COPYRIGHT PROTECTION OF STILL IMAGES USING SELF-SIMILAR CHAOTIC WATERMARKS

Sofia Tsekeridou, Nikos Nikolaidis, Nikos Sidiropoulos and Ioannis Pitas

Department of Informatics
Aristotle University of Thessaloniki
Box 451, Thessaloniki 54006, Greece
e-mail: pitas@zeus.csd.auth.gr

ABSTRACT

A spatial domain watermarking algorithm for still images is proposed in this paper. The watermarks are generated by combining scaled versions of 2-D chaotic signals, in order to attain a self-similar structure. In addition, the 2-D chaotic signal generation procedure contains operations which ensure that lowpass watermarks are obtained. Such characteristics (lowpass spectrum, self-similarity) enable robustness against compression, lowpass filtering or, generally, distortions of lowpass nature, as well as, cropping and scaling. An additional advantage of the proposed algorithm is that the detection procedure does not require the original image.

1. INTRODUCTION

Copyright protection of multimedia data in our fully digital, totally wired era is a very challenging task that drew the attention of both scientists and copyright holders. Data hiding or steganography has emerged as the only viable solution to this problem. Data hiding techniques aim at embedding statistically undetectable and perceptually transparent signals, called watermarks, in digital data (still images, audio, video, etc.). Watermarks carry information about the copyright owner of the host data and can be used to resolve copyright disputes. In order to be of any value for copyright protection, watermarks should be permanently embedded into the digital products, i.e., they should be able to withstand both hostile and unintentional data manipulations.

Several watermarking methods have been proposed so far in the scientific and patent literature. For an overview of the recent advances in the area, the reader can consult [1, 2, 3]. The major drawback of most existing watermarking methods is their sensitivity to geometric distortions inflicted on an image. To cope with such cases, all possible combinations of geometric distortions (scaling, cropping, etc.) that might have been applied on the host signal should be checked during watermark detection. However, the computational complexity of this brute force detection approach is rather prohibiting. In order to deal more efficiently with geometric distortions, one of the following approaches can be implemented:

- Utilization of salient image features as anchor points for watermark embedding and detection.
- Use of watermarks that, due to their special structure and embedding domain, are invariant to geometric distortions.
- Use of watermarks with a structure that results in significant reduction in the space of possible distortions that should be examined during detection.

The method proposed in this paper is based on the last approach. Self-similar watermarks are constructed by combining scaled versions of a 2-D chaotic signal called *base watermark*. Chaotic signals are used due to their controllable spectral and correlation properties by chaotic map related parameters. The watermarks are embedded in the spatial domain and detected by comparing the normalized correlation between the watermarked image and the watermark against a properly selected threshold. Thus, watermark detection does not require the original image. The threshold is evaluated under a desired false alarm probability constraint, i.e., desirable system detection reliability. Watermark detection in geometrically distorted images is conducted by searching the space of possible distortions. The watermark's self-similar structure significantly reduces the size of the search space, thus reducing the computational complexity in the detection stage. Experimental results prove the efficiency of the current approach against various image distortions, such as filtering, compression, cropping and scaling.

2. WATERMARK GENERATION

The watermark signal generation is a three step procedure. A 1-D chaotic signal is initially produced. The 1-D signal is then warped to generate the 2-D base watermark. Finally, the self-similar watermark signal is constructed. The first two steps utilize a methodology similar to the one proposed in [4]. The following subsections describe the watermark generation procedure in more detail.

2.1. 1-D chaotic signal generation

A one-dimensional chaotic map is used to generate 1-D sequences of real numbers:

$$z(n+1) = F(z(n), \lambda) \tag{1}$$

where $n = 0, 1, 2...$ denotes the map iteration index and λ is a system parameter. By thresholding $z(n)$ using an appropriately selected threshold z and multiplying the result with the watermark strength parameter a, a bipolar, zero mean sequence $s(n) \in \{-a, a\}$ is obtained. The chaotic nature of the map guarantees watermark sensitivity to the sequence starting point $z(0)$, low cross-correlation between different watermarks and cryptographical security. The parameter λ can be used to control the mean frequency of the $-a, a$ transitions in $s(n)$ and thus the frequency characteristics of the sequence. Since resistance to lowpass filtering and compression is among the basic requirements of a watermarking scheme, λ values that result in lowpass sequences should be used.

2.2. 2-D base watermark construction

In order to obtain the 2-D base watermark signal W_0, a scanning order, i.e., an algorithm for mapping the 1-D signal $s(n)$ of dimensions $N_W \cdot M_W$ to the 2-D array W_0 having dimensions $N_W \times M_W$, should be chosen. Unfortunately, the obvious choice of raster scanning results in 2-D watermark signals with high frequencies since the frequency content of the initial 1-D sequence cannot be retained in both dimensions in its 2-D version. The following methods result in much smoother 2-D signals:

- *Cellular smoothing*. The 2-D signal resulting from raster scanning is smoothed by applying rules of cellular automata [5], i.e., by moving the a-valued pixels so as to form large uniform neighborhoods.
- *Peano Scan*. Peano space filling curves [6] are applied to construct $W_0(n_1, n_2)$. Watermark generation using Peano scan is very fast compared to cellular smoothing and produces 2-D signals that are sufficiently lowpass.

A combination of cellular smoothing and Peano scan is also possible.

2.3. Self-similar watermark construction

The final step of the watermark generation procedure is to incorporate spatial self-similarity. This is accomplished in the way shown in Figure 1. $W_0(n_1, n_2)$ is decimated $l-1$ times (using nearest neighbor decimation) with decimation factors $1/2, 1/4 \ldots 1/2^{l-1}$ to obtain signals $W_1, \ldots, W_{l-1}$ that, from now on will be called watermark components. With each of these watermark components, we create a watermark layer of dimensions $N_W \times M_W$ by replicating (tiling) it in both the horizontal and the vertical dimension. By superimposing these $l-1$ layers with the base watermark, an l-layered watermark $W(n_1, n_2)$ is generated. It can be proven that such a watermark can be represented by the following expression:

$$W(n_1, n_2) = \sum_{f=0}^{l-1} \sum_{i=0}^{2^f-1} \sum_{j=0}^{2^f-1} W_b(2^f n_1 + i\lceil \frac{N_W}{2^f} \rceil, \; 2^f n_2 + j\lceil \frac{M_W}{2^f} \rceil) \quad (2)$$

It is evident that the watermark dimensions $N_W \times M_W$ are independent of the image size. In order to be embedded in an image, the watermark W is scaled to the image dimensions $N \times M$. The parameters that are necessary for the watermark generation and which represent the final key for detection are $\{z(0), \alpha, N_W, M_W\}$. Watermarks generated using this scheme are non-invertible. This means that even if the attacker could manage to obtain the watermark W, the determination of the corresponding key would be impossible.

3. WATERMARK EMBEDDING AND DETECTION

Watermark embedding takes place in the spatial domain in an additive way:

$$Y(n_1, n_2) = X(n_1, n_2) + W(n_1, n_2) \quad (3)$$

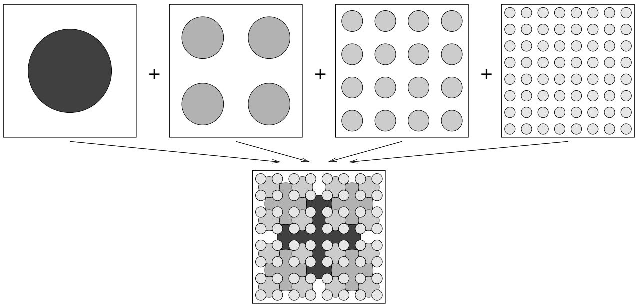

Fig. 1. Self-similar watermark generation procedure.

where X is the original image and Y the watermarked image.

Watermark detection is performed by evaluating the normalized correlation between the watermark signal $W(n_1, n_2)$ and the image under investigation $Y'(n_1, n_2)$

$$c = \frac{\sum_{n_1} \sum_{n_2} Y'(n_1, n_2) W(n_1, n_2)}{\sum_{n_1} \sum_{n_2} W^2(n_1, n_2)} \quad (4)$$

Based on the central limit theorem, it can be safely assumed that c attains a Gaussian distribution for any Y'.

