2004

A scalable and oblivious digital watermarking for images

W. Lu
University of Wollongong

R. Safavi-Naini
University of Wollongong, rei@uow.edu.au

Takeyuki Uehara
University of Wollongong, takeyuki@uow.edu.au

Wanqing Li
University of Wollongong, wanqing@uow.edu.au

Publication Details

This paper originally appeared as: Lu, W, Safavi-Naini, R, Uehara, T and Li, W, A scalable and oblivious digital watermarking for images, Proceedings. ICSP '04. 2004 7th International Conference on Signal Processing, 31 August - 4 September 2004, vol 3, 2338-2341. Copyright IEEE 2004.

A scalable and oblivious digital watermarking for images

Abstract
Scalable compression algorithms, such as JPEG, can compress images to different quality or resolution levels so that the target systems with different display capabilities, can display the image. Digital watermarking is widely used for protection of copyright and identification of ownership on digital images. It is desirable to have scalable watermarking systems, where the watermark is detectable when the watermarked image is at low quality or low resolution levels. This paper presents an oblivious block-based spread-spectrum-like watermarking system which is robust against scalable JPEG compression, cropping and shifting. The system is secure against the common watermarking attacks. Experimental results support these claims.

Disciplines
Physical Sciences and Mathematics

Publication Details
This paper originally appeared as: Lu, W, Safavi-Naini, R, Uehara, T and Li, W, A scalable and oblivious digital watermarking for images, Proceedings. ICSP '04. 2004 7th International Conference on Signal Processing, 31 August - 4 September 2004, vol 3, 2338-2341.

A Scalable and Oblivious Digital Watermarking for Images

Wenming Lu, Rei Safavi-Naini, Takeyuki Uehara, Wanqing Li
wl86, rei, takeyuki, wanqing@uow.edu.au
University of Wollongong, Australia

Abstract— **Scalable compression algorithms, such as JPEG, can compress images to different quality or resolution levels so that the target systems with different display capabilities, can display the image. Digital watermarking is widely used for protection of copyright and identification of ownership on digital images. It is desirable to have scalable watermarking systems, where the watermark is detectable when the watermarked image is at low quality or low resolution levels. This paper presents an oblivious block-based spread-spectrum-like watermarking system which is robust against scalable JPEG compression, cropping and shifting. The system is secure against the common watermarking attacks. Experimental results support these claims.**

I. Introduction

Recent developments in digital technologies and devices have made digital image distribution and duplication an effortless task. A digital image can be taken by a digital camera, then stored in a notebook, transferred to a hand-held PC, or a mobile phone. However, these devices have different capabilities to display or store an image. The original image usually contains some redundant information. A scalable compression algorithm, such as JPEG, can be used to produce a compressed image at various quality or resolution level to suit different storage and display systems.

Digital watermarking is widely used for protection of ownership and copyright on digital images[2]. Because of different capability of the end devices and display systems, the watermarked image would be processed by a scalable compression algorithm for a particular target system. Therefore, different devices will receive only part of the watermark embedded in the image. Piper *et al.*[5] point out that it is necessary to design scalable watermarking system, where the watermark is detectable to the required strength when the watermarked image is at various quality or resolution levels.

Piper *et al.*[5] discussed how to obtain scalability under JPEG2000 compression by carefully selecting transform coefficients for embedding the watermark. JPEG compression is widely used and it is important to obtain scalability under JPEG compression. Cox *et al.*[1] proposed a secure spread spectrum (SSS) watermarking in the DCT domain. The is scalable against JPEG compression. In the scheme, an image is globally DCT transformed and the 1000 most significant AC coefficients is chosen to embed a watermark drawn from the normal distribution $N(0,1)$. The watermark can survive JPEG compression at a quality as low as 10% and down-sampling by 4 in both dimensions. But SSS is non-oblivious and needs the original image for watermark detection. This makes SSS unsuitable for some applications, in which the original image may not be available. Non-oblivious watermarking requires large space to store all original images and it is impractical. In [10], an oblivious watermarking scheme is proposed. In this scheme, an image is globally DCT transformed and the 25000 to 41000 AC coefficients from a zig-zag path are chosen to embed the watermark. This system does not need original image for watermark detection. However, the scalability against JPEG is sacrificed. The watermark will be undetectable when the watermarked image is down-sampled by 4 in both dimensions, because the selected coefficients are higher than those in SSS. Hsu [11] proposed a blind block-based DCT watermarking system. An image is divided into 8×8 blocks and then DCT transformed. The middle band AC coefficients are chosen to embed a binary watermark sequence. Because the middle band components are chosen for the marking space, the system suffers the same problems as in [10], that is the scalability is also sacrificed.

In the paper, we propose an oblivious and scalable block-based DCT (BBD) watermark system, in which lower frequency components except the DC components, are chosen as the marking space. Because human eyes are more sensitive to lower frequencies, we design an adaptive algorithm to adjust the watermark strength in each block to keep the watermark invisible and to provide the scalability and robustness. BBD is secure, scalable and robust. We also describe possible attacks against BBD and show these attacks can be made ineffective. We provide the experimental results to support our claims.

II. Watermarking Scalability under JPEG

A. Scalable JPEG Compression

Scalable compression allows an image to be compressed for a number of target bit rates [5]. This provides flexibility in which the image, once compressed, can be displayed by devices with different resolution or processing capabilities. For still images, scalability of compression has two aspects:
i)resolution scalability which is the ability to display visual data at a number of target spatial resolutions, it is also called spatial scalability; and ii)quality scalability which is the ability to display visual data at a number of quality levels.

JPEG is a scalable compression algorithm[6] that compresses images to different quality levels by choosing a quality parameter. JPEG spectral selection mode can also provide images at different quality levels in case part of the coefficients are available. JPEG hierarchical mode can provide images at multiple resolution levels.

B. Watermarking Scalability

Some work has been done on designing progressive watermarking schemes [3], [4]. A review of these works is given in [5] and scalable watermarking is discussed. A scalable watermarking algorithm has the property that the watermark is detectable in any portion of the scaled content which is of acceptable quality. The scaled content means that the image is at either lower quality or resolution level.

Scalable watermarking for the JPEG compression means that the watermark is detectable when the watermarked image is at a predefined quality or resolution level and above according to the requirements of different applications. In the paper, we design a watermarking system for owner identification or copyright protection, in which the watermark is detectable on the JPEG compressed or down-sampled images at low levels.

0-7803-8406-7/04/$20.00 © 2004 IEEE.

C. How to gain scalability in JPEG?

JPEG compression discards less significant frequency components. Because the quantization coefficients are larger for higher frequency components and the most significant components are usually located in lower frequency parts, JPEG compression will usually discard higher frequency components.

Down-sampling is used to produce an image at lower resolution levels. Down-sampling an image discards higher frequency coefficients in DCT domain. If all AC coefficients are set to 0 and IDCT is applied to the block, all pixels in the block result in the same value which equals to the average of all pixels. Therefore, down-sampling an image by s in both dimensions is equivalent to setting all AC coefficients to 0 in an s×s block. Similarly, down-sampling by different parameters less than s means that certain higher frequency of AC coefficients are lost. According to the discussion, we can conclude that the watermark should be embedded into lower frequency coefficients to obtain the scalability.

III. A Scalable and Oblivious Watermarking

A. Watermark Embedding and Detection

BBD watermark embedding

In BBD scheme, an image is divided into *macro blocks* with size $M \times M$ first. Suppose there are m macro blocks in an image. Each macro block is further divided into *base blocks* with size $B \times B$. Every macro block contains $(\frac{M}{B})^2$ base blocks. The further division of macro blocks into base blocks is because DCT transform on small block is more efficient. The DCT is applied to each base block to produce the coefficient matrix. From the matrix for each base block, certain AC coefficients with length l are chosen by a zigzag path to construct a sequence S_i for the ith base block. For each macro block, we construct a sequence C_j as the marking space with length $(\frac{M}{B})^2 l$ by combining sequences S_1, S_2, ...S_n together. The watermark W drawn from the normal distribution $N(0,1)$ is inserted into C_j by equation (1).

$$C_j' = C_j + \alpha W, j = 1, 2, ..., m \quad (1)$$

α is the strengthening parameter which strike the balance between the watermark invisibility and robustness. C_j' then replaces C_j in the matrices. An IDCT is applied to each matrix to produce the watermarked block. This process is repeated for every macro block.

BBD watermark Detection

When detecting the watermark in a received image, a sequence C_j' $(i = 0, 1, ..., m)$ is extracted from each macro block the same way constructing the marking space C_j. A final sequence C' for the watermark detection is produced by,

$$C' = \frac{1}{m}\sum C_i', i = 1, 2, ..., m \quad (2)$$

the watermark response is defined as,

$$r(C', W) = \frac{\overline{C}' \cdot W}{\sqrt{\overline{C}' \cdot \overline{C}'}} \quad (3)$$

in which $\overline{C}' = C' - \mu_{C'}$, $\mu_{C'}$ is the mean of C'. Figure 1 shows the watermark embedding and detection process.

