Multiple Re-Watermarking Scenarios

Andreas Mascher-Kampfer[1,*], Herbert Stögner[1], and Andreas Uhl[1,2,+]

[1]School of Telematics and Network Engineering, Carinthia Tech Institute, Austria
[2]Department of Computer Sciences, Salzburg University, Austria
[+]Corresponding author e-mail: uhl@cosy.sbg.ac.at

Keywords: Multiple watermarking, successive watermarking, re-watermarking, robust watermarking

Abstract – The use of classical robust watermarking techniques for multiple re-watermarking is discussed. In particular we focus on a comparison of the usefulness of blind and non-blind algorithms for this type of applications. A surprisingly high number of watermarks may be embedded using both approaches, provided that additional data is recorded in the non-blind case.

1 Introduction

Watermarking [2] has been proposed as a generic technique to solve various problems associated with topcis in the areas of digital rights management (DRM) and multimedia security [3]. According to the respective applications, watermarking technology exhibits significantly different properties, e.g. with respect to robustness (as required for ownership claims) or fragility (as required for integrity investigations). Whereas watermarking has evolved to a mature technology in the last decade, several issues remain to be solved until large scale deployment is to be expected. Multiple watermarking is one of those issues.

Mintzer et al. [6] discuss three types of watermarking applications in the context of multiple watermarking and identify different ways how to employ and to interpret multiple watermarking. Multiple watermarks can be used to address multiple applications or one application may be addressed several times. For example, a first watermark can be used to embed ownership information, a second one for integrity verification, and a third one for captioning. On the other hand, there can be multiple copyright watermarks, multiple verification watermarks, or multiple watermarks for multiple captions.

Focussing on the way how single watermarking techniques are actually fused into multiple watermarking schemes, Sheppard et al. [7] distinguish three main categories of multiple watermarking techniques:

1. Composite watermarking: All watermarks are combined into a single watermark which is subsequently embedded in one single embedding step.
2. Segmented watermarking: The host data is partitioned into disjoint segments and each watermark is embedded into its specific share.
3. Successive watermarking: Watermarks are embedded one after the other. This approach is also denoted *Re-watermarking* in literature.

In this work, we focus on multiple re-watermarking using robust embedding techniques. In Section 2 we will identify the technological requirements for our target application scenario and we will discuss multiple re-watermarking techniques with emphasis on the differences when using blind or non-blind detection algorithms. Corresponding re-watermarking experiments are described in Section 3 and Section 4 concludes the paper.

2 Multiple re-watermarking

The embedding of unique watermarks for receiver identification is called *fingerprinting*. In case a cover medium is sold, it may be of interest that information concerning both, the original owner and the recipient, are embedded. In case re-selling occurs, each time the cover medium is sold the corresponding informations can be embedded using watermarking technology. In this case we can *trace back* the way of the cover medium to its origin and are able to reconstruct the entire *trading chain*. We want to support this scenario with multiple watermarking technology. Fingerprinting solves the question **what** to embed but not **how** to embed it.

Composite watermarking is not very useful in this scenario since all watermarks to be embedded have to be present prior to embedding to generate the one single composite mark. Segmented watermarking suffers from the fact that at least the approximate number of watermarks to be embedded needs to be known in advance. Additionally, the techniques developed so far are restricted in terms of the number of marks that can be embedded. Therefore, successive or re-watermarking seems to be the most promising approach for our target scenario. Obviously, all watermarks embedded serve the same purpose so the multiple applications case does not apply.

Shieh et al. [8] propose a successive watermarking scheme where the first mark is embedded in a vector quantization domain whereas the second watermarking scheme operates in the middle DCT frequency band. This approach is suited in principle for our scenario, but it is restricted to two watermarks in the described setting

*This artificial name represents a group of students working on this paper in the framework of the Multimedia I lab in winterterm 2005/2006: Michael Dorfer, Severin Kampl, Alexander Maier, Andreas Palli, and Günter Scheer.

and it is problematic in general due to the limited number of different watermarking domains available. Sheppard et al. [7] employ a blind spatial domain algorithm and a non-blind DCT domain algorithm for multiple re-watermarking by simply embedding different marks successively. They report good performance in the first case and decreasing watermark correlations in the second case. We will investigate the behaviour of blind and non-blind algorithms in the re-watermarking scenario more thouroughly in the following.

