Attack on 'Watermarking Method Based on Significant Difference of Wavelet Coefficient Quantization'

Peter Meerwald⋆, Christian Koidl, and Andreas Uhl

***Abstract*—This paper describes an attack on the recently proposed 'Watermarking Method Based on Significant Difference of Wavelet Coefficient Quantization' [1]. While the method is shown to be robust against many signal processing operations, security of the watermarking scheme under intentional attack exploiting knowledge of the implementation has been neglected. We demonstrate a straightforward attack which retains the fidelity of the image. The method is therefore not suitable for copyright protection applications. Further, we propose a countermeasure which mitigates the shortcoming.**

***Index Terms*—Watermarking, copyright protection, attack, quantization.**

I. Introduction

Copyright protection is an important watermarking application where information identifying the copyright owner is imperceptibly embedded in multimedia data such that this watermark information is detectable even in degraded copies. Quantization-based watermarking is an attractive choice as it combines high watermark capacity with robustness against manipulation of the cover data. The ability to embed many watermark bits (in the range of 256 to 1024 bits) allows to hide a small black-and-white logo image. An extracted logo image can be used to visually judge the existence of a particular watermark. Alternatively, the normalized correlation measure between the embedded and extracted watermark provides for numerical evaluation.

Recently, Lin et al. [1] proposed a robust, blind watermarking scheme based on the quantization of the significant difference between wavelet coefficients. Their results for a 512 bit watermark demonstrate good robustness for a wide variety of signal processing attacks such as JPEG compression, median filtering, sharpening and mild rotation. However, in the copyright protection scenario, a watermarking method must not only withstand unintentional processing of the cover data but also intentional, targeted attack by a malicious adversary.

For the attack scenario in this paper, we assume that we have access to only a single watermarked image but possess full knowledge of the implementation details of the watermarking scheme. A public detector is not available. According to the classification suggested by Cayre et. al [2], this constitutes a watermark-only-attack (WOA). Following Kerckhoffs' principle [3], a watermarking system should be 'secure' even if everything except the key is known. Watermark 'security' versus robustness is a controversial topic. Kalker [4] states that 'security refers to the inability by unauthorized users to have access to the raw watermarking channel'.

While general signal processing, geometric and protocol level attacks [5]–[7] have received ample attention in the literature, only few works investigate targeted attack directed towards the weakness of a particular watermarking algorithm. The attacks mounted on the proposed scheme during the 'Break Our Watermarking System' (BOWS) contest [8] expose vulnerabilities and indicate design guidelines for robustness and security to be incorporated in new watermarking schemes. It is thus worthwhile to consider attacking a particular watermarking method. Benchmarking may provide a robustness evaluation [9], however in the copyright protection scenario a detailed analysis for potential weaknesses is required. For example, Das et al. [10] describe a successful analysis of another wavelet-based quantization watermarking method [11]. Although the scheme demonstrates good robustness against many signal processing operations, the embedding locations are revealed and can then be efficiently attacked. We exploit a similar weakness in SDWCQ and note that [1], [11] both perform ad-hoc quantization of small vectors, ignoring established security measures such as a key-dependent dither vector as proposed in the QIM embedding framework [12].

In Section II, we briefly review the watermarking method proposed by Lin et. al [1] based on the 'Significant Difference of Wavelet Coefficient Quantization' (SDWCQ). Our attack is presented in Section III and after discussing the weakness, we propose a countermeasure in Section IV. Section V provides experimental results of the attack's performance and the robustness of the modified scheme. Finally, we conclude the paper in section VI with cautionary notes.

II. Watermarking Method

The SDWCQ method [1] selects the LH3 subband obtained by a 3-level DWT for watermark embedding. Consecutive coefficients of the subband are grouped into blocks of a fixed size, see Figure 1. The block size 7 is suggested in the paper as a tradeoff between capacity, robustness and security. A pseudo-random permutation of the blocks is performed and only the first N_w blocks are selected. Each block $1 \leq i < N_w$ encodes one bit of watermark information $w_i \in \{1, -1\}$ by imposing a constraint on the largest and second largest coefficient within the block. Let max_i and sec_i denote these two coefficient values for each block and $max_i - sec_i$ denotes the *significant difference*. If watermark symbol 1 is to be embedded in block i, max'_i is replacing max_i and set to

$$max'_i = \begin{cases} max_i + T, & \text{if}\,(max_i - sec_i) < \max(\epsilon, T)) \\ max_i, & \text{otherwise} \end{cases}, \quad (1)$$

where T is a threshold controlling the embedding strength (see [1]) and ϵ is the average significant difference value of all n blocks,

$$\epsilon = \left\lfloor \frac{1}{N_w} \sum_{i=1}^{N_w} (max_i - sec_i) \right\rfloor, \quad (2)$$

where $\lfloor \cdot \rfloor$ denotes the floor operator. Similarly, to embed -1, max'_i is set to equal sec_i.

For watermark extraction, an adaptive threshold γ is defined as

$$\gamma = \left\lfloor \frac{1}{\lfloor \alpha N_w \rfloor} \sum_{i=1}^{\lfloor \alpha N_w \rfloor} \varphi^\star_i \right\rfloor, \quad (3)$$

where $\varphi^\star_1 \leq \varphi^\star_2 \leq \ldots \leq \varphi^\star_{N_w}$ are the ordered significant differences of the received image and $0 < \alpha \leq 1$ is sensitive to the ratio between the two watermark symbols. For equiprobable watermark symbols, α is set to 0.9 (see [1] for details). The difference $max^\star_i - sec^\star_i$ between the largest and second largest coefficient of each received block is compared against γ to extract one bit of watermark information $w^\star_i$,

$$w^\star_i = \begin{cases} 1, & \text{if}\ (max^\star_i - sec^\star_i) \geq \min(\gamma, T) \\ -1, & \text{otherwise} \end{cases}. \quad (4)$$

To judge the presence of the watermark in the received image, the normalized correlation (NC) between the embedded and extracted watermark defined as

$$\mathrm{NC}(\mathbf{w}, \mathbf{w}^\star) = \frac{1}{N_w} \sum_{i=1}^{N_w} w_i w^\star_i \quad (5)$$

Supported by Austrian Science Fund project FWF-P19159-N13.

P. Meerwald, Ch. Koidl and A. Uhl are with the Department of Computer Sciences, University of Salzburg, A-5020 Salzburg, Austria (e-mail: {pmeerw, ckoidl, uhl}@cosy.sbg.ac.at).

⋆ Corresponding author. Phone +43-662-8044-6347, Fax +43-662-8044-172. EDICS: 1-ENCR.

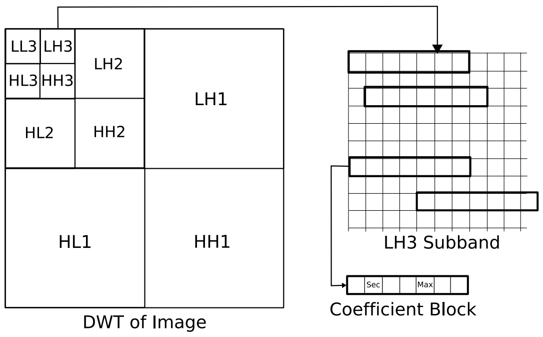


Fig. 1. Coefficients blocks in LH3 DWT subband

is compared against a decision threshold ρ. If $\mathrm{NC}(\mathbf{w}, \mathbf{w}^\star) \geq \rho$, the watermark is declared present, otherwise absent. For a watermark of length $N_w = 512$ and a false-positive probability of approximately 1.03×10^{-7}, ρ is set to 0.23.

III. Attack

The security measures employed by SDWCQ are the pseudo-random permutation of the blocks and the watermark bits. However, the permutations merely change the order in which blocks are watermarked and thus the block locations where watermark bits are embedded in the subband. In case the number of watermark bits N_w is smaller than the number of available blocks N_b, the attacker does not know which blocks to target. The application scenario [1] assumes $N_w = 512$, block-size 7 and for a subband size of 64×64 the number of available blocks $N_b = \left\lfloor \frac{64 \cdot 64}{7} \right\rfloor = 585$. Crucially, the permutations do not disguise which coefficients make up a block. Therefore an attacker can derive the values max_j and sec_j for all blocks $1 \leq j \leq N_b$ which potentially carry watermark information. In [1], the authors claim that targeting all largest coefficients would significantly degrade the image quality and thus the commercial value of the attacked copy. This is not the case as we show below.

The attack computes the significant difference for all blocks $1 \leq j \leq N_b$ in the subband LH3. If $max_j - sec_j < {}^{T^\diamond}\!/_2$, then block j is presumably carrying watermark symbol -1 which we want to change to encode 1. Hence, the attack increases the significant difference between the attacked coefficients $max_j^\diamond$ and $sec_j^\diamond$

$$max_j^\diamond = \begin{cases} max_j + T^\diamond + \Delta, & \text{if } (max_j - sec_j) < {}^{T^\diamond}\!/_2) \\ max_j, & \text{otherwise} \end{cases}, \quad (6)$$

where $T^\diamond$ is a crude estimate of the threshold T used for embedding. $T^\diamond$ can be easily determined by observing the first sharp increase in ordered significant differences, see Figure 2. The variable Δ is a small positive constant to guarantee that the significant difference is always $> T$, thus the extractor will always decode watermark symbol $w_i^\star = 1$ for all i (see Eq. 4). We set $\Delta = 2$ for all images. Results showing the effectiveness of the attack are presented in Section III. The watermark can be completely removed with an average PSNR of 54.59 dB between the watermarked and attacked image. Note that [1] defines $0 < \gamma \leq T$, therefore we apply $\min(\gamma, T)$ in Eq. 4, different from [1, Eq. 6]. Clearly, γ becomes much larger than T under attack (see Eq. 6 and Eq. 3).

We do not see the point in confining $\gamma \leq T$. In case we lift the constraint $\gamma \leq T$, we resort to a different attack strategy and aim to move the significant differences $\varphi_j = max_j - sec_j$ close to the decision threshold γ. The significant difference is increased by $T^\diamond + \Delta_1$ for blocks likely carrying watermark symbol -1, otherwise

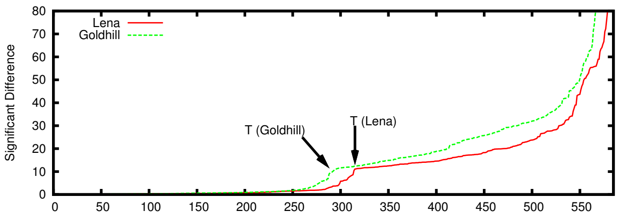


Fig. 2. Threshold T determined by observing the ordered significant differences φ_j for two watermarked images

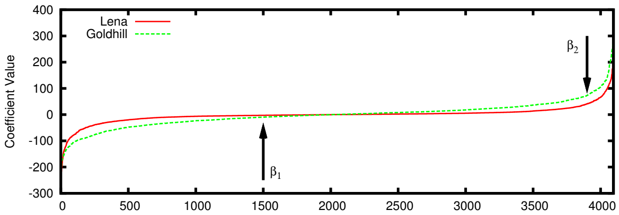


Fig. 3. Ordered wavelet coefficients ψ_j for two watermarked images

max_j is decreased by ${}^{T^\diamond}\!/_2 + \Delta_2$.

$$\begin{matrix} max_j^\diamond \\ sec_j^\diamond \end{matrix} = \begin{cases} \begin{matrix} max_j + ({}^{T^\diamond}\!/_2 + \Delta_1) \\ sec_j - ({}^{T^\diamond}\!/_2 + \Delta_1) \end{matrix}, & \text{if } (\varphi_j < {}^{T^\diamond}\!/_2) \\ \begin{matrix} max_j - ({}^{T^\diamond}\!/_2 + \Delta_2) \\ sec_j \end{matrix}, & \text{if } (\varphi_j < {}^{3T^\diamond}\!/_2 + \Delta_2) \end{cases} \quad (7)$$

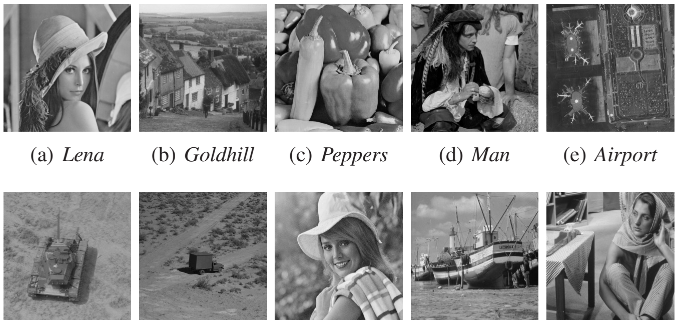
Δ_1 is set to 2 as before and Δ_2 is determined for each image such that slightly more than 128 likely locations for watermark symbol 1 are altered (assuming ratio 1 : 1 between watermark symbols). Again, the watermark can be completely removed. The average PSNR is 53.56 dB, with more detailed results in Section III.

IV. Discussion and Countermeasure

The previous section shows how an attacker can exploit knowledge of the watermarking scheme's implementation to gain access to the embedding locations. Specifically, the embedding subband (LH3), the formation of consecutive coefficients into blocks and the quantization rule (Eq. 1) are utilized. If kept secret, the embedding threshold T and the block size can be easily estimated from the received image. The two pseudo-random permutations ($Per(S1, N_w)$ and $Per(S2, 4096/7)$ in [1]) fail to protect the embedding locations. According to Kalker's definition [4], the SDWCQ method is insecure because the attacker can manipulate the raw watermark channel of significant differences and thus remove the watermark while maintaining a high PSNR for the attacked image. Further, the weakness permits to copy a watermark to another image.

A simple countermeasure is to establish a key-dependent pseudo-random mapping of wavelet coefficients to coefficient blocks. For example, we can apply the pseudo-random permutation function Per defined in [1] with a secret seed $S3$ on the wavelet coefficients of subband LH3, $Per(S3, 4096)$, before grouping non-overlapping wavelet coefficients into blocks. This modification conceals which wavelet coefficients make up a block, thus the significant differences can not be determined and the attack proposed in the previous section is mitigated. A related alternative modification was proposed

Even without having access to the significant differences, we can use properties of the SDWCQ method to attack the watermark. First, the SDWCQ scheme constrains embedding of the watermark to the



(a) *Lena* (b) *Goldhill* (c) *Peppers* (d) *Man* (e) *Airport*

(f) *Tank* (g) *Truck* (h) *Elaine* (i) *Boat* (j) *Barbara*

Fig. 4. Ten 512×512 gray-scale test images

LH3 subband of the DWT. Second, only large positive coefficients are likely to contribute to the significant difference. Third, setting max'_i equal to sec_i in order to embed -1 might result in an increased number of wavelet coefficients pairs with the same value, thus revealing potential embedding locations of $w_i = -1$.

It is well known that the energy of wavelet detail subband coefficients is concentrated in just a few large coefficients for natural images. Based on this fact and the first two assumptions above, we can design an attack which sets all positive coefficients to zero, excluding only the largest. Formally, let $\psi_1 \leq \psi_2 \ldots \leq \psi_{N_c}$ denote the $N_c = 4096$ ordered wavelet coefficients of subband LH3. Then choose two indices $\beta_1 < \beta_2$ and set

$$\psi_j^{\diamond} = \begin{cases} 0, & \text{if } (\beta_1 \leq j \leq \beta_2) \\ \psi_j, & \text{otherwise} \end{cases} . \tag{8}$$

Reasonable values are $\beta_1 = 1500$ and $\beta_2 = 3900$, see Figure 3. Since the image's energy is concentrated mainly in large coefficients and negative coefficients are hardly affected, the image quality is not severely degraded. The average watermark correlation is reduced to 0.156, well below the detection threshold. The average PSNR between the watermarked and attacked image is 42.57 dB. See Table IV for detailed results.

V. Results

The implementation of the SDWCQ watermarking scheme, its modification and the related attacks are available as Python code at http://www.wavelab.at/sources. For our experiments, we use ten 512×512 gray-scale image freely available from the USC SIPI image database[1], see Figure 4.

We embed a random watermark sequence of length $N_w = 512$ with approximately the same number of watermark symbols 1 and -1 in each image. Note that Lin et al. [1] also consider the case where the ratio is $1 : 3$ which might be useful for binary logo watermarking where the logo comprises an uneven number of black and white pixels. The ratio between watermark symbols affects the embedding strength in terms of PSNR: with equiprobable symbols, the PSNR is lower than indicated in [1]. To compensate, we choose $T = 12$ instead of $T = 10$.

The Daubechies-7/9 wavelet filter is used for the DWT. The block size is set to 7 as suggested. For watermark extraction the parameter α is set to 0.9 to reflect the even distribution of watermark symbols (see [1, Fig. 12]). In the following we evaluate our attack on SDWCQ (including the detection variant described in Section III) and on the modified SDWCQ scheme proposed in Section IV. The experiment is repeated ten times and we report the averaged normalized correlation (NC) for the extracted watermark as well the PSNR (dB) between the watermarked and attacked image (w,a), the original and attacked image (o,a), and the original and watermarked image (o,w).

TABLE I

Attack results on the SDWCQ scheme averaged over 10 test runs for block-size 7, $N_w = 512$, $T = 12$ and $\alpha = 0.9$

Image	$\varnothing$ NC	$\varnothing$ PSNR (dB)		
		(w,a)	(o,a)	(o,w)
Lena	−0.091	54.58	46.89	46.63
Goldhill	−0.039	54.64	46.47	45.91
Peppers	−0.056	54.47	45.39	45.05
Man	0.006	54.65	43.31	42.85
Airport	−0.028	54.53	45.63	45.10
Tank	−0.022	54.58	49.71	48.97
Truck	−0.014	54.63	45.59	44.96
Elaine	−0.063	54.54	47.52	47.37
Boat	−0.047	54.69	46.24	45.82
Barbara	−0.041	54.60	46.62	46.19
Average	−0.039	54.59	46.34	45.88

TABLE II

Attack results on the SDWCQ scheme (γ unrestrained) averaged over 10 test runs (same parameters)

Image	$\varnothing$ NC	$\varnothing$ PSNR (dB)		
		(w,a)	(o,a)	(o,w)
Lena	0.020	54.42	46.42	46.63
Goldhill	−0.109	53.36	45.79	45.91
Peppers	−0.023	54.08	45.02	45.05
Man	0.025	51.94	42.70	42.85
Airport	−0.108	53.00	45.00	45.10
Tank	−0.112	54.22	48.81	48.97
Truck	−0.121	52.43	44.79	44.96
Elaine	−0.066	54.39	47.01	47.37
Boat	−0.040	53.79	45.69	45.82
Barbara	−0.014	53.96	46.04	46.19
Average	−0.055	53.56	45.73	45.88

TABLE III

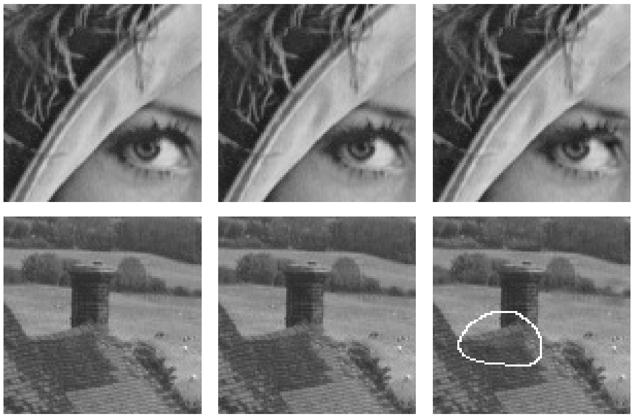
Attack results on the SDWCQ scheme (symbol ratio 1:3) over 10 tests runs (block-size 7, $N_w = 512$, $T = 10$ and $\alpha = 0.6$)

Image	$\varnothing$ NC	$\varnothing$ PSNR (dB)		
		(w,a)	(o,a)	(o,w)
Lena	−0.021	53.13	44.74	45.07
Goldhill	0.083	52.53	44.05	44.33
Peppers	−0.043	52.80	43.48	43.62
Man	0.026	50.70	41.04	41.45
Airport	−0.030	51.87	43.35	43.64
Tank	−0.024	53.58	47.41	47.72
Truck	0.054	51.67	43.08	43.30
Elaine	−0.056	53.44	45.62	45.97
Boat	−0.063	52.60	43.91	44.21
Barbara	−0.031	53.24	44.22	44.49
Average	−0.011	52.56	44.09	44.38

Table I presents the results of the attack on the SDWCQ watermarking method. The averaged normalized correlation is close to zero for all images, the watermark is completely removed. The PSNR between the watermarked and attacked image is 54.59 dB on average, significantly higher than the average embedding PSNR of 45.88 dB between the original and watermarked image. Overall, the PSNR of the attacked image is 0.46 dB higher compared to the watermarked image. The results for the SDWCQ variant with unrestrained γ are provided in Table II. Again, the watermark is completely removed but the PSNR of the attacked image against watermarked image is approximately 1 dB lower than before, 53.56 dB.

Regarding the case where the watermark comprises $\{-1, 1\}$ sym-

[1] http://sipi.usc.edu/database/



(a) original image (b) SDWCQ attack (c) modified SDWCQ attack

Fig. 5. Image quality of cropped image region after attack on the *Lena* and *Goldhill* image; PSNR (dB): 46.78 and 46.51 for the attack on SDWCQ, 41.52 and 36.49 for the attack on modified SDWCQ

TABLE IV
ATTACK RESULTS ON THE MODIFIED SDWCQ SCHEME AVERAGED OVER 10 TEST RUNS FOR BLOCK-SIZE 7, $N_w = 512$, $T = 12$ AND $\alpha = 0.9$

Image	∅ NC	∅ PSNR (dB)		
		(w,a)	(o,a)	(o,w)
Lena	0.176	46.68	41.88	44.14
Goldhill	0.158	39.83	36.54	40.55
Peppers	0.145	45.37	39.54	41.42
Man	0.132	40.31	36.62	40.20
Airport	0.165	41.02	38.19	42.62
Tank	0.148	42.79	40.59	45.78
Truck	0.157	39.63	37.68	43.80
Elaine	0.156	45.96	40.95	43.20
Boat	0.166	40.16	37.23	41.60
Barbara	0.153	43.99	39.53	42.18
Average	0.156	42.57	38.88	42.55

bols in the ratio $1 : 3$ we note that the scale parameter α for the detector has to be changed to 0.6 (see [1], Fig. 12) and $T = 10$ now. It can easily be verified that the detection threshold ρ has be to adapted to maintain the target false positive error rate. If we assume a probability of error (P_E) of 0.25 for each watermark bit, the threshold 0.68 results in a probability of false positive error (P_{fp}) of 5.86×10^{-7} according to [1], Eq. (9). The NC can be reduced to zero as before, however at a slightly larger expense in PSNR. Note that in practice is would be sufficient to reduce the NC just below the detection threshold. The attack performance is illustrated in Table III.

In Table IV we report the results for the proposed targeted attack on the modified SDWCQ scheme which occludes the embedding locations. We observe that the normalized correlation, 0.156 on average, is consistently below the detection threshold of 0.23 (for a false-positive rate of 10^{-7}). The PSNR between the original and attacked image is 38.88 dB on average yet the images have good perceptual quality as confirmed by visual inspection. We also assess the objective image quality using the SSIM metric [13]. For the watermarked images, the SSIM is 1 (perceptually identical). The average SSIM value for the attacked images is 0.98. For comparison, JPEG compression (Q=95) which has a very minor impact on the perceived image quality, also yields 0.98 on the SSIM scale. So even for the low PSNR (o,a) value of 38.88 dB, the perceptual quality of the attacked images is maintained according to the SSIM metric. Hence, also the modified SDWCQ method must be considered broken. The proposed attack would not be successful if the watermark energy would be spread over more subbands.

In Figure 5 we confirm that the attacked images are visually almost identical to the original image using cropped 96×96 image regions of the *Lena* and *Goldhill* image. Only in direct comparison, differences become noticeable; for example the tiles on the roof of the *Goldhill* image appear slightly brighter (marked with white circle). The PSNR between the original and the attacked SDWCQ images shown is 46.78 and 46.51 dB; the PSNR after attack on the modified SDWCQ scheme is 41.52 and 36.49 dB for *Lena* and *Goldhill*, respectively.

With the modified SDWCQ method, the average PSNR of the watermarked images is more than 3 dB lower compared to the original scheme for the same embedding parameters. Due to pseudo-random assignment of the coefficients to a block, the average significant difference is increased. Hence, in case watermark symbol -1 is embedded, the coefficient max'_i is on average changed by a larger amount; see Eq. 1. Consequently, the modified SDWCQ scheme does not suffer from blocks with approximately equal-valued coefficients due to smooth image regions and the robustness is improved.

The attack on SDWCQ relates to the security of the scheme as an unauthorized user can gain access to the watermark bits. It is then possible to alter or copy the watermark. On the other hand, the attack on the modified SDWCQ scheme relates to the robustness of the watermarking method as it is not possible to directly alter individual watermark bits or copy the watermark information.

VI. CONCLUSION

This paper presents an attack on the SDWCQ method, a recently published watermarking scheme for copyright protection. The attack exploits knowledge of the scheme's implementation and the lack of protection of the embedding locations to completely remove the watermark with high PSNR. Further, we propose a simple modification to SDWCQ which occludes the quantized coefficients' locations, inhibiting the attack. However, also modified SDWCQ is prone to a targeted attack.

We highlight the need for a detailed security analysis, assuming the attacker is familiar with the watermarking scheme's implementation. We expect several quantization based watermarking schemes to be vulnerable to similar attacks. Evaluation of the robustness against common signal processing operations is insufficient for watermarking schemes in the copyright protection scenario.

REFERENCES

[1] W.-H. Lin, S.-J. Horng, T.-W. Kao, P. Fan, C.-L. Lee, and Y. Pan, "An efficient watermarking method based on significant difference of wavelet coefficient quantization," *IEEE Transactions on Multimedia*, vol. 10, no. 5, pp. 746–757, Aug. 2008.

[2] F. Cayre, C. Fontaine, and T. Furon, "Watermarking security: theory and practice," *IEEE Transactions on Signal Processing*, vol. 53, no. 2, pp. 3976–3987, Oct. 2005.

[3] A. Kerckhoffs, "La cryptographie militaire," *Journal des sciences militaires*, vol. 9, pp. 5–83, Jan. 1883.

[4] T. Kalker, "Considerations on watermarking security," in *Proceedings of the IEEE Workshop on Multimedia Signal Processing, MMSP '01*, Cannes, France, Oct. 2001, pp. 201–206.

[5] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Attacks on copyright marking systems," in *Information Hiding: Second International Workshop*, ser. Lecture Notes in Computer Science, D. Aucsmith, Ed., vol. 1525. Portland, OR, USA: Springer Verlag, Berlin, Germany, Apr. 1998, pp. 218–238.

[6] S. Voloshynovskiy, S. Pereira, T. Pun, J. K. Su, and J. J. Eggers, "Attack on digital watermarks: Classification, estimation-based attacks and benchmarks," *IEEE Communications Magazin*, vol. 39, no. 8, pp. 118–126, Aug. 2001.

[7] P. Comesana, L. Perez-Freire, and F. Perez-Gonzalez, "Blind newton sensitivity attack," *IEE Proceedings on Information Security*, vol. 153, no. 3, pp. 115–125, Sep. 2006.

[8] A. Piva and M. Barni, “The first BOWS contest: break our watermarking system,” in *Security, Steganography, and Watermarking of Multimedia Contents IX*, ser. Proceedings of SPIE, E. J. Delp and P. W. Wong, Eds., vol. 6505. San Jose, CA, USA: SPIE, Jan. 2007.

[9] F. A. P. Petitcolas, C. Fontaine, J. Dittmann, M. Steinebach, and N. Fatès, “Public automated web-based evaluation service for watermarking schemes: Stirmark benchmark,” in *Proceedings of SPIE, Security and Watermarking of Multimedia Contents III*, vol. 4314, San Jose, CA, USA, Jan. 2001, pp. 575–584.

[10] T. K. Das and S. Maitra, “Analysis of the ’Wavelet Tree Quantization’ watermarking strategy and a modified robust scheme,” *Multimedia Systems*, vol. 12, no. 2, pp. 151–163, Aug. 2006.

[11] S.-H. Wang and Y.-P. Lin, “Wavelet tree quantization for copyright protection watermarking,” *IEEE Transactions on Image Processing*, vol. 13, no. 2, pp. 154–165, Feb. 2004.

[12] B. Chen and G. W. Wornell, “Quantization index modulation: A class of provably good methods for digital watermarking and information embedding,” *IEEE Transactions on Information Theory*, vol. 47, no. 4, pp. 1423–1443, May 2001.

[13] Z. Wang, A. Bovik, H. Sheikh, and E. Simoncelli, “Image quality assessment: from error visibility to structural similarity,” *IEEE Transactions on Image Processing*, vol. 13, no. 4, pp. 600–612, Apr. 2004.