameters that control the performance of the embedding method. Sections 4 and 5 present the embedding and the detection algorithm, respectively. Section 6 provides some experimental results while section 7 concludes the paper.

2 PSEUDORANDOM NOISE SEQUENCES

The watermark is embedded in the form of a pseudorandom noise (PN) sequence. (PN) sequences are binary sequences that appear to be statistically random and have properties similar to random sequences generated by sampling a white noise process. (PN) sequences are generated by pseudorandom number generators using an initial seed (key). There are several such utilizations including GoldCodes, m-sequences, Legendre sequences and perfect maps (O'Ruanaidh, 1998). Different keys produce different sequences thus, unless the algorithm and key are known, the sequence is impractical to predict. If the key consists of K registers then a sequence is a maximal length sequence if it has length 2^K-1. Maximal length sequences have pseudo-randomness properties i.e. over one period, there are 2^{K-1} ones and $2^{K-1}-1$ zeros (Luby, 1996). Moreover, the autocorrelation function is binary valued. Specifically, for a sequence $p_1\ p_2 \ldots p_N$ of period N the autocorrelation function, $R_{xx}(k)$, is

$$R_{xx}(k) = \frac{1}{N}\sum_{n=1}^{N} p'_i p'_{i+k} \tag{1}$$

where $p'_i = 1-2p_i$ and k represents the k-th shifted version of the sequence. The value of $R_{xx}(k)$ equals 1 if k=0 and $-1/N$ otherwise. In other words, the sequence produced by the generator is uncorrelated to all of its circular shifts for $k\neq 0$.

Let us suppose that a watermark W is a binary message $b_1\ b_2\ \ldots\ b_L$ consisting of L bits. Each symbol b_i is encoded to a zero mean pseudorandom vector of length N. Since there are two states for each symbol b_i, therefore two (PN) sequences of length N are used, the first one corresponding to state 0 and its complementary to state 1.

Corresponding each symbol b_i to its (PN) sequence produces the spread spectrum encoded watermark W_s which is a binary sequence of length.

$$L_s = NL \tag{2}$$

The spread spectrum version W_s of the watermark forms a symmetric key cryptosystem since in order to embed or extract the watermark, it is necessary to know the key used to generate the pseudorandom sequences.

3 THE 2D FOURIER TRANSFORM

Let $I(x,y)$ denote the original image defined on a integer grid where $0\leq x<N_x$ and $0\leq y<N_y$. The two dimensional discrete Fourier transform (DFT) of I is

$$F(u,v) = \sum_{x=0}^{N_x-1}\sum_{y=0}^{N_y-1} I(x,y)e^{-2\pi jux/N_x - 2\pi jvy/N_y} \tag{3}$$

The watermark is embedded in the magnitude $M(u,v)=|F(u,v)|$ of the Fourier transform. Its phase $P(u,v)=\angle\ F(u,v)$ is not affected but only used during the inversion of the 2D DFT.

Let us assume that the center of the 2D DFT transform corresponds to the zero frequency term. Let also $R\subset M$ the set of coefficients where the watermark is embedded. R corresponds to a ring determined by radius r_1 and r_2 with $0<r_1<r_2<N_R$ where $N_R = min\{N_x,N_y\}/2$. The values for r_1 and r_2 must be chosen so that the image deformation produced by the embedding process is minimal. The most proper area to embed the watermark is the middle frequencies of the spectrum since small radius values affects the low frequencies leading to visibly image distortions while high radius values affect the higher frequencies that are most sensitive to compression attacks (Cox, 1997). It is,

$$R = \{M(u,v):\ r_1 \leq \sqrt{u^2+v^2} \leq r_2\} \tag{4}$$

In the proposed method the values of r_1 and r_2 are in the range $0.5N_R \leq r_1, r_2 \leq 0.8N_R$

The number L_R of coefficients that satisfy equation (4) is related to the difference between r_1 and r_2. If the coefficients are sorted according to angle

θ=arctan($\frac{v}{u}$) then R can be considered as a one dimensional signal. However, the magnitude of the Fourier transform is symmetric, that is $R(k)= R(k+L_R/2)$, where $0\leq k<L_R/2$. Therefore, in order to preserve symmetry, the watermark is embedded twice in R. The maximum number of coefficients candidates where each copy of the watermark can be embedded is $L_{RR} = L_R/2$.

In order to increase the security of the embedding process, not all of the L_{RR} candidate coefficients are used in each semi-ring. Instead, a key S_L, provided by the user, is used as seed for a random number generator which selects a subset of coefficients in each semi-ring. The number $\hat{L}_{RR}$ of chosen coefficients, where $\hat{L}_{RR} < L_{RR}$, is a system's parameter and controls the security level. Indeed, the possible combinations of $\hat{L}_{RR}$ elements out of L_{RR} is

$$\binom{L_{RR}}{\hat{L}_{RR}} = \frac{L_{RR}!}{\hat{L}_{RR}!(L_{RR}-\hat{L}_{RR})!} \tag{5}$$

If for example, L_{RR}=1000 and only $\hat{L}_{RR}$=900 elements are used for watermarking then there are about 6.39×10^{139} possible positions where the encoded watermark W_s can be embedded in each semi-ring.

If a maximal length sequence generated by K_m registers is used then according to (2) the longest encoded watermark W_s that fits in has length

$$L_s=NL=(2^{K_m}-1)L \tag{6}$$

The value of K_m is integer and can be calculated as

$$(2^{K_m}-1)L=\hat{L}_{RR} \Rightarrow K_m=\left\lfloor \log_2\left(\frac{\hat{L}_{RR}}{L}+1\right)\right\rfloor \tag{7}$$

where $\lfloor x \rfloor$ denotes the greatest integer less than or equal to x. In the spread spectrum encoded watermark W_s each symbol b_i is replaced by a (PN) sequence of length N.

However, applying a maximal length sequence as above may leave a significant number of candidate coefficients unused. Indeed, according to (7) the maximum number of available coefficients is used only if $\frac{\hat{L}_{RR}}{L}=2^{K_m}$-1. In case where $2^{K_m-1}\leq\frac{\hat{L}_{RR}}{L}<2^{K_m}$-1 there is a total number of $\hat{L}_{RR}-(2^{K_m}-1)L$ unused coefficients. For example, if the watermark string has a typical length L=64 bit and $\hat{L}_{RR}$=1000 coefficients then according to (6) the spread spectrum encoded watermark is L_s=960 bits long. On the other hand, if $\hat{L}_{RR}$=950 then L_s is significantly reduced to L_s=448 which leads to a "loss" of 502 candidate coefficients. In order to avoid this problem a non-maximal length sequence is used instead. In that case, the length of the encoded watermark W_s is

$$L'_s=dL \tag{8}$$

where d equals to $\left\lfloor \frac{\hat{L}_{RR}}{L} \right\rfloor$. The quantity d denotes the first d digits of a (PN) sequence generated by K'_m registers where $K'_m=\left\lceil \log_2\left(\frac{\hat{L}_{RR}}{L}+1\right)\right\rceil$. Symbol $\lceil x \rceil$ denotes the smallest integer greater than or equal to x. In other words, the (PN) sequence is generated by K'_m registers and only d of its digits are used for each symbol b_i. It should be noticed that a maximal length sequence is still achieved if $d=2^{K'_m}$-1.

The above analysis demonstrates that the proper choice of $\hat{L}_{RR}$ is a trade-off between security level and robustness. Clearly, according to (5) the number of possible combinations is maximized as $\hat{L}_{RR}$ reaches $L_{RR}/2$. Thus, the best level of security is achieved if only half of the L_{RR} coefficients are used. On the other side, according to (8), an increased number of used coefficients allows a watermark of greater length to be embedded resulting to a more robust encoding scheme.

4 WATERMARK EMBEDDING

In order to accomplish image watermarking, a watermark W as well as a private key K are required. Key K={ K'_m, $\hat{L}_{RR}$, S_L} consists of the number K'_m of registers in the (PN) sequence generator, the number $\hat{L}_{RR}$ of chosen coefficients and the seed S_L of the random number generator (see section 3).