Fig. 1 vizualizes our target scenario. We embed three marks (A, B, C) successively into the image I using some embedding technique $\oplus$. After inserting the marks, we result in the respectively marked images I_A, $I_{A,B}$, and $I_{A,B,C}$.

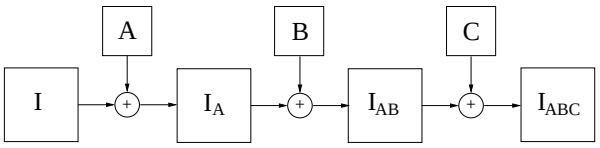


Figure 1: Multiple Re-Watermarking scenario.

Detection of a watermark W in the eventually marked image I' in case of a non-blind algorithm works as follows:

$$D_W(I, I') = K(I - I', W)$$

where K computes a correllation-type similarity measure. In case of a blind algorithm no original image I is involved:

$$D_W(I') = K(I', W)$$

In the multi re-watermarking scenario $I' = I_{A,B,C}$. In case of a non-blind algorithm the "original" image (i.e. the image before the watermark was embedded) is required for detecting the mark. In case of multiple re-watermarking only for detection of the mark A the original image I is the correct reference original before watermark embedding. For example, for detecting mark C, image $I_{A,B}$ is the required reference image. This immediately reveals an instrinsic disadvantage of non-blind schemes when used in our scenario: in addition to the embedded watermarks also the original reference images before mark embedding have to be recoreded and kept for a later detection process (which is much more demanding in terms of storage capacity of course).

Detection of the marks A, B, C is facilitated as follows:

$$\begin{aligned} D_C &= K(I_{A,B} - I_{A,B,C}, C) = K(f(C), C) \\ D_B &= K(I_A - I_{A,B,C}, B) = K(f(BC), B) \\ D_A &= K(I - I_{A,B,C}, A) = K(f(ABC), A) \end{aligned}$$

where f(ABC) is an expression involving the watermarks A, B, C only. Clearly, we expect the detection result of C to be superior to that of A (and to be equivalent to the value of single embedding using the same technique) since the additional watermarks involved in the correlation computation of A and B will simply act as noise. The more watermarks are involved, the lower the amount of correlation is expected to be. In case the original image I is used to detect e.g. mark C, we result in $D_C = K(I - I_{A,B,C}, C) = K(f(I, A, B, C), C)$ where the expression $f(I, A, B, C)$ results from the fact that an incorrect reference image is used in the detection process. No significant correlation is to be expected, except for mark A where the original image I is indeed the correct reference.

In case of a blind algorithm, the detection of the marks A, B, C is facilitated as follows:

$$\begin{aligned} D_C &= K(I_{A,B,C}, C) = K(f(I, A, B, C), C) \\ D_B &= K(I_{A,B,C}, B) = K(f(I, A, B, C), B) \\ D_A &= K(I_{A,B,C}, A) = K(f(I, A, B, C), A) \end{aligned}$$

Note that contrasting to the non-blind case the expressions of the type $K(f(I, A, B, C), C)$ should result in reasonable correlation values due to the blind algorithm design principles provided that the watermarks do not interfer severely with each other. Those expressions should be almost identical for all three marks A, B, C (note that this contrasts to the non-blind case where we expect a decrease in correlation). However, the values are expected to be lower compared to single watermark embedding since $K(f(I, A, B, C), A) \leq K(f(I, A), A)$ due to watermark interference.

In the following section we will try to experimentally validate our observations.