We have chosen the detection threshold to be 6. This approximately corresponds to the false positive detection of 1 in 10^9 [7].

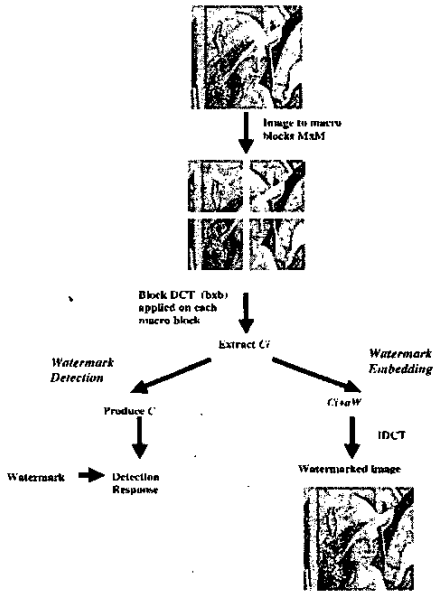

Fig. 1. BBD: Watermark embedding and detection

Fig. 2. *lena*(left), *lenawm*(right) PSNR to *lena* 41.75

B. Adaptive Choice of Parameter α

Human eyes are more sensitive to lower frequencies. We design an adaptive method to decide the strengthening parameter α to assure image quality. In this method, we initialize α at a starting point and set an upper bound U for α, and a desired watermark detection response D for the macro block. For each macro block after constructing the marking space C_j, we insert the watermark into C_j and produce a forecasting detection response. If the forecast is less than D, we increase α by a fixed step u until either watermark detection reaches D or α is equal to U. This technique allows the watermark to be inserted into a macro block to its highest possible value, while maintaining the quality. The method is as follows:

$$\begin{array}{|c|}\hline initialize\ \alpha,\ U,\ u\ and\ D \\ do\{ \\ \alpha = \alpha + u \\ C_j' = C_j + \alpha W \\ calculate\ r(C_j', W) \\ \}while(r(C_j', W) < D\ \&\&\ \alpha < U) \\ \hline\end{array}$$

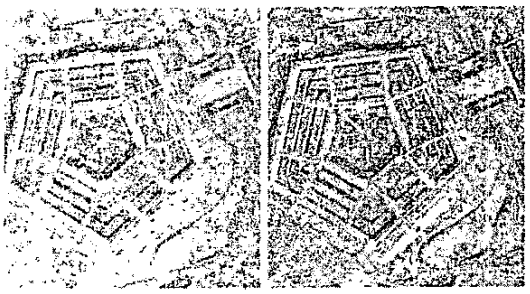

Fig. 3. *pentagon*(left) , *pentagonwm*(right) PSNR to *pentagon* 41.52

IV. System Evaluation

In this section, we show that BBD is as scalable as SSS, the watermark is detectable on images compressed by JPEG to 10% quality level and down-sampled by 4 in both dimensions. The performance is much better than other oblivious systems [10], [11]. BBD is also secure against multiple-watermarking attack and robust against cropping and shifting without the original image. SSS is not able to detect the watermark on the cropped images without the original image making up for the lost part.

A. Choices of Parameters

In our experiments, the macro block size M is 64, and the base block size B is 8 because our goal is to make the watermark survive the JPEG compression 10% and down-sampling by 4 in both dimensions. Those parameters will strike the balance between system efficiency, watermark invisibility and robustness. There are 64 base blocks on each macro block. We insert the watermark into lower frequency coefficients(1st to 14th ACs). The length of the watermark sequence is 896. The maximum detection response is around 30 according to equation (3). We set the desired macro block watermark detection response D at 5 and the upper bound U for α at 5, the increasing step u at 0.5, and the initial value for α is 0.5.

BBD performs better on larger size images. The larger the image is, more macro blocks are available, the more the watermark is repeated in the image, and so that the watermark tends to be more scalable. To verify this, we select two gray-scale images *pentagon* of 768×768 and *lena* of 512×512, and watermark them with the same set of parameters(The results on other images are similar). The watermark is repeated 144 times on *pentagon* against 64 on *lena*. The watermarked images are *lenawm* and *pentagonwm*, respectively. $PSNR$ between *pentagon* and *pentagonwm* is 41.52, and 41.75 between *lena* and *lenawm*. The high PSNR values assure the quality of the watermarked images. The images are shown in Figure 2 and 3.