If the image under consideration hosts the watermark W that we are searching for, i.e., if $Y' = X + W$, the mean value of c is equal to one. If the image under investigation contains no watermark ($Y' = X$) or if the image is watermarked with a different watermark from the one we are searching for ($Y' = X + W'$), the mean value of the correlator output is zero. Detection is performed by comparing c against a properly selected threshold T:

Y' is watermarked by W if $c \geq T$

Y' is not watermarked by W if $c < T$.

Threshold T is chosen according to the desired false alarm probability P_{fa} (i.e. the probability to detect a watermark when it does not exist).

For watermark detection in an image that has been subject to geometric distortions, e.g., to a combination of uniform scaling and cropping, the correlation between the image under investigation and the watermark, scaled and shifted using various combinations of scaling factors and shift parameters should be evaluated. The self similar structure of the watermarks generated by our algorithm reduces substantially the search regions required for watermark detection in such cases. Consider for example a system utilizing a 3-layered watermark W of original size $N_W \times M_W$. In such a case, the size of the watermark components would be $N_W \times M_W$ for the base watermark W_0, $N_W/2 \times M_W/2$ for the watermark component W_1 and $N_W/4 \times M_W/4$ for the watermark component W_2. Thus, if the watermark is scaled using all scale factors in the range $[1/k, 1]$, where $k \geq 2$, the dimensions of the base watermark in layer zero will span the range $N_W/k \times M_W/k \leftrightarrow N_W \times M_W$. In the same manner, the dimensions of the four watermark components W_1 in the first layer will span the range $N_W/2k \times M_W/2k \leftrightarrow N_W/2 \times M_W/2$, whereas the sixteen components W_2 of the second layer will span the range $N_W/4k \times M_W/4k \leftrightarrow N_W/4 \times M_W/4$. Thus by scaling the watermark signal using all scaling factors in the range $[1/k, 1]$ we can ensure that all scaled versions of the base watermark W_0 with scaling factors $[1/(k2^{l-1}), 1]$ will be generated. Given the fact that in a watermarked image the base watermark can be found in l scales $1, 1/2, \ldots, 1/2^{l-1}$, it is easy to conclude that by scaling the $N_W \times M_W$ watermark W using all scales in the range $[1/k, 1]$ we can ensure that a match between at least one of the watermark components and a component of the same dimensions in the watermarked image will occur, for all images, where, due to the watermark resizing to the image size prior to embedding or due to a subsequent resizing manipulation, the base watermark exists in any of the scales in the range $[1/(k2^{l-1}), 2^{l-1}]$.

In the case of cropping, watermark detection is performed by scaling the watermark using scales in the range $[1/k, 1]$, generating (for each scaling factor $1/s$) a number of shifted versions of the watermark and checking the correlator output for each of the shifts in both horizontal and vertical directions. However, due to the self similar structure of the watermark, a peak in the correlator output will occur not only when a perfect alignment between the watermark and the cropped image exists but also if a watermark component in one of the layers becomes aligned with a component of one of the layers (same or not) on the watermarked image. The worst case that may happen is the component of the watermark highest layer (layer 0) to get aligned with a component of the watermarked image lower layer (layer $l-1$). In such a case, the horizontal and vertical shift search ranges are the biggest and are equal to $(-\frac{1}{2}\frac{N_W}{s}, \frac{1}{2}\frac{N_W}{s})$ and $(-\frac{1}{2}\frac{M_W}{s}, \frac{1}{2}\frac{M_W}{s})$, respectively. The best case occurs when the components of similar layers get aligned which further means that components of the lowest layer $l-1$ get aligned as well. In such a case, the respective search ranges are the smallest possible: $(-\frac{1}{2}\frac{N_W}{s2^{l-1}}, \frac{1}{2}\frac{N_W}{s2^{l-1}})$ and $(-\frac{1}{2}\frac{M_W}{s2^{l-1}}, \frac{1}{2}\frac{M_W}{s2^{l-1}})$. This is justified bearing in mind that the centers of two such successive components are spaced $N_W/(s2^{l-1})$ pixels apart in the horizontal dimension and $M_W/(s2^{l-1})$ in the vertical dimension. In order not to perform exhaustive search with respect to translation, which will result in no gain whatsoever, search ranges may be initialized with their smallest values and gradually increased until the correlation value exceeds the detection threshold. Obviously, when searching for a watermark in an image that is scaled or cropped (or both) the values expected for the correlator output when a partial match occurs are smaller than the peak that would have been detected when a full match occurs, i.e. smaller than unity, but still sufficiently larger than the detector threshold.

