

Improved Geometric Warping-Based Watermarking

Dima Pröfrock, Mathias Schlawweg, Erika Müller

*Institute of Communication Engineering, Faculty of Computer Science and Electrical Engineering, University of Rostock,
Richard-Wagner-Str. 31, 18119 Rostock, Germany
{dima.proefrock, mathias.schlawweg, erika.mueller}@uni-rostock.de*

Abstract

In this paper, we propose a blind geometric warping-based watermarking for images and videos. We put emphasis on high robustness and security as well as decreased complexity. Our previous works have shown that the geometric structure of images and videos is a suitable embedding domain for watermark information. To describe the geometric structure, detection or segmentation methods are used, which can result in additional security holes, in more required computing effort, in loss of robustness and in loss of watermark blindness. In this work, we propose a watermarking approach that doesn't use detection and segmentation processes. Our watermark approach is based on the result of a filtering that is used to describe the geometric structure. Additionally, an efficient realisation of the filter is developed and a scheme of watermark embedding is proposed. The watermark bits are spreaded over the whole frame and coded in the spatial positions of edges and corners. We show that the resulting watermark can be embedded without visible quality degradations. Beside of this, it achieves high robustness to strong lossy compression and other distortions at a high watermark capacity. For example, a H.264/AVC compression that degrades the video quality down to PSNR of 20.6 dB induces a watermark Bit Error Rate of 0.0013 at a watermark capacity of 20 bits per frame.

1. Introduction

Digital watermarking offers contributions in the fields of protection of the authenticity of data and the copyrights of authors. It describes techniques to embed additional information, the watermark, into digital data [1]. The desired watermark properties strongly depend on the specific application. One property is the robustness describing the possibility to extract the watermark after permitted or malicious modification (attacks) of

the digital data. An overview of different attacks, such as cropping, rotating, scaling, compression or noise, and their classifications can be found in [2]. Robustness to many attacks can be important. However, mostly these watermarks are not robust to strong lossy compression or contain only a low amount of information (watermark capacity). High robustness to strong lossy compression and a suitable capacity can be achieved using geometric warping-based watermarking approaches [3], [4]. The watermark is embedded by changing the geometric structure of images or videos. Because compression algorithms try to maintain the geometric structure, these watermarks can be very robust.

Using the geometric structure as embedding domain, issue a challenge to the watermarking procedure. The watermark information is coded into the spatial position of edges or corners. Usually, edges and corners have to be detected for embedding the watermark. In blind watermarking approaches, these positions have to be reconstructed for watermark extraction. Therefore, (content dependent) features of images or videos are used to select watermark embedding positions. Maes et al. [4] use salient points, Pröfrock et al. use edge strength to select blocks [3] or to segment images [6]. If the image content is changed (e.g. by compression) these selection processes can be corrupted. There are methods to prevent failures by creating a gap in the feature distribution [6] or using error correction codes [9], [10]. However, these steps induces additional quality degradations or reduce the watermark capacity and robustness, respectively. Furthermore, an attacker can use the knowledge about the used image features to de-synchronize the watermark. Hence, the usage of content dependent selection of embedding positions or content dependent segmentation processes results in decreased watermark efficiency (robustness, capacity, quality, computational complexity) and in additional security holes.

In this paper, we propose a geometric warping-based watermarking approach that embