Cryptologia, 30:173–180, 2006

ISSN: 0161-1194 print
DOI: 10.1080/01611190500541824

Augmented Watermarking

KIRANMAYI PENUMARTHI AND SUBHASH KAK

Abstract We introduce the concept of augmented watermarking in which in addition to the hidden watermark placed within the image an explicit watermark-dependent random sequence (noise) is added to it. The receiver first detects the watermark, computes the random sequence for which the watermark serves as the seed, and then subtracts out this random sequence. This system can be devised with several watermark and noise layers which define a regime in which different users have different rights related to the quality of the signal.

Keywords digital watermarking, digital rights management

Introduction

Consider the problem of broadcasting noisy versions of a signal together with side information so that individuals with digital rights can recover the noise-free, high-quality signal from it. Here, we propose a solution to this problem based on the concept of what we call augmented watermarking. In this technique, explicit watermark-dependent noise is added in addition to the hidden watermark placed within the signal. The receiver first detects the watermark, computes the random noise sequence for which the watermark serves as the seed, and then subtracts out the noise. This system can be devised with several watermark and noise layers which define a regime in which different users have different rights related to the quality of the signal.

The proposed technique generalizes the idea of recursive secret sharing, which appeared in the pages of this Journal a few years ago [2]. The earlier technique used a threshold scheme with two shares in which several secret messages were hidden in one of the shares of the original image and each of these could serve as a watermark for authentication and other applications. In the new technique proposed in this paper, not only authentication but also the question of varying digital rights can be addressed.

Noisification of Watermarked Signal

Watermarking may be done in a variety of ways, by adding a random sequence either directly on the image or its transform [1, 3]. Figure 1 presents the schematic for the augmented watermarking technique, where in addition to the watermark a noisy sequence is also added to the image.

Address correspondence to Subhash Kak, Department of Electrical and Computer Engineering, Louisiana State University, Baton Rouge, LA 70803, USA. E-mail: eekak@lsu.edu

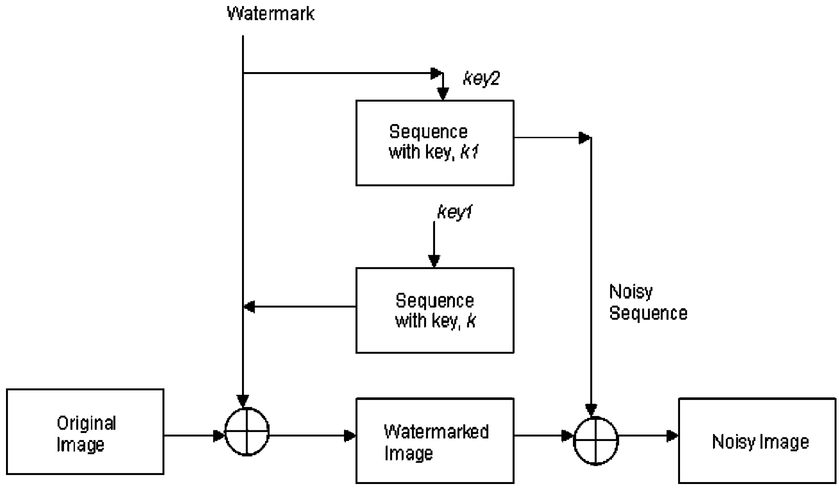

Figure 1. Augmented watermarking scheme.

For illustration, we consider the 512×512 image of Lena, here represented by $I(x, y)$. The image is watermarked using a spread spectrum technique, and noise, based on the watermark, which is also the key, is added to the watermarked image. Assume $b(x, y)$ is the spreading signal, and let the key for generating the PN sequence $W(x, y)$ be *key*1. The watermarked image $I_w(x, y)$ is therefore:

$$\begin{aligned} I_w(x,y) &= k_1 \times W(x,y) + I(x,y) \\ &= a(x,y) \times b(x,y) + I(x,y) \end{aligned}$$

where

$I_w(x, y)$ denotes the watermarked image.
$I(x, y)$ denotes the actual cover image.
$W(x, y)$ denotes a pseudorandom noise pattern that is added to the image.
k_1 denotes the gain factor with which the sequence is embedded.