4. SIMULATION RESULTS

A three-layered watermark of size 1024×1024 has been used to mark five different greyscale images of size 960×960. The watermark strength parameter a has been chosen so as to produce watermarked images with SNR 28dB and 34dB. Obviously, the stronger the embedded watermark is, the more visible but robust it tends to be. A threshold that allows for a false alarm probability smaller or equal to 10^{-4} has been selected. The threshold is calculated by testing different watermarks on an image that contains a watermark different from the one that we are trying to detect. When no distortions are present, the detection ratio is evaluated equal to 100%. Watermark detection in linear (mean) and nonlinear (median) filtered images has also been tested. The detection ratios attained are illustrated in Table 1. The method proves robust against mean and median filtering of size 3×3 even for weak watermarks. However, for windows of greater size, its performance deteriorates. Robustness to JPEG compression with different compression ratios has also been studied. Detection results are plotted in Figure 2. The method proves robust even for weak watermarks (34dB) and high compression ratios.

The method has also been successfully tested in scaled and

Table 1. Detection Ratios (%) after mean and median filtering.

SNR	Filter Type			
	Moving Average		Median	
	3×3	5×5	3×3	5×5
28	100	74	100	100
34	100	10.9	100	84.15

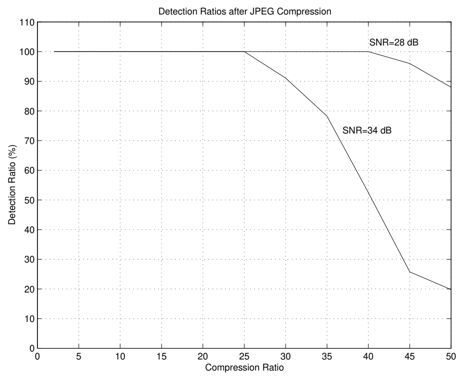

Fig. 2. Watermark resistance to JPEG compression.

cropped images. Its self-similar structure enabled significant reduction in the range of scaling factors and shifts, that should be tested during detection. Uniform scaling is directly dealt with without use of search ranges. This is achieved bearing in mind that the watermark size is independent of the image size. Thus, detection in an image that is apriori known to be a scaled version of the original, involves only watermark resizing to the size of the image under investigation ensuring that both the embedded watermark and the one used in detection are scaled with the same factor. The results obtained after watermarked image scaling with scaling factors in the range $[0.25, 4.0]$ lead to 100% detection ratio for any scaling factor.

Finally, a combination of cropping and scaling requires testing simultaneously a range of scaling factors and horizontal/vertical translations. As already discussed, the scaling factor search range is set to $[\frac{1}{k}, 1.0]$, $k = 2$. In order to test the system's performance in this case, the watermarked image of initial size 960×960 has been cropped to the region $[50 : 850, 80 : 880]$. The cropped image has then been scaled with a scaling factor of 1.5. Figure 3(a) depicts the correlator output for various shifts and a fixed scaling factor $\frac{1}{s} = 0.703125 = 0.75 \times \frac{960}{1024}$, i.e., the correct one. The correlation peak is observed for x translation equal to -75 ($= -50 \times 1.5$) and y translation -120 ($= -80 \times 1.5$). The correlation peak is obtained when the 0th and 1st layers of the test (scaled and shifted) watermark coincide with the 1st and 2nd layers of the embedded one. The shift ranges that have to be tested in this case are $(-\frac{1}{2}\frac{N_W}{s2^1}, \frac{1}{2}\frac{N_W}{s2^1})$ and $(-\frac{1}{2}\frac{M_W}{s2^1}, \frac{1}{2}\frac{M_W}{s2^1})$, i.e., half the ranges required in the brute force approach. Figure 3(b) shows respective correlation values when a different than the embedded watermark is tested. It is easily observed that the correlation peak in Figure 3(a) is significantly greater than any other correlation value. To further test performance, correlation values are shown for different watermark scale factors and horizontal shifts and a fixed vertical shift (equal to the actual shift), under correct watermark presence (Figure 3(c)) and presence of a different watermark (Figure 3(d)). It is again concluded that detection is possible since the correlation peak is far greater than any other correlation value.

