Dual Watermarking for Protection of Rightful Ownership and Secure Image Authentication

Mathias Schlauweg, Dima Pröfrock, Benedikt Zeibich and Erika Müller
Institute of Communications Engineering, Faculty of Computer Science and Electrical Engineering
University of Rostock
Rostock 18119, Germany
+49 (0) 381 498 7304

{mathias.schlauweg, dima.proefrock, benedikt.zeibich, erika.mueller}@uni-rostock.de

ABSTRACT

A digital watermarking approach highly robust to lossy image compression is presented. It is shown how geometrically warping objects can be used to imperceptibly embed information into images for the purpose of property rights protection. Common lossy image compression is optimized for maintaining the geometric image structure. Hence, as we demonstrate, the embedded information is not affected by a successive embedding approach in the compression domain. This second watermarking scheme is used for an efficient JPEG2000-based image authentication, which is robust to JPEG compression and other allowed signal processing operations. We enhance positive wavelet-based watermarking approaches proposed in recent years by image adaptive perceptual modeling and error correction coding without raising a security gap. Our new method is secure in contrast to most of the schemes proposed so far. Lots of popular features of the JPEG2000 compression framework such as quality and resolution scalability, lossless image rotation and flipping are supported. All coefficients of the wavelet decomposition are protected using our new extended scalar quantization and hashing scheme.

Categories and Subject Descriptors

D.2.11 [**Software Engineering**]: Software Architectures – *Information Hiding;* H.2.0 [**Database Management**]: General – *Security, Integrity and Protection;* H.3.1 [**Information Storage and Retrieval**]: Content Analysis and Indexing – *Indexing Methods;* I.4.9 [**Image Processing and Computer Vision**]: Applications*;* K.6.5 [**Management of Computing and Information Systems**]: Security and Protection – *Authentication, Insurance.*

General Terms: Algorithms, Security, Verification.

Keywords: Dual watermarking, normed centre of gravity (NCG), authentication, JPEG2000, error correction coding (ECC).

1. INTRODUCTION

With the increasing reliance on digital media and the unprecedented growth of internet distribution possibilities, methods for integrity verification of digital contents are also continually acquiring increasing importance. Since digital images can be modified or forged by a wide variety of available manipulation software, it is rather difficult to tell if a picture is the original one or if it has been tampered with. Further, the illegal distribution of copyrighted contents without any quality degradation is facilitated and hence copyright protection is becoming increasingly important as well.

Digital watermarking is a technique that embeds information into host multimedia signals in an imperceptible way and promises to be the enabling technology for intellectual property rights protection and data security [1]. One significant advantage of the digital watermarking approach is that the protection is robustly integrated with the raw media data, independent of the specific representation format. The embedded data should survive any signal processing operation the host signal goes through such as lossy compression or digital-to-analog conversion. In other words, if someone is able to remove the watermark, the perceptual quality of the host signal should be destroyed as well.

In general, the watermark embedding process affects the fidelity of the underlying host signal. Fidelity, robustness and the amount of data, which can be embedded without visible artifacts, often conflict. Most of early watermarking techniques have focused on embedding the watermark information applying a global power constraint such as the Peak-Signal-to-Noise-Ratio (PSRN) to satisfy fidelity constraints. But, the PSNR value is unparticular reflecting human's visual system, because local image properties such as edges or textures are not considered. Later on, watermarking systems have been proposed that allowed the embedded signal to be locally varied in response to the local properties of the corresponding host signal [2], [5], [13]. In this paper, we actually go the extra mile and neglect the PSNR value. We use the fact that all common lossy image compression techniques are PSNR-optimized. We embed watermark information by geometrically shifting objects and object borders in a given host image. If an observer has no original image for comparison, the embedding process is imperceptible. As a consequence, this approach turns out to be extremely robust to common image compression.

After we propose our new embedding technique in Section 2 and show the robustness to JPEG as well as JPEG2000 compression, we introduce a second watermark embedding stage that embeds further information during image compression (Section 3). Experimental results and analyses are given in section 4. Section 5 concludes our work.

MCPS'06, October 27, 2006, Santa Barbara, California, USA.

2. DIGITAL WATERMARKING ROBUST TO COMMON LOSSY COMPRESSION

Multimedia compression tries to convey the information in a multimedia content as efficiently as possible, with the fewest number of bits. Digital watermarking, on the other hand, tries to sneak additional bits of information into the original content. As the "additional information" does nothing to improve the quality of the content, an ideal compressor would completely suppress the hidden information.

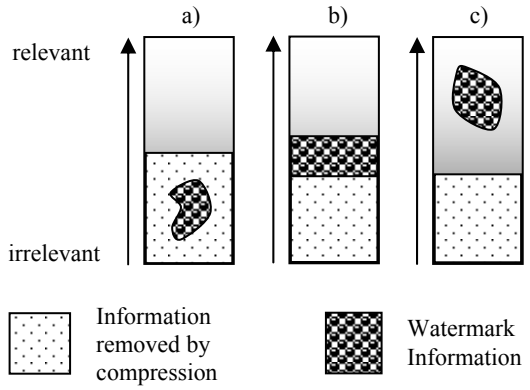

Figure 1. Watermark embedding using gaps of compression algorithms a), with defined embedding strength b) or using relevant image/video information c)

The optimal way to embed watermark information with robustness to lossy compression is to embed the watermark in the relevant part of the data. Because common compression algorithms are PSNR-optimized, usually the relevance is defined by the PSNR value. Because of this PSNR optimization, compression algorithms for videos as well as images try to maintain the geometric structure. Slightly shifting objects or object borders would yield strong degradation of the PSNR value although the modification is imperceptible to a human observer. For example see Figure 2. The PSNR between both images is 27.7 dB, usually a value associated with strong lossy compression in conjunction with visible artifacts, e.g., block artifacts known from JPEG compression. However, the visible difference between the two images shown in Figure 2 is imperceptible. A watermarking approach using this kind of shifting or scaling objects would be very robust to lossy compression.

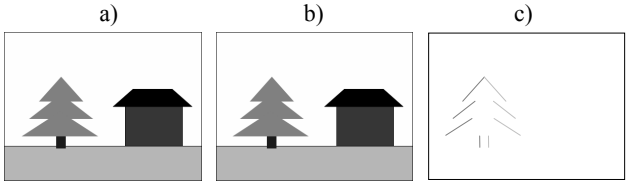

Figure 2. Original image a), image changed by geometric warping b), difference image c). The geometric warping moved the tree some pixels to the left.

Figure 3 shows a frame from the test video sequence "Bus". After slight as well as strong lossy compression with the state-of-the-art video compression standard H.264/AVC the spatial position and size of objects or object borders remain unchanged.

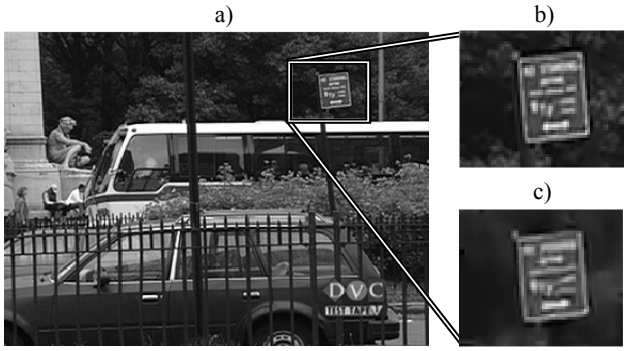

Figure 3. Spatial position and size of the traffic sign remain unchanged after slight b) as well as strong c) lossy compression

2.1 The NCG-Geometric-Warping Approach

In [5], we proposed to change the geometric structure of single video frames, or in other words the position and size of objects, to embed watermark information. We introduced a new statistic, the Normed Centre of Gravity (NCG), which describes the gravity centre of gray value pixel blocks. We demonstrated the high robustness to the new H.264/AVC video compression standard, developed for a broad range of applications.

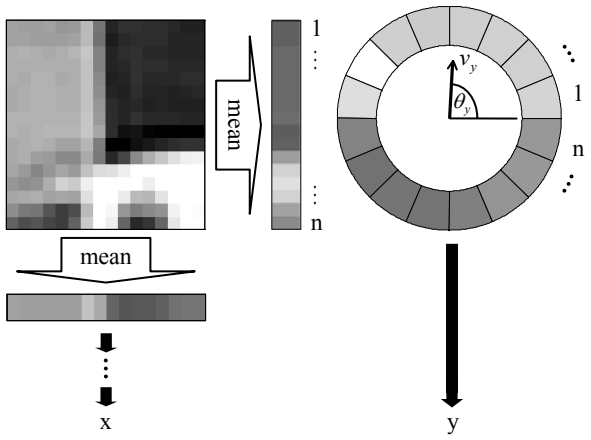

Figure 4. Computing scheme for the NCG x,y-coordinates

Every video frame is separated into non-overlapping pixel blocks in the spatial domain. The mean values of all rows and all columns of these blocks are computed, yielding the vectors $\underline{m}_x$ and $\underline{m}_y$. Both vectors are arranged in two circles, as shown in Figure 4. Afterwards, the 2-dimensional vector $\underline{v}_k$ (k = x or y) is computed:

$$v_k = \begin{pmatrix} \sum_{i=1}^{n} m_k(i) \cdot \cos\left(\frac{\pi}{n} + \left((i-1)\cdot\left(\frac{2\cdot\pi}{n}\right)\right)\right) \\ \sum_{i=1}^{n} m_k(i) \cdot \sin\left(\frac{\pi}{n} + \left((i-1)\cdot\left(\frac{2\cdot\pi}{n}\right)\right)\right) \end{pmatrix} \quad (1)$$

For both vectors, angle θ_k and length L_k are computed. The vector angles are used to determine the x,y-coordinates of the blocks gravity centre, that are independent from block borders.

$$x = \frac{n \cdot \theta_x}{2 \cdot \pi} \qquad y = \frac{n \cdot \theta_y}{2 \cdot \pi} \tag{2}$$

To embed watermark bits, robust blocks have to be chosen, and it must be able to find the same blocks during watermark extraction although, e.g., lossy compression has been performed. Robust blocks are blocks with high $L = \sqrt{L_x^2 + L_y^2}$. In [5], we determined a threshold L = 430 for blocks robust to H.264/AVC compression with even very low data rates. We suggested creating a gap around this threshold to tolerate slight changes due to compression. Further, a mapping process was presented that allows using a quantization-based watermark embedding approach [9] to hide information within the host video frame. The structure of the quantization lattice is self-adapting depending on L_x and L_y. For a detailed description of the computation and the mapping process we refer the reader to [5].

The watermark embedding process results in visible artifacts, as shown in Figure 5 b) and c). However, the visible difference is imperceptible if an observer does not compare single pixels of the original and the watermarked frame. The frame in Figure 5 a) contains 22 watermarked blocks at a resolution of 352x288 pixels. For instance, the wooden bole in the bottom right corner contains six of them. But, without comparing the original pixels with the changed pixels nobody is able to notice these blocks.

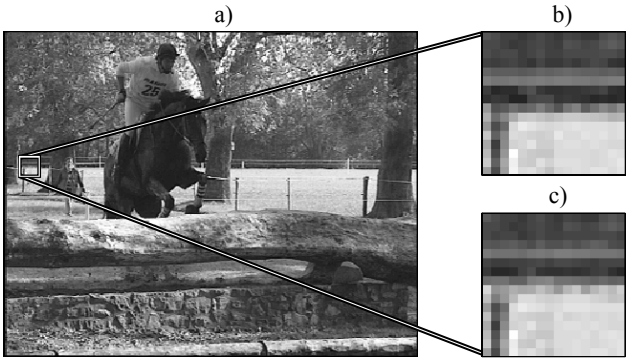

Figure 5. Watermarked frame of test video "Horse" a), original block b) and watermarked block c)

2.2 Using the NCG Approach for Still Images

Although H.264/AVC intra frame coding can also be used to compress still images it is obvious to test the robustness of our new NCG statistic to common JPEG and JPEG2000 still image compression. Of course, the embedding capacity of the proposed geometric warping scheme is low compared to other watermarking approaches commonly used for still images. But, due to the fact that the few embedded bits are very robust to compression, we claim that this approach can be combined with a second watermarking process working in the compression domain. This second embedding process should not affect the information previously hidden imperceptibly in the spatial domain.

The term Dual Watermarking is often used in the literature. Two different watermarks are embedded in the same host data to aim at different applications. For instance, in 0, the authors proposed a dual watermarking technique in the DWT domain for intellectual property protection and authentication. In [3], a DCT-DWT approach is presented combining image authentication (primary watermark) and compression of color components (secondary watermark). In [4], a JPEG2000-based approach is presented to protect content integrity by embedding a fragile and a robust watermark into different resolution layers and different embedding regions of a host image. But, all these approaches have in common that the second embedding process slightly affects the robustness of the firstly embedded bits. Because our approach does not, we claim a new meaning for our "dual watermarking".

Information which is embedded during the second watermarking process could be a signature for image authentication, as we show in the next section. Also, it could be any kind of data for re-synchronization of the firstly embedded watermark to enhance the robustness of the overall scheme to, e.g., geometric attacks such as image rotation, scaling or translation.

Figure 6. Watermarked still image "Lena" with 18 bits embedded (left), difference to the original (right)

In Figure 6, the well known standard test image "Lena" is shown watermarked using the geometric warping approach. 18 bits have been embedded into the 512x512 pixel image using the same threshold L = 430 as in the tests of robustness to H.264/AVC compression. We tested the robustness to JPEG as well as JPEG2000 compression for a larger set of images from the uncompressed colour image database UCID [15]. As can be seen in Figure 7 and Figure 8, our new NCG statistic is robust to strong still image compression, too. The amount of bits that can be embedded during the watermarking process depends on the image content and the threshold L. If an image has more homogenous areas, less robust blocks will be found for embedding.

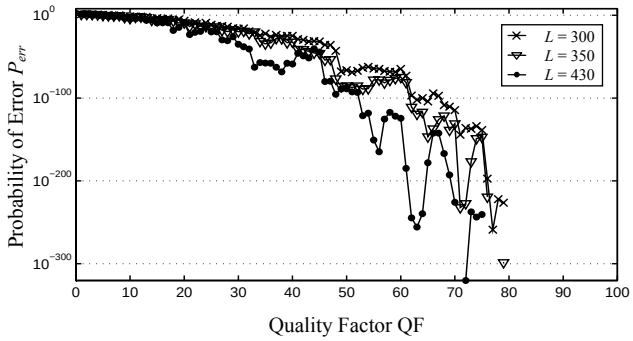

Figure 7. Robustness to lossy JPEG compression

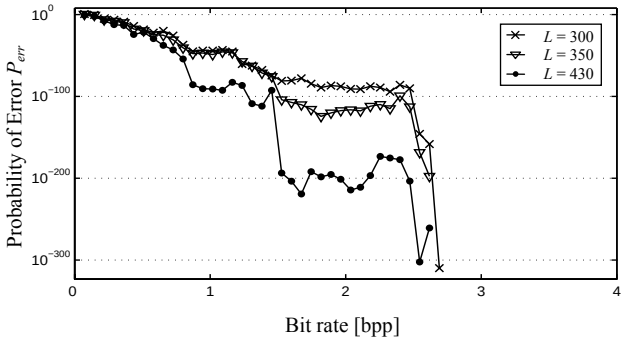

Figure 8. Robustness to lossy JPEG2000 compression

For instance, using the image "Lena" at L = 300 we are able to embed 48 bits, that are even robust to JPEG2000 compression at 0.2 bpp, usually a value associated with strong visible artifacts. The probability of occurrence of errors for this case is lower than 0.0001 percent, which could be improved using error correction coding if necessary.

3. DIGITAL WATERMARKING IN THE COMPRESSION DOMAIN USED FOR SECURE IMAGE AUTHENTICATION

Since the geometric warping watermarking approach using the proposed NCG statistic turns out to be robust to compression, we can append a second embedding stage that works during image compression. As mentioned above, the first stage could be used to embed data for copyright issues. The secondly embedded watermark could be a signature for authentication purpose to check the image for content manipulations.

The integrity of a digital image is pre-eminent in fields such as forensics, medical imaging and military or industrial photography. For example, courts make decisions affecting an individual's liberty based, in part, on images presented as evidence. The burden of proof of authenticity always lies with the person seeking to admit. He must provide other evidence to support this authenticity. Further, military photographs may determine target locations based on their content and interpretation. Thus, it is important to maintain the integrity of all images from capture through final use.

To prevent illegitimate tampering and fraudulent use of modified images authentication techniques were introduced. As known from the classical cryptography, to verify the exact data integrity, a signature may be generated from the source signal by the use of secure hash functions and encryption. A recipient decrypts the signature and matches it with the hash generated from the received signal. If even one bit of the signal has been modified, it will no longer match the signature, so any tampering can be detected. But this so-called fragile property is sometimes not practical when considering distribution of images. For instance, lossy compression has to be performed to reduce the amount of data or signal processing is applied to correct gamma, to de-noise or to resample an image. These manipulations change the pixel values but not the content and hence not the authenticity.

To tolerate certain kinds of signal processing semi-fragile authentication methods for digital images have been developed. The aim is to allow admissible manipulations such as JPEG compression, but to reject malicious manipulations that change the visual content. Commonly used techniques extract features representing the image content and re-embed these features as watermark information into the host image data [3], [4], [7-12]. Some approaches involve image positions of edges, contours or zero-crossings in the spatial domain whose existence is proved during the verification process. Other methods are based on single coefficients or on relationships between pairs of different coefficients in the transform domain (e.g., DCT, DWT or DFT).

In [12], we analyzed authentication systems in the DCT domain of JPEG compression and found out that large tolerance margins are required resulting in dramatic security gaps. The coefficients of the wavelet domain turn out to be much better suited for authentication watermarking purpose. Because DWT is a global transform, watermark embedding in the low frequency coefficients does not result in block artifacts in watermarked images, as shown in [13]. Hence, we generate and embed the image content dependent features in the wavelet domain of JPEG2000.

Our proposed system works very efficiently, since it is directly integrated in the JPEG2000 compression process. The framework is structured modularly so that single components such as the used hash function or the encryption scheme can be replaced without influencing the overall functionality.

3.1 Feature Extraction in the DWT-domain

As opposed to the JPEG compression framework, the quantization in JPEG2000 is bit-plane oriented. The quantization interval is always an exact power of two and hence simple JPEG2000 re-compression does not require the coefficients to be re-quantized. This is also the basis for the well known "encode once; decode many" strategy of the JPEG2000 specification [14]. But even if small allowed operations are applied to the watermarked image in the spatial domain, the upper bit-planes of the quantized DWT-coefficients turn out to be very stable. Thus, for our authentication scheme, we define an extended version of the scalar dead-zone quantization technique used in the JPEG2000 coding framework. This extension is completely new and outperforms existing quantization-based watermarking approaches in the wavelet-domain of JPEG2000, such as the one in [11].

The image **I** is DWT-transformed with the bi-orthogonal 9/7-wavelet filter, at first, and approximated by a finite number of bit-planes ($0 \le b \le b_{\max} \le \text{sign}$).

$$\mathbf{I} \overset{\text{DWT}}{\mapsto} \mathbf{W} = \left\{ \mathbf{W}_b,\ 0 \le b \le b_{\max} \le \text{sign} \right\} \qquad (3)$$

Afterwards, the transformed image **W** has to be pre-quantized using the step size δ. Therefore, every wavelet coefficient $\boldsymbol{w}$ of the transformed image is quantized to an invariant value, which is not changed during the signature embedding process [9]. Except for the dead-zone, the magnitude of every coefficient is set to the centre of the according δ-sized hash interval, in Figure 9 marked with the symbols **II**. Coefficients in the ranges $[-\delta \le \boldsymbol{w} \le -\delta/2]$ or $[\delta/2 \le \boldsymbol{w} \le \delta]$ are set to -δ/2 or δ/2 respectively. The other coefficients of the dead-zone are left unchanged resulting in higher image quality. We justify this approach by the fact that DWT coefficients are most often very small due to the very good energy concentration capability of the wavelet transform. Finally, all

coefficients can be hashed using a secure cryptographic hash function, such as MD5, SHA-1 or SHA-256.

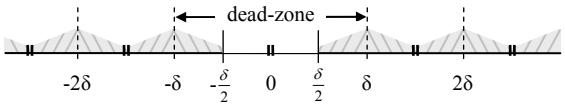

Figure 9. Extended scalar quantization with dead-zone

3.2 Variable Resolution

To support various resolutions, we propose to divide the DWT-transformed image **W** into Z regions $\mathbf{W}^1$, $\mathbf{W}^2$, ..., $\mathbf{W}^Z$, as shown in Figure 10. From every region $\mathbf{W}^i$ or, in other words, from every DWT-level a hash value $\mathfrak{H}(\mathbf{W}^i)$ is calculated.

Figure 10. Different hashes to support resolution changes

If the coefficients of $\mathbf{W}^1$ are set to zero, the hash values of all other DWT-levels $\{\mathfrak{H}(\mathbf{W}^2),...,\mathfrak{H}(\mathbf{W}^Z)\}$ do not change.

$$h = \{\mathfrak{H}(\mathbf{W}^1), \mathfrak{H}(\mathbf{W}^2), ..., \mathfrak{H}(\mathbf{W}^Z)\} \quad (4)$$

This multi-hash approach makes the watermarked image robust to resolution changes that are powers of two. The "encode once; decode many" strategy of the JPEG2000 specification directly benefits from this approach.

The bit length of the overall hash h must be less than the maximum signature key length of the encryption scheme. For example, in our tests, we used Z = 4 levels for the DWT decomposition, MD5-hashing (128 bit each) and 728 bit RSA-encryption. Besides the bits used for the hash value h, we also include position, date and time of the image capture process in the data to be encrypted. This should deter a forger from photographing fake sceneries at a different position or different time using the same camera.

3.3 Watermark Embedding

To embed the encrypted signature as a watermark we use the well-known quantization index modulation technique called dither modulation. Roughly speaking, the used host signal samples are mapped bit-wise to the elements of a set of two different quantizers, as can be seen in Figure 11. Except for the dead-zone, in every hash interval there are two quantization points, marked with ✖'s and ○'s. If a binary information bit "0" has to be embedded, the coefficient magnitude is set to the point marked with ✖, otherwise, the point marked with ○ is chosen. For more detailed descriptions, we refer to [9].

A special case occurs, if the used coefficient is in the dead-zone and a binary bit "1" has to be embedded. In this case we suggest applying the following extended equations to achieve lower embedding induced distortions:

$$\begin{aligned} &\text{if} \quad -\delta \le w \le -\delta/4 \quad \text{then} \quad w = -\delta/4 \\ &\text{if} \quad \delta/4 \le w \le \delta \quad \text{then} \quad w = \delta/4 \\ &\qquad\qquad \text{else don't change } w \end{aligned} \quad (5)$$

Since the quantization in JPEG2000 is bit-plane oriented, the embedding process only affects one single bit-plane, which we identify by $\mathbf{W}_s$. The bit-planes below $\mathbf{W}_s$ remain unchanged, since they were set to zero due to the pre-quantization process.

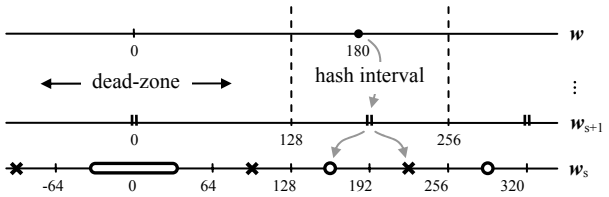

Figure 11. Watermark embedding process using an extended dither modulation (QIM)

We suggest applying error correction coding (ECC) to the signature before embedding takes place. In our tests, we use BCH(511,367,16) coding and embed the resulting 1022 bits in the upper LL-subband of the wavelet decomposition. Finally, the watermarked image may either be transferred as JPEG2000-compressed file or be transformed back to the spatial domain.

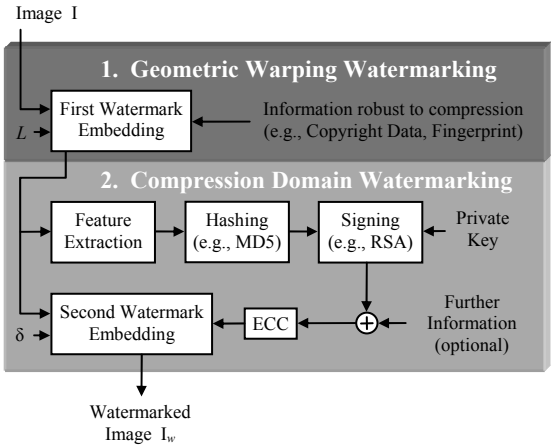

Figure 12. Watermark generation and embedding

At the verification site, the watermark bits are extracted by nearest neighbor quantization to one of the two quantizer subsets. Afterwards, error correction coding is used to get the submitted signature bits. If the watermarked image has been distorted by, e.g., lossy file format conversions, error correction coding can help to reconstruct the distorted signal samples. Without ECC, the allowed distortion to the watermarked coefficients would be only δ/4 but using ECC errors with an absolute value δ/2 can be

reconstructed, as in Figure 14. The quantization cell may be thought of as a shifted overlapped version of the original cell. Hence, the range of accepted channel distortion is raised without security loss, as we demonstrated in [9].