Let the key for embedding the noise sequence into the watermarked image be *key2*. The watermark is resized and split into bits of length t, and each bit string is converted into a decimal number and the elements are concatenated into the key. For example, consider the following 9×12 image to be the watermark:

The image is read in the from of a matrix (9×12) as

$$\begin{array}{cccccccccccc}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\
1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\
1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\
1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\
1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 \\
1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 \\
1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1
\end{array}$$

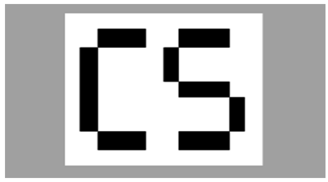

Figure 2. Watermark.

The elements of the matrix are rearranged, column wise, into a single array and two zeros appended at the end to make it divisible by our choice of t = 5 (and each block of 5 bits is converted into a decimal number, which is the key for embedding the noise):

11111	11111	10000	01110	11111
31	31	16	14	31
01101	11110	11011	11101	11111
13	30	27	29	31
11111	10011	11110	11011	01101
31	19	30	27	13
10110	11011	01101	11111	00111
22	27	13	31	7
11111	11100			
31	28			

The key for embedding noise into the image is, therefore,

31 31 16 14 31 13 30 27 29 31 31 19 30 27 13 22 27
13 31 7 31 28

This key is used as the seed in a random sequence generator which produces the sequence $W(x, y)$. Noise is added with the gain of k_{11} to the watermarked image producing the augmented watermarked and noisified image $I_{ww}(x, y)$:

$$\begin{aligned} I_{ww}(x, y) &= k_{11} \times W(x, y) + I_w(x, y) \\ &= k_{11} \times W(x, y) + (k \times W(x, y) + I(x, y)) \\ &= k_{11} \times W(x, y) + (a(x, y) \times b(x, y) + I(x, y)) \end{aligned}$$

The value of gain for embedding the watermark, and the value of gain for adding the noise, should be proportional to the length of the substring used to calculate the noise key. Ordinarily, gains in the range 0.2 to 2 are used. For simulations where heavy noise is added to distort the image to the maximum extent, gains in the range 2 to 20 are used. The watermark should be small for the spread spectrum watermarking.

The peak signal to noise ratio (PSNR) is a measure of the noisification of the image. As the noise is added with a high gain, the PSNR, changes as shown in Figure 3. But once the watermark has been recovered, the noise will be subtracted out.

Image Retrieval

The receiver first calculates the watermark. The key for adding the noise is obtained from the watermark using the same algorithm by which it is calculated at the

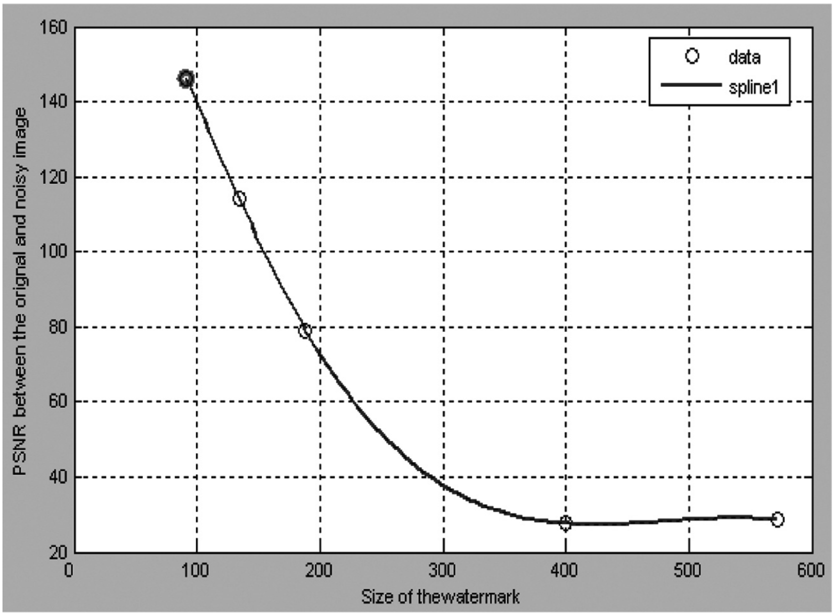

Figure 3. Variation of PSNR with the size of the watermark.

sender's end, and the noise is removed from the image. This leaves the receiver with the watermarked image. Using the key which is used for embedding, the watermark is removed from the image to obtain the original image, if so desired. It is assumed that the gain factors are known in advance to the receiver, or they might be sent as part of the protocol that sets up the communication.