3 Experimental study

3.1 *Settings and Methods*

For our experiments we have chosen the well known image "Lena" with the size of 512×512 pixels and 8 bpp as host image for watermark embedding. We have used the Watermarking Toolbox [1] developed by Peter Meerwald for watermark embedding and detection, unless denoted otherwise all embeddings have been done with the default settings of the implementation using an embedding strength to result in a final host image PSNR of 38dB (containing all embedded watermarks). Non-blind techniques are operated either with original image I or with correct reference images ($I_{A,B}$ etc.) in the detection process. While experiments have been conducted with all available algorithms, only results corresponding to three selected schemes are reported here (since the remaining results correspond well to those presented):

1. Wang et al. [9]: a non-blind, wavelet-based spread-spectrum technique which embeds into the significant middle and high frequency coefficients.

[1] `http://www.cosy.sbg.ac.at/~pmeerw/Watermarking/source/`

2. Corvi et al. [1]: a non-blind, wavelet-based spread-spectrum technique which embeds into the significant low and middle frequency coefficients.

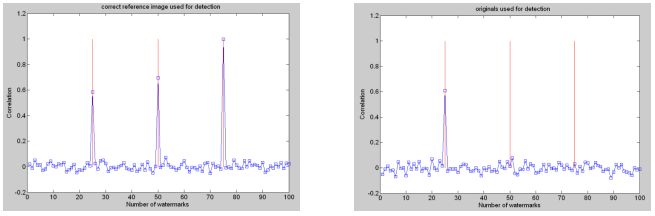
3. Koch et al. [5]: a blind, 8×8 pixel block DCT-based quantization technique which embeds into randomly chosen blocks.

The three algorithms exibit watermark detection correlation values of 1.0, 0.95, and 0.8 respectively. Note that the only blind algorithm delivers the lowest peak correlation value.

3.2 *Results*

The following result graphs have to be read as follows: n watermarks have been embedded and $200 - n$ or $100 - n$ randomly generated plus the actually embedded n marks are fed into the detection process. The positions of the truly embedded marks are indicated by n vertical lines, the mark at the rightmost position has been embedded as the last mark (i.e. it corresponds to mark C in Fig. 1), all other indicated positions are ordered in time in the same manner.

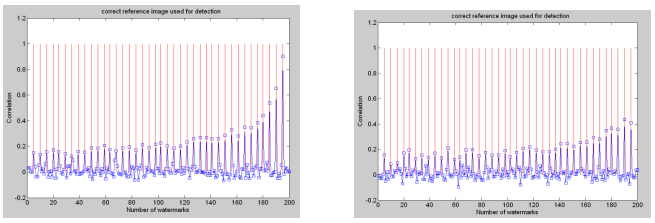
Fig. 2 shows the results of the Wang algorithm. When employing the correct reference images in detection the rightmost response – corresponding to the last mark embedded – is the highest (see Fig. 2.a) exhibiting a similar correlation value as compared to single marking. Watermarks further left in the plot (embedded at an earlier stage) show decreasing correlation values. Note that this exactly matches the prediction in the last section. When using the original image in the detection process – Fig. 2.b – only the first mark embedded is detected, at a significantly lower correlation value as compared to single detection.



(a) Correct reference used (b) Original image used

Figure 2: Wang algorithm detection response 3 WMs embedded (non-blind vs. blind detection).

Fig. 3 shows that a large number of watermarks may be embedded using this approach – still the 40 highest correlation values of the determined 200 correspond to the 40 embedded marks (Fig. 3.a). Fig. 3.b shows that even a certain amount of robustness is retained – under JPEG compression at quality 60% still all 40 embedded marks can be detected when setting the decision threshold accordingly.



(a) Correct reference used (b) JPEG compression

Figure 3: Wang algorithm detection response 40 WMs embedded (correct reference used in detection).