As already mentioned, due to the symmetry of the Fourier transform domain, the encoded watermark W_s is embedded twice in the ring R of magnitude coefficients. Let $R_{i=1,2}$ denote the two sets of coefficients where the encoded watermark W_s will be embedded, one on each semi-ring. The magnitude of these coefficients is modified as

$$M_w(u,v) = M(u,v) + g\ W_s \qquad (9)$$

where $M(u,v) \in R_{i=1,2}$.

The constant g is a factor that controls the strength of the embedded watermark. The watermarked image $I'(x,y)$ is obtained by applying the inverse Fourier transform

$$I'(x,y) = \frac{1}{N_x N_y} \sum_{x=0}^{N_x-1} \sum_{y=0}^{N_y-1} F'(u,v) e^{2\pi j (ux/N_x + vy/N_y)} \qquad (10)$$

where $F'(u,v) = M_w(u,v) e^{jP(u,v)}$.

5 WATERMARK DETECTION

For the detection of the watermark the private key K={ K'_m , $\hat{L}_{RR}$, S_L} is used and a two step process is applied: First the correlation between the marked (and possibly corrupted due to an attack) coefficients and the watermark itself is computed in order to detect the most probable offset position of the watermark inside each semi-ring. Second, the coefficients are divided into d length sequences and compared to the (PN) sequences used during the embedding process in order to extract the original watermark message.

Specifically, let $F'(u,v)$ denote the DFT transform of a possibly watermarked image and $M'(u,v)$ its magnitude. Let also $R \subset M'$ denote the ring of coefficients determined as in section 3. The encoded watermark W_s is constructed from the pseudorandom sequence generator using the same number of registers K'_m as in the encoding phase. Additionally, in each semi-ring the set $R_{i=1,2}$ of $\hat{L}_{RR}$ coefficients where the watermark may be embedded is determined using the same random seed S_L as during the embedding phase.

In order to detect the watermark even in a rotated image the embedded watermark is cross-correlated with all possible shifts of the extracted watermark. Indeed, according to the rotation property of the Fourier transform, rotating the image through some angle in the spatial domain causes the rotation of the Fourier transform space by the same angle (O'Ruanaidh, 1998). The correlation between R_i and W_s is given by

$$C_{RW}(m) = \begin{cases} \sum_{n=0}^{N-m} R_i(n+m) W_s(n) & 0 \le m \le N \\ C_{WR}(-m) & N \le m < 0 \end{cases} \qquad (11)$$

where $N = \hat{L}_{RR}$ -1. The shifted position of the maximum correlation is at $p = \arg\max_m (C_{RW})$. If $p \neq 0$ then W_s is shifted p times in order to match R_i. The set R_i of coefficients in each semi-ring contains L (PN) sequences each one of length d. The correlation of the k-th sequence in R_i and W_s where k=1… L, can be estimated by the Pearson correlation coefficient

$$r_k = \frac{\sum_{j=1}^{d} (R_i(k,j) - \overline{R}_i(k))(W_s(k,j) - \overline{W}_s(k))}{(d-1) s_{R_i}(k) s_{W_s}(k)} \qquad (12)$$

where $R_i(k,j)$, $W_s(k,j)$ denote element j of the k-th sequence in R_i and W_s, respectively, while $\overline{R}_i(k)$ and $\overline{W}_s(k)$ denote their sample mean values. The quantities $s_{R_i}(k)$ and $s_{W_s}(k)$ denote the standard deviation of R_i (k) and $W_s(k)$. Clearly, the closer the coefficient r_k is to 1, the stronger the correlation between the sequences R_i (k) and $W_s(k)$. The extracted watermark W' is calculated by applying the above estimation process to all L (PN) sequences of R_i. As already mentioned in section 2 there are two (PN) sequences used for encoding W_s, the first one corresponding to state 0 and its complementary to state 1. Thus, if r_k>0 then the k-th bit of watermark W' is set to the state of the (PN) sequence $W_s(k)$ otherwise to its complementary.

6 EXPERIMENTAL RESULTS

This section presents some experiments that demonstrate the robustness of the proposed algorithm against common image processing operations and geometric transformations.