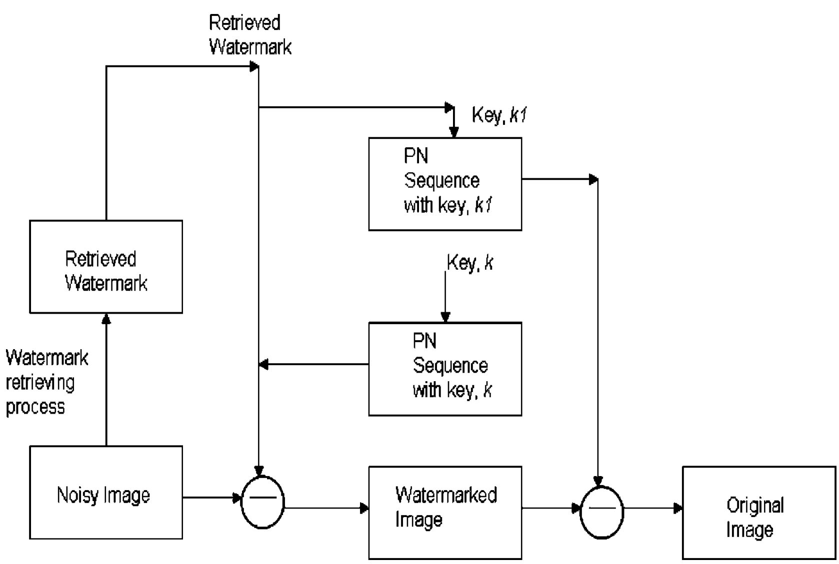

Figure 4. Image retrieval.

Figure 5. Augmented watermarking for decimal sequences.

Mathematically,

$$\begin{aligned} I_w(x,y) &= I_{ww}(x,y) - k_{11} \times W(x,y) \\ &= I_{ww}(x,y) - a(x,y) \times b(x,y) \\ I(x,y) &= I_w(x,y) - k_1 \times W(x,y) \\ &= I_w(x,y) - a(x,y) \times b(x,y) \end{aligned}$$

Experiments were conducted on augmented watermarking by using different kinds of random sequences (PN, as well as decimal) in a spread spectrum watermarking

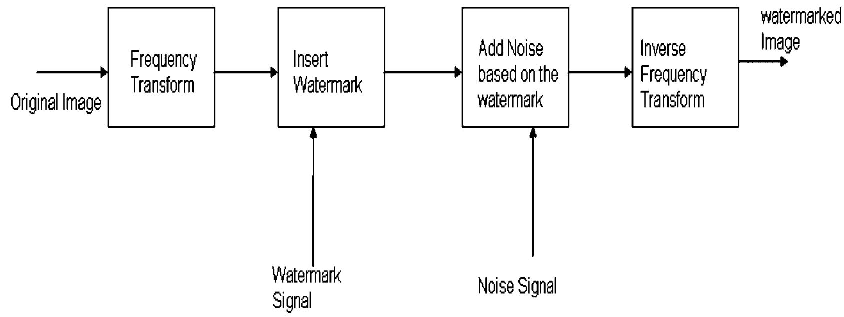

Figure 6. Frequency domain watermarking.

technique. The gain for embedding watermark into the image was $k_1 = 20$, and the gain for adding noise to the image was $k_{11} = 50$. Figure 5 presents the various steps for augmented watermarking using decimal sequences; the results for PN sequences are similar.

We now provide an illustration of this technique for a general frequency domain watermarking system as shown in Figure 6.

Consider the case of the DCT domain. On applying the discrete cosine transform to the original image to be $I(x, y)$,

$$I_{dct}(x, y) = DCT(I(x, y)).$$

The image after watermarking is

$$I_w(x, y) = I_{dct}(x, y) + k_{11} \times W(x, y).$$

Noise is added to the watermark at this stage. This noise is retrieved from the watermark as in the previous methods.

The gain for embedding watermark into the image, $k_1 = 2$ and the gain for adding noise to the image, $k_{11} = 50$. Here, the watermark itself affects the quality of the image, but when it, together with the embedded noise, is removed, the image is recovered perfectly (Figure 7).

Conclusions

Assume an image is watermarked with, say, three images $a_1(x, y)$, $a_2(x, y)$, and $a_3(x, y)$, where the spreading sequences be $b_1(x, y)$, $b_2(x, y)$, and $b_3(x, y)$. Assume, further, that if user A has partial rights, he can only remove one of the watermarks obtaining an image that is clearer compared to that of the final watermarked image but much noisier than the original image. We may consider multiple watermarks overlaid on top of one another, so that the clarity of the image seen by the end user depends on the digital rights of a person. Thus, the method of augmented watermarking can be used for the design of a DRM system.

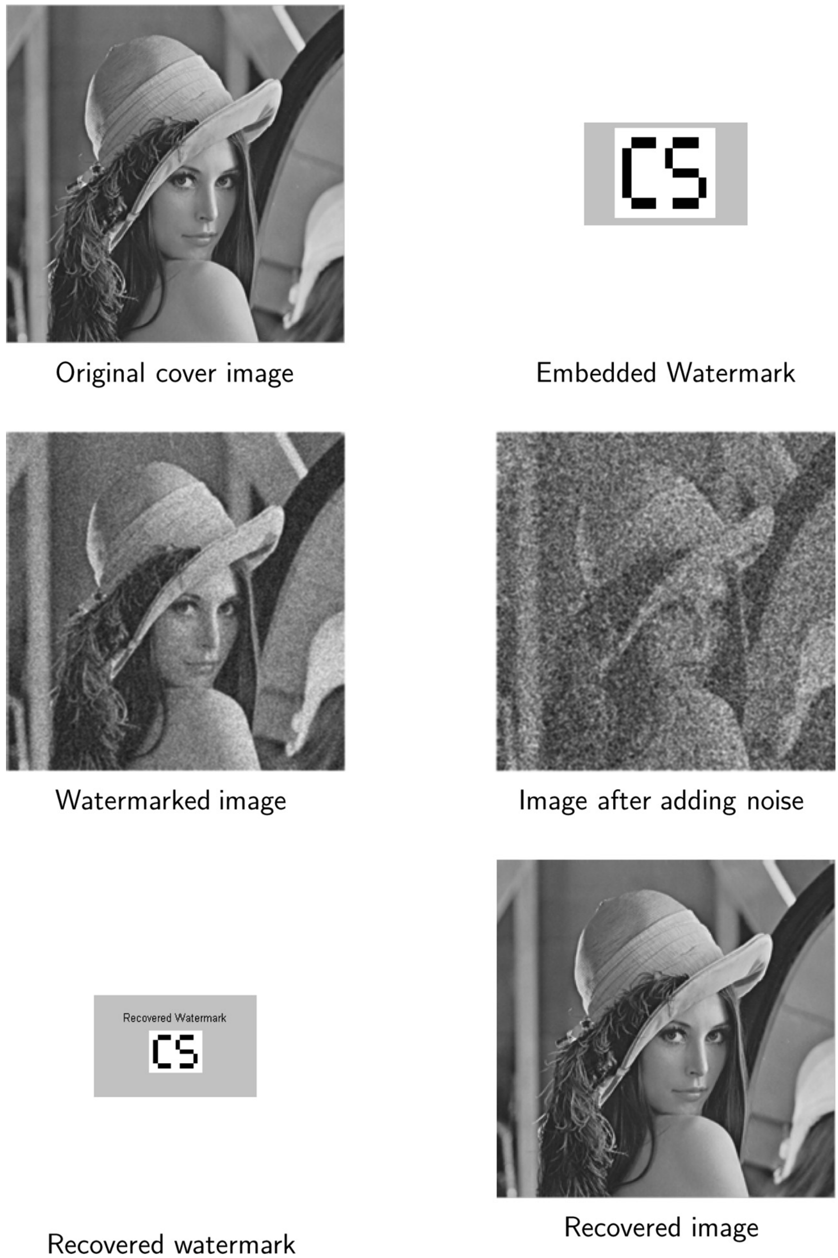

Figure 7. Augmented watermarking for decimal sequences.

About the Authors

Kiranmayi Penumarthi completed her MS in electrical engineering from LSU in 2005. Her interests lie in cryptography and signal processing.

Subhash Kak is the Delaune Distinguished Professor of Electrical Engineering at LSU, where he has taught since 1979. He has worked on various aspects of cryptology, including speech scrambling, theory of random sequences, and public key ciphers.

References

1. Arnold, M., S. D. Wolthusen, and M. Schmucker. 2003. *Techniques and Applications of Digital Watermarking and Content Protection*. Norwood, MA: Artech House Publishers.
2. Gnanaguruparan, M. and S. Kak. 2002. "Recursive Hiding of Secrets in Visual Cryptography," *Cryptologia*, 26:68–76.
3. Mandhani, N. and S. Kak. 2005. "Watermarking Using Decimal Sequences," *Cryptologia*, 29:50–58.