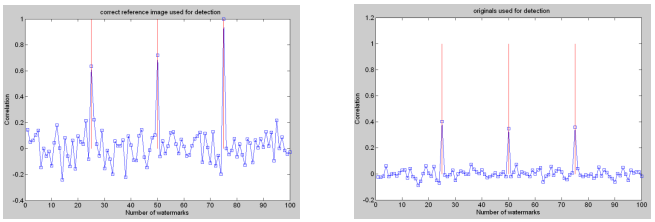
Fig. 4.a displays the image with all watermarks embedded corresponding to the results in Fig. 3.a. Almost no quality degradation is visible.

(a) Wang, 40WM, 38.4 dB (b) Koch, 33WM, 38.4 dB

Figure 4: Visual quality of images with a large number of watermarks embedded.

Fig. 5 covers the same situation for the Corvi algorithm as Fig. 2 does for the Wang algorithm. The results when the correct reference images are used are in perfect accordance (Fig. 5.a), whereas they are not in the case the original image is used in the detection process (Fig. 5.b). Here the Corvi algorithm does not behave as predicted and is able to detect all three embedded marks with almost equal correlation values, contrasting also to the results of the Wang algorithm. In the case of the Wang algorithm the most significant wavelet coefficients (according to their magnitude) are manipulated – by changing the value of these coefficients the set of significant coefficients is different each time a mark gets inserted, therefore the watermark detection process loses synchronization since it is not clear which coefficients have been significant at the time of embedding the mark. In addition to that, the watermarks interfer with each other, since often the same coefficients are selected and simply re-marked, which leads to a more or less severe overwriting of the previously embedded information. The Corvi algorithm on the other hand manipulates all approximation subband coefficients after a three level decomposition – consequently, the synchronization problem does not occur. The reduction in correlation as compared to the sin-

gle watermarking case is due to watermark interference similar to the Wang algorithm case.

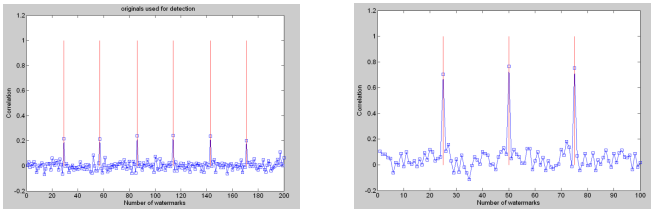


(a) Correct reference used

(b) Original image used

Figure 5: Corvi algorithm detection response 3 WMs embedded (non-blind vs. blind detection).

Fig. 6.a increases the number of watermarks embedded using the Corvi algorithm to 6 (only the original is used for detection). While the absolute detection correlation again drops significantly as compared to the case shown in Fig. 5.b with 3 embedded marks, the values are consistently above those of the random marks and they do not depend on the embedding order. However, it is clear that the number of marks that can be detected using the approach with the original image only cannot be further increased reliably, whereas a much higher number can be embedded if the correct reference images are employed.

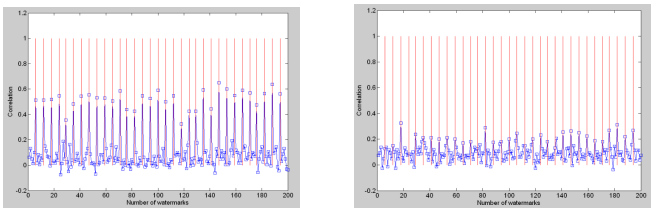


(a) Corvi with original used in detection, 6 WMs

(b) Koch algorithm, 3WM

Figure 6: Algorithm detection response 6 and 3 WMs embedded (blind detection mode).

Fig. 6.b shows the result of the Koch algorithm. The correlation values are significantly below those of single watermark detection, but they do not depend on the embedding order as predicted for blind algorithms in the last section. The algorithm-specific reason for the reduced correlation values as compared to single marking is that the sets of blocks used to embed the different marks are not disjoint so that some blocks are marked repeatedly which degrades correlation. As the final test, we increase the number of marks embedded by the Koch algorithm and we subject the marked image to JPEG compression. Fig. 7.a shows that the 33 highest correlation values of the determined 200 correspond to the 33 embedded marks. The absolute correlation values are lower as compared to the case of embedding 3 marks, but not as pronounced as for the Corvi algorithm (compare Figs. 5.b and 6.a). Note also that very low correlation values as occurring in the case of the Wang algorithm when embedding 33 watermaks (compare Fig. 3.a) do not show up. Fig.4.b shows the image containing all 33 watermarks corresponding to the results in Fig. 7.a. Some local distortions on a block basis are visible, especially close to dominant edges.



(a) 33 marks embedded

(b) JPEG compression

Figure 7: Koch algorithm detection response 33 WMs embedded (blind detection).

Moderate JPEG compression however (quality at 60%) is not tolerated in this setting as displayed in Fig. 7.b. It is no longer true that the 33 highest correlation values of the determined 200 ones correspond to the 33 embedded marks. On the one hand this may be due to the lower robustness of blind algorithms in general (compare the small impact of JPEG compression on the Wang algorithm with 40 marks embedded – Fig. 3.b), on the other hand the embedding domain of the Koch algorithm exactly matches the compression domain of JPEG, which is known to be contraproductive for watermark robustness [4].

The non-blind Wang and the blind Koch algorithms have found to behave exactly as predicted in the multiple re-watermarking scenario. The non-blind Corvi algorithm behaves as predicted when used with correct reference images but may be also operated in a blind fashion using the original image in the detection process. In this case it behaves like a blind algorithm, however the number of marks that can be embedded is low. This interesting property of this algorithm is due to the absence of the synchronization problem as observed in other algorithms.

4 Conclusion

The use of classical single watermarking schemes in a multiple re-watermarking scenario is discussed. We have found that non-blind as well as blind algorithms may be employed for that purpose provided that correct reference image data is recorded and stored for the non-blind algorithms. A surprisingly large number of different watermarks may be detected and also robustness is maintained to a certain extent using this approach, however, detection correlation drops for an increasing number of embedded marks which limits scalabilty to long trading chains.

Acknowledgements

This work has been partially supported by the Austrian Science Fund, project no. 15170.

References

[1] Marco Corvi and Gianluca Nicchiotti. Wavelet-based image watermarking for copyright protection. In *Scandinavian Conference on Image Analysis, SCIA '97*, Lappeenranta, Finland, June 1997.

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

[3] B. Furht and D. Kirovski, editors. *Multimedia Security Handbook*. CRC Press, Boca Raton, Florida, 2005.

[4] Brigitte Jellinek and Andreas Uhl. A remark on the interplay between image compression and watermark embedding techniques. In S. Loncaric and H. Babic, editors, *Proceedings of the 2nd IEEE Region 8 - EURASIP Symposium on Image and Signal Processing and Analysis (ISPA'01)*, pages 68–73, Pula, Croatia, June 2001.

[5] Eckhard Koch and Jian Zhao. Towards robust and hidden image copyright labeling. In *Proceedings of the IEEE International Workshop on Nonlinear Signal and Image Processing*, pages 452–455, Marmaras, Greece, June 1995.

[6] F. Mintzer and G. W. Braudaway. If one watermark is good, are more better? In *Proceedings of the International Conference on Accoustics, Speech, and Signal Processing*, volume 4, pages 2067–2070, Phoenix, Arizona, USA, May. 1999.

[7] N. P. Sheppard, R. Shafavi-Naini, and P. Ogunbona. On multiple watermarking. In *Proceedings of the ACM Multimedia and Security Workshop 2001 (MMSW-01)*, pages 3–6, Ottawa, Canada, Oct. 2001. ACM Press.

[8] C.-S. Shieh, H.-C. Huang, F.-H. Wang, and J.-S. Pan. An embedding algorithm for multiple watermarks. *Journal of Information Science and Engineering*, 19(2):381–395, Mar. 2003.

[9] Houng-Jyh Wang and C.-C. Jay Kuo. Watermark design for embedded wavelet image codec. In *Proceedings of the SPIE's 43rd Annual Meeting, Applications of Digital Image Processing*, volume 3460, pages 388–398, San Diego, CA, USA, July 1998.