B. Scalability

Figure 4 shows the watermark detection response on *pentagonwm* and *lenawm* using 1000 random watermark sequences. Among them, only the watermark inserted reports a response well above threshold. Table1 shows the PSNR between the original and the watermarked images, detection on the watermarked images($D1$), detection on JPEG compressed watermarked images at quality 10%($D2$) and on the down-sampled watermarked images by 4 in both dimensions($D3$).

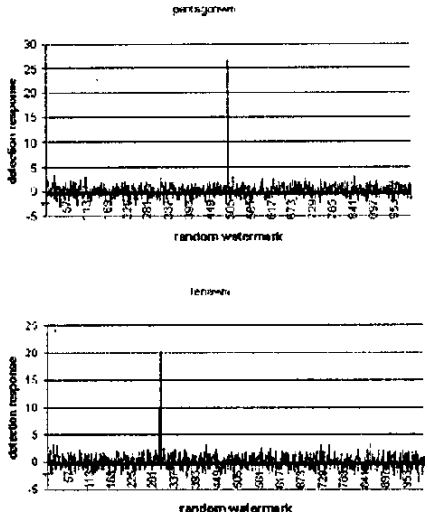

Fig. 4. Watermark detection on *pentagonwm*(top) and *lenawm*(bottom)

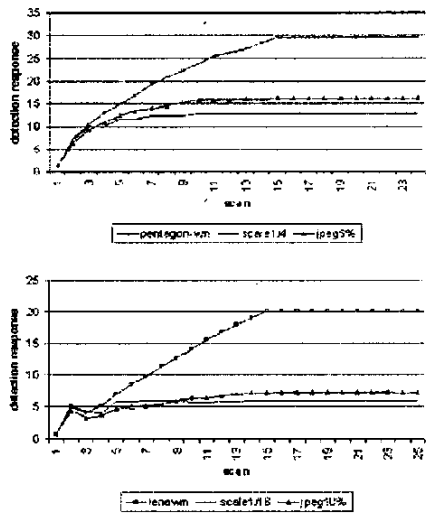

Fig. 5. BBD: watermark mostly on the first 15 scans (coefficients) *pentagonwm*(top), and *lenawm*(bottom)

image	$PSNR$	$D1$	$D2$	$D3$
lena	41.75	20.15	7.22	5.94
pentagon	41.52	26.75	19.01	11.29

Table 1: BBD's performance

Figure 5 shows the detection on the first 25 scans of the JPEG spectral selection mode for *pentagonwm* and *lenawm*, together with JPEG compressed at 10% and down-sampled by 4 in both dimensions. The watermark information is distributed mostly on the first 15 scans of the watermarked images. However, after the first several scans, the watermark detection response is above the threshold. We also see that BBD performs better on *pentagon*. For smaller size images, higher scalability can be obtained by sacrificing the watermark invisibility, that is by strengthening watermark

existence on the macro blocks by increasing α.

We have seen that the watermark can survive down-sampling by 4 in both dimensions. If the image is down-sampled by 8 in both dimensions, the DCs will be the only coefficients left. Intuitively, the watermark must be embedded into the DC components to survive this huge level of down-sampling. But there are some difficulties. Firstly, the number of DC components is limited so the size of the marking space is not large enough. Secondly, the watermark embedded into DC degrades the image quality. One solution is to use 16×16 DCT transform on the image and select AC coefficients from lower frequency parts to embed the watermark. That is, change the base block size to 16, keep the macro block size at 64, and select 1st to 53rd AC coefficients from the 16×16 matrix. α is set at 10. The watermark detection response is 28.35 on the watermarked *pentagon* and 6.07 on the down-sampled watermarked *pentagon* by 8 in two dimensions. This is very impressive score because the down-sampled image is only $\frac{1}{64}$ of the original image in area.

C. Security

a) The multiple-watermarking attack: BBD is secure against multiple-watermarking attack[1]. The multiple-watermarking attack uses the same watermarking algorithm to watermark an image many times. This is equivalent to adding noise to the existing watermark. Watermark resistance against this attack depends on the length of the watermark sequence. According to [1], theoretically an image can be watermarked n times.

$$n \leq \frac{N}{T^2} \tag{4}$$

where N is the length of the embedded watermark and the T is the detection threshold. In our experiments, the length of the watermark sequence is 896 and T is 6. Hence, an image can be watermarked 24 times and each watermark is still detectable. In practice, the watermark detection is affected by other factors, such as rounding process and the strength of the watermark in the image and so the resistance is less. We watermark *pentagon* using 11 random watermarks. The detection response for watermarks are 8.12, 8.61, 7.17, 9.03, 8.54, 9.43, 10.05, 9.42, 9.59, 9.61 and 9.98, respectively. However, the resulting image has PSNR 26.75 to the original image which is too low and unacceptable (JPEG 10% compressed *pentagon* has PSNR 26.89 to *pentagon*).

b) The secret-guessing attack: For watermarked image, an attacker can extract the sequence C' as in (3), which is highly correlated with the secret watermark W. The attacker may launch a brute-force attack by removing the watermark in each macro block. This can be fixed by scrambling the secret watermark. The embedded watermark W is permuted by some key-based permutation algorithm.