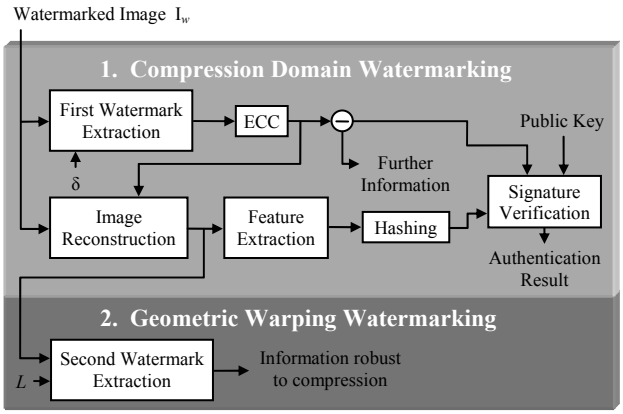

Figure 13. Watermark extraction and verification

Further, as we will show in the next subsection, this kind of error correction coding can also be used for an image adaptive embedding extension with two different quantization step sizes.

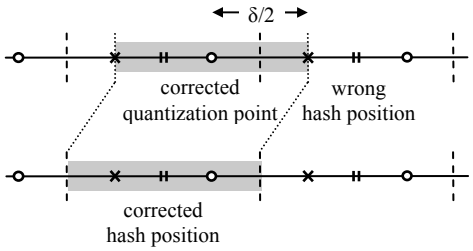

Figure 14. Hash interval reconstruction using ECC

3.4 Image Adaptive Perceptual Modeling

In [13], a watermarking method was proposed that embeds information in the upper DWT-subband similar to our approach but not for authentication purpose. As opposed to our scheme, watermark embedding is done by adding information to the wavelet coefficients, instead of quantization. The authors presented a way to reduce the embedding induced visual distortions by applying a block-based texture classification. Wavelet blocks with strong texture are separated from blocks with weak texture by simply searching for blocks with larger coefficients. In this way, information bits can be embedded with different strength due to the fact that the human visual system (HVS) is less sensitive to changes in regions with edges or transitions.

To adapt this texture masking approach to our authentication scheme, feature extraction as well as watermark embedding has to be modified as follows.

3.4.1 Block organization

After the image has been DWT-transformed, each pixel block in the spatial domain corresponds to several blocks in the DWT domain. For example, if we use $Z = 4$ for the decomposition, one coefficient in the LL^4-subband spatially occupies 16 x 16 pixel.

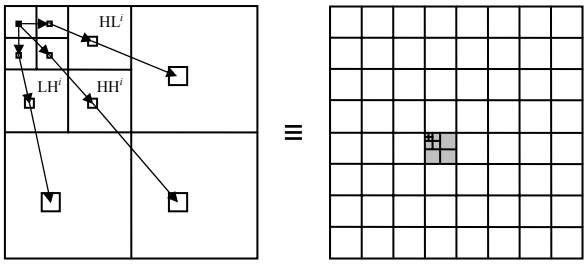

Figure 15. Wavelet block tree organization ($Z = 3$)

3.4.2 Texture classification and pre-distortion

Except for the LL^4-subband, wavelet coefficients have large amplitude where the image has transitions and strong texture. This means blocks composing of coefficients with large amplitude in the corresponding subbands LH^i, HL^i, and HH^i are better suited for embedding than blocks with small coefficients. To separate strong blocks from weak blocks from several tests on natural images we found out that the following approach is suited best:

1. Look for coefficients composing the same block with absolute values larger than a given threshold T.
   - $T_1 = 9$ for the coefficients of LH^4, HL^4
   - $T_2 = 18$ for the coefficients of HH^4
2. Use a *Closing*-Operation for all three resulting 32x32 binary masks to eliminate small gaps
3. If at least two of three threshold decisions at the same spatial position are positive, the corresponding block is strong
4. Use an *Erosion*-Operation for the final bit mask and a pre-distortion if the absolute coefficient values are close to the threshold to lower recognition errors during verification.

3.4.3 Adaptive watermark embedding

The texture block classification yields a LL^4-subband-sized mask which can be used during the signature embedding process. For example, in strong textured blocks bits can be embedded with larger step size δ_1. In other blocks δ_2 is used, where $\delta_1 > \delta_2$.

Figure 16. Weak textured region a), strong textured region b)

As can be seen in Figure 17 b), the visual embedding induced distortions are lower in homogenous areas using this new content adaptive approach. We tested the occurrence of recognition errors in the bit mask due to image distortions in the spatial domain. For

example, Gaussian lowpass filtering, manipulations of contrast or brightness and even strong JPEG compression yield acceptable error rates, lower than 0.6 percent.