5. CONCLUSIONS

Self-similar chaotic watermarks are introduced for spatially watermarking still greyscale images. The watermark generation process ensures a lowpass watermark spectrum with the purpose to make them robust against lowpass distortions. This is experimentally proven since they are observed to be satisfactorily robust against moving average and median filtering as well as JPEG compression. Their self-similar structure proves very useful under image geometric distortions, especially scaling and cropping or a combination of both. Search ranges both in scaling factors and horizontal/vertical shifts are significantly reduced.

6. REFERENCES

[1] F. Hartung and M. Kutter, "Multimedia watermarking techniques," *Proceedings of the IEEE*, vol. 87, no. 7, pp. 1079–1107, July 1999.

[2] M.D. Swanson, M. Kobayashi, and A.H. Tewfik, "Multimedia data embedding and watermarking technologies," *Proceedings of the IEEE*, vol. 86, no. 6, pp. 1064–1087, June 1998.

[3] G. Voyatzis and I. Pitas, "The use of watermarks in the protection of digital multimedia products," *Proceedings of the IEEE*, vol. 87, no. 7, pp. 1197–1207, July 1999.

[4] G. Voyatzis and I. Pitas, "Chaotic watermarks for embedding in the spatial digital image domain," in *Proc. of ICIP'98*, October 1998, vol. II, pp. 432–436.

[5] D. Kaplan and L. Glass, *Understanding Nonlinear Dynamics*, Springer, New York, 1995.

[6] C. Gotsman and M. Lindenbaum, "On the metric properties of discrete space filling curves," in *Proc. of ICPR'94*, 1994, vol. III, pp. 98–102.

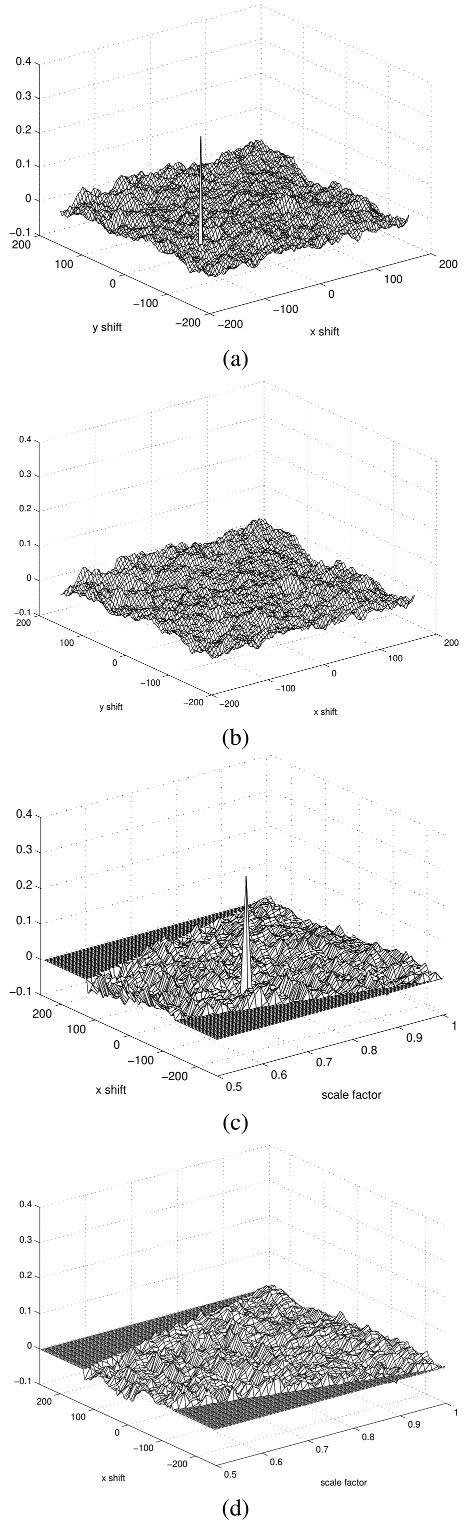

Fig. 3. Correlation values after image cropping and scaling under correct watermark presence (a,c) and presence of a different watermark (b,d), for a fixed (correct) scaling factor (a,b) or fixed (correct) vertical shift (c,d).