As already mentioned in section 3 the number of randomly selected coefficients $\hat{L}_{RR}$ is an important parameter in the proposed watermarking scheme since it affects both the security level and robustness of the method. As an example, Table 1 presents the recovery performance in two cases where different amounts of coefficients are selected in each semi-ring. In both cases the standard test Lena image is used and a watermark message of 96 bits is embedded. The ring's radius is intentionally chosen about 80% of the 2D DFT domain radius which corresponds to high frequencies that are very sensitivity to compression attacks but provide better visual results since the embedding process leaves the image perceptually unmodified. The capacity of each semi-ring is L_{RR}=648 coefficients. In the fist case, the 90% of these coefficients are randomly chosen i.e. $\hat{L}_{RR}$=583. Thus, the total number of coefficients used is L_s=576 which corresponds to a (PN) sequence of 6 symbols per watermark bit. In the second case, the 60% of these coefficients are used that is $\hat{L}_{RR}$=388 corresponding to L_s=384 and a (PN) sequence of 4 symbols per watermark bit. As shown in Table 1, there is a significant loss of robustness comparing the two implementations. For instance, for a Jpeg compression factor of 70% the percent of bit correctly recovered falls from 75% to 65%. On the other hand the security level is significantly raised. Indeed, according to (5) the possible positions in each semi-ring where the encoded watermark W_s can be embedded raises from 2.47×10^{90} in the first case up to 7.42×10^{187} in the second one. If, however, the maximal length (PN) sequence were used then according to (6) only 3 symbols per watermark bit would be used. Clearly, as shown in the last column of Table 1, this decreases further the recovery performance.

Table 1: Percent of recovered bits for two different sets of selected coefficients.

Jpeg factor	90% (6 symbols/bit)	60% (4 symbols/bit)	maximal length (PN) (3 symbols/bit)
90	92	89	85
70	75	65	51
50	59	53	50
30	61	51	47

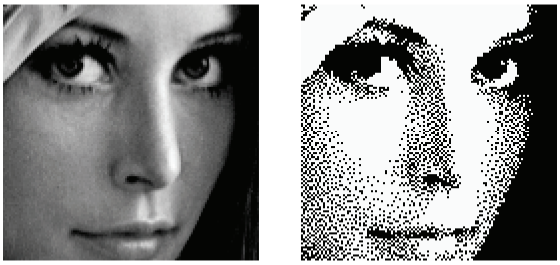
Embedding the watermark using the longest possible (PN) sequence allows sufficient recovery even when several possible attacks are applied to the watermarked image. For the following experiments the standard test images Lena and Baboon were used, both of size 512×512. The ratio $\hat{L}_{RR} / L_{RR}$ is set up to 0.85 and the ring is located at radius $0.6N_R$. The gain factor g is set to 5 in both cases. Table 2 provides the bits recovery percentage when Jpeg compression is applied to the watermarked image.

Table 2: Jpeg compression results.

CF	Lena	Baboon	CF	Lena	Baboon
100	100	100	50	97	100
90	100	100	40	92	100
80	100	100	30	91	100
70	100	100	20	75	100
60	100	100	10	61	94

The 90% of the watermark is retrieved for compression factors (CF) down to 30 which correspond to significantly degraded images. Apparently, the watermark in the Baboon image appears robust even for CF about 10.

Figure 1 depicts a sub-area of the Lena image in two color depth resolutions. The left watermarked image is without color reduction while on the right one the color depth is reduced to 2 colors leading to a black & white version of the image. The watermark is successfully extracted with only 3 wrong bits out of 64 (95% success). Furthermore, in the Baboon image the watermark is exactly retrieved.



(a) (b)

Figure 1: Color depth reduction results. (a) original image (b) black & white (2 colors). The watermark is successfully detected in both versions.

The method's robustness has also been tested on resized and cropped images. Table 3 summarizes the corresponding watermark retrieval results. Similar cropping results have been achieved when an additional offset of (100,100) pixels from the image's center is applied.

Table 3: Percent of recovered bits for several resize and crop attacks.