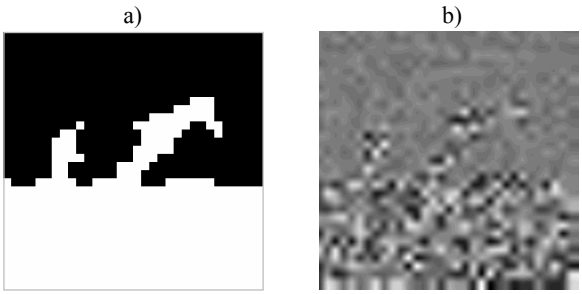

Figure 17. Binary LL^4-mask a), difference of adaptively watermarked image to original image b)

3.4.4 Security aspects of the perceptual adaptation

The DWT-coefficients in our implementation range from -2048 to 2048. We recommend the use of $\delta_1 = 3 \cdot \delta_2$ not larger than 40 for perceptually acceptable image quality using natural images.

Since from every DWT-subband after the quantization process a cryptographic hash value is calculated, it can be recognized if only one single coefficient has left its δ-sized quantization interval due to admissible or malicious modifications. An attacker has to consider this while searching for two images or fabricating two images that have the same features.

3.5 Watermark Removal

As in Figure 11, a signature bit is embedded in the lower or the upper half of the hash interval. Since the distribution of the coefficients of a 2d-DWT-transformed image in each hash interval can be approximated by a uniform distribution, this position is not optimal. To reduce this noise, which is higher than simple quantization noise, the verification algorithm could move the quantized coefficients back to the centre of the hash intervals after the signature bits are extracted.

A common JPEG2000 decoder does not need to extract the embedded watermark information to visualize the compressed image. But, if our technique of watermark removal is applied, the embedding induced distortions can be lowered to approximately 90 percent at the receiver site. It is obvious that after applying this kind of image reconstruction the correct extraction of the firstly embedded geometric watermark information can be gained.

4. EXPERIMENTAL RESULTS

In this section, we provide some results. For the sake of visibility, in our figures, we only show the curves for the well-known test images "Clown" and "Goldhill". Further, we tested our algorithms with similar results for a large set of test images from the uncompressed colour image database UCID [15].

To implement our JPEG2000-based authentication watermarking algorithm, we chose the well-known "Kakadu" reference software [14]. This implementation enabled us, to also consider the entropy coding stage with bit truncation EBCOT. In addition to the demonstrated curves this implementation was ported to a full Camera-Pocket PC application and web-based verification.

In Figure 18, the rate-PSNR curves of the watermarked 512 x 512 pixel image "Clown" are shown with and without the previously applied geometric warping watermarking using $L = 300$. It can be seen that the geometric warping has strong effect on the PSNR value of the host image. For example, if only the geometric warping takes place and no further information is embedded the difference between the host image and the watermarked one is approximately 37.72 dB.

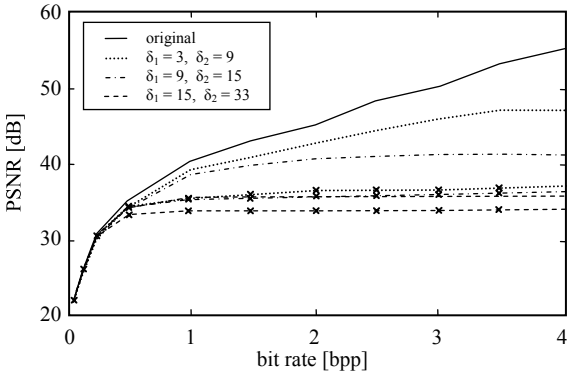

Figure 18. Rate-PSNR curves of watermarked image "Clown" with and without previously applied geometric warping. The geometrically warped curves are marked with ✖'s.

In Figure 19, we demonstrate the robustness of the authentication process against allowed JPEG compression, whereas in one case error correction is used at the verification site and in the second case it is not used. For the latter, of course, less information bits have to be embedded yielding slightly lower visual distortions. For detailed considerations on the efficiency of error correction coding for watermark embedding, we refer to our work in [9]. Here, in the case of not using ECC, we filled the signature with random bits to be able to compare both methods. What can be seen clearly is that ECC makes the authentication work more constant and reliable at the same amount of embedding induced distortions. Small disturbances in the spatial domain, such as noise or compression, have less effect on the verification.

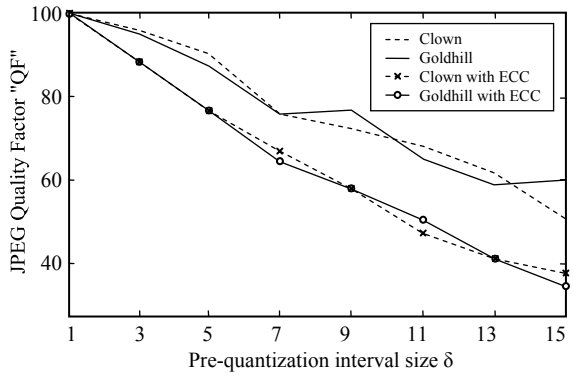

Figure 19. Robustness against JPEG re-compression with and without error correction coding (ECC)