D. Robustness against cropping and shifting

BBD provides robustness against cropping. The same watermark sequence is inserted into all macro blocks. For cropped image, watermark detection can succeed if the cropped image contains more than a certain number of macro blocks. Experiment shows that the watermark detection succeeds on all 192×192 blocks, only 9 macro blocks, of *pentagonwm* and *lenawm* which keep synchronization to the watermark embedding. In SSS, the original image must be available to make up for the cropped part to facilitate watermark detection.

The algorithm is also robust against shifting when the size of the cropped image is large. Suppose the coordinate of the top-left position of an image is (0,0). We crop an image of size 448×448 from *pentagonwm* such that in the cropped image, the top-left corner starts at (64,64). This will keep synchronization of the embedding because macro blocks are of size 64. The cropped image reports the watermark detection response 21.11. If the image is cropped from (64,65), one pixel right shifting from the watermark embedding position, the watermark detection response is 12.06. If the image is cropped from (65,64), one pixel down shifting from the watermark embedding, the watermark detection response is 13.05. When we crop the image from (65,65), the watermark detection response on the cropped image is 6.31, still above the threshold.

V. Conclusion

We proposed a new watermarking algorithm that works in DCT domain. Our experiments show that the new watermarking algorithm is scalable and robust. It can survive JPEG compression at very low quality levels and down-sampling to low resolution levels. The resolution scalability can be adjusted by choosing different base block sizes for applying DCT on an image. BBD is robust against cropping and shifting, and also secure against multiple-watermarking attack. We also point out a attack against BBD and provide a solution.

One of the important properties of the watermarking scheme is that it is oblivious, which does not need the original image for the watermark detection. This is important advantages of BBD over watermarking system, such as SSS. Compared with other oblivious systems in [10], [11], the scalability is the main advantage. The system is as scalable as SSS while maintaining the oblivious property.

References

[1] I.J. Cox, J. Kilian, T. Leighton and T. Shamoon, Secure Spread Spectrum Watermarking for Multimedia, *IEEE Trans.on Image Processing*, pp1673-1687, 1997

[2] I.J Cox, M.L Miller, J.A Bloom, Watermarking Applications and their Properties, *Intl.Conf.on Information Technology*, pp6-10, Las Vegas, 2000

[3] T.P.C Chen and T. Chen, Progressing Image Watermarking, *Proc. IEEE International Conference on Multimedia and Expo.*, vol.2, pp1025-1028, July 2000

[4] P.C Su, H.J Wang, C-C. J. Kuo, An Integrated Approach to Image Watermarking and JPEG2000 Compression, *Journal of VLSI Signal Processing*, vol.27, 2001

[5] A Piper, R Safavi-Naini and A Mertins, Coefficient Selection Methods for Scalable Spread Spectrum Watermarking, *International Workshop on Digital Watermarking*, pp255-266, Seoul, 2003

[6] David Salomon, Data Compression, 2nd Edition, Springer, 2000

[7] M.L Miller, J.A Bloom, Computing the Probability of False Watermark Detection, *Proc.3rd International Workshop on Information Hiding*, pp146-158, 1999

[8] C.S Lu and H.Liao, Multipurpose watermarking for image authentication and protection, *IEEE Trans. Image Processing*, vol.10, pp. 1579-1592, 2001

[9] C.S.Lu, S.K.Huang, C.J. Sze, and H.Y M.Liao, Cocktail Watermarking for Digital Image Protection, *IEEE Transactions on Multimedia*, vol.2, no.4, pp. 209-224, 2000

[10] A.Piva, M.Barni, F.Bartolini and V.Cappellini, DCT-based Watermarking Recovering without Resorting to the Uncorrupted Original Image, *International Conference on Image Processing*, vol.1, October, 1997

[11] C-T. Hsu and J-L. Wu, Hidden Digital Watermarks in Images, *IEEE Transactions on Image Processing*, vol.8, No.1, 1, January, 1999