Resize			Crop		
%	Lena	Baboon	%	Lena	Baboon
200	100	100	90	100	100
150	100	100	80	100	100
70	100	100	70	98	100
50	97	98	60	98	98
30	58	59	50	91	84

Another common attack on watermark images is stretching. Figure 2 depicts several stretched versions of the Lena image. The detection process can correctly retrieve the watermark even for stretching ratios up to 170%×50%. In the extreme case of ratio 60%×180% only 3 bits out of 64 are incorrectly retrieved from the Lena image.

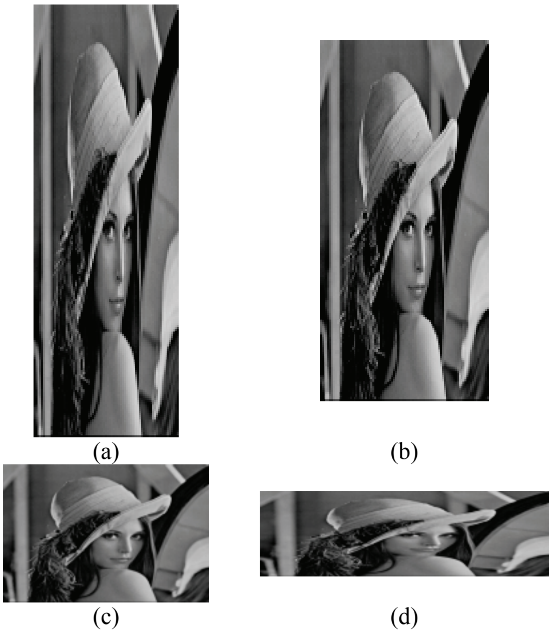


Figure 2: Several aspect ratios applied to Lena image. (a) 60%×180%, (b) 70%×150%, (c) 120%×80% and (d) 170%×50%.

7 CONCLUSIONS

In this paper a watermarking scheme is presented that uses randomly chosen coefficients along a ring in the transform domain in order to embed a watermark message. The watermark is constructed using non maximal pseudorandom sequences so that each watermark bit is encoded by the longest possible pseudorandom sequence. Furthermore, an extra parameter is introduced that defines the amount of randomly chosen coefficients which are used for watermark embedding. If higher security levels are required then a fewer number of coefficients should be used. On the other hand more watermark coefficients lead to longer pseudorandom sequences and consequently to an increased robustness of the encoding process. Experimental results show that the method is robust to a variety of image processing operations and geometric transformations like Jpeg compression, color reduction down to black & white, cropping with and without an offset, stretching with aspect ratio modification and resizing. Future work will focus on the adaptive determination of the proper set of frequency coefficients that provides maximal (PN) sequences for a given watermark length.

REFERENCES

Alturki, F. Mersereau, R. 2000. Robust oblivious digital watermarking using image transform phase modulation. In *Proc. of the International Conference on Image Processing*, vol. 2, pp. 84–87.

Cox I. J., Kilian J., Leighton F. T., Shamoon T. 1997. Secure spread spectrum watermarking for multimedia. In *IEEE Transactions on Image Processing*, vol. 6 (12), pp. 1673-1687.

Dugad, R. , Ratakonda, K., Ahuja, N, 1998. A new wavelet-based scheme for watermarking images. In *Proc. IEEE Int. Conf. Image Processing (ICIP 1998)*, vol. 2, pp. 419–423.

Hyung S. K., Heung-Kyu L. 2003. Invariant image watermark using Zernike moments. In *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 13, issue 8, pp. 766–775.

Kimpan, S. Lasakul, A. Chitwong, S. 2004. Variable block size based adaptive watermarking in spatial domain. In *Proc. of the IEEE International Symposium on Communications and Information Technology,* vol. 1, pp. 374–377.

Kumsawat, P., Attakitmongcol, K. 2005. A New Approach for Optimization in Image Watermarking by Using Genetic Algorithms. In *IEEE Transactions on Signal Processing*, vol. 53, no. 12, pp. 4707-4719.

Luby M., 1996. *Pseudorandomness and Cryptographic Applications*. Princeton Univ Press.

O'Ruanaidh J., Pun T., 1998 .Rotation, scale and translation invariant spread spectrum digital image watermarking. In *Signal Processing*, vol. 66, no. 3, pp. 303–317.