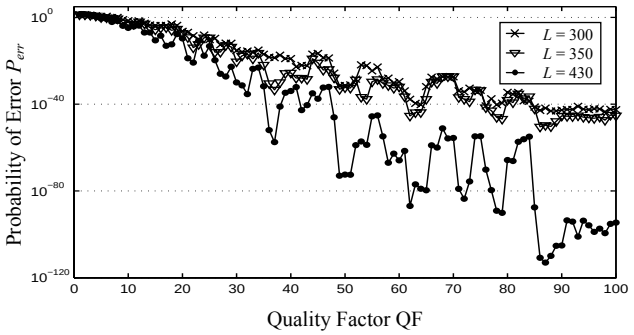

Figure 20. Robustness of the geometrically embedded bits to lossy JPEG transcoding after the authentication information embedding process ($\delta_1 = 21$, $\delta_2 = 7$, Bit rate = 1 bpp)

5. CONCLUSION

In this paper, we presented a very efficient JPEG2000-based image authentication watermarking scheme, which is robust to JPEG as well as JPEG2000 re-compression and other allowed signal processing operations. Our new method supports lots of popular features of the JPEG2000 compression framework such as quality and resolution scalability, lossless image rotation and flipping. The scheme is secure in contrast to most of the authentication schemes proposed so far in the wavelet domain. All coefficients of the wavelet decomposition are quantized and hashed using secure cryptographic hash functions. Image adaptive perceptual modeling is applied to lower the embedding induced visual distortions. We showed that error correction coding yields impressive robustness improvements of the embedded image content dependent signature without raising a security gap. Further, we introduced a new extended version of the scalar quantization in contrast to the one commonly used in JPEG2000, which lowers the overall visual distortions during the embedding process. Prior to the authentication watermark embedding another watermarking process is proposed to be applied. This second approach hides information highly robust to lossy image compression by geometrically warping image objects in an imperceptible way. Hence, as we demonstrated, the subsequent authentication embedding process in the compression domain has no effect on the prior hidden watermark for property rights protection purpose.

6. REFERENCES

[1] Cox, J., Miller, M. The First 50 Years of Electronic Watermarking. *EURASIP Journal of Applied Signal Processing, 2*, Feb. 2002, 126-132.

[2] Podilchuk, C. I., and Zeng, W. Image Adaptive Watermarking Using Visual Models. *IEEE Journal of Selected Areas in Communication, 16*, May. 1998, 525-539.

[3] Sharkas, M., ElShafie, D., and Hamdy, N. A Dual Digital-Image Watermarking Technique. In *Proc. of 3rd World Enformatika Conference*, April 2005, 136-139.

[3] Zhao, Y., Campisi, P., and Kundur, D. Dual Domain Watermarking for Authentication and Compression of Cultural Heritage Images. In *IEEE Transactions on Image Processing, 13*, Feb. 2004, 430-448.

[4] Lie, W.-N., Hsu, T.-L., Lin, G.-S., Ho, W.-J. Fragile Watermarking for JPEG-2000 Images. In *Proc. of 16th Conference on Computer Vision, Graphics and Image Processing*, Aug. 2003, 823-826.

[5] Pröfrock, D., Schlauweg, M., and Müller, E. Video Watermarking by Using Geometric Warping without Visible Artifacts. In *Proc. of 8th Workshop on Information Hiding*, July 2006, 99-104.

[6] Ekici, Ö., Sankur, B., Coşkum B., Nazi U., and Akcay, M. Comparative evaluation of semifragile watermarking algorithms. *Journal of Electronic Imaging, 13*, Jan. 2004, 209-216.

[7] Zhu, B. B., Swanson, M. D., and Tewfik, A. H. When seeing isn't believing. *IEEE Signal Processing Magazine, 21*, 2004, 40-49.

[8] Rey, C. and Dugelay, J.-L. A Survey of Watermarking Algorithms for Image Authentication. *EURASIP Journal of Applied Signal Processing, 6*, March 2002, 613-621.

[9] Schlauweg, M., Pröfrock, D., Palfner, T., and Müller, E. Quantization-based semi-fragile public-key watermarking for secure image authentication. In *Proc. of SPIE, 5915*, July 2005, 41-51.

[10] Lin, C. Y. and Chang, S.-F. Semi-fragile Watermarking for Authenticating JPEG Visual Content. In *Proc. of SPIE, 3971*, Jan. 2000, 140-151.

[11] Meerwald, P. Quantization Watermarking in the JPEG2000 Coding Pipeline. In *Proc. of Int. Conference on Communication and Multimedia Security*, May. 2001, 69-79.

[12] Schlauweg, M., Palfner, T., Pröfrock, D., and Müller, E. The Achilles' Heel of JPEG-based Image Authentication. In *Proc. of IASTED Int. Conference on Communication, Network and Information Security, 499*, Nov. 2005, 1-6.

[13] Huang, D., Liu, J., Huang, J., and Liu, H. A DWT-based Image Watermarking Algorithm. In *Proc. of IEEE Int. Conference on Multimedia and Expo*, Aug. 2001, 313-316.

[14] Taubman, D. S. and Marcellin, M. W. JPEG2000: Image Compression Fundamentals, Standards and Practice, Kluver Academic Publishers, 2002.

[15] Uncompressed Colour Image Dataset [Online] - Available: http://vision.doc.ntu.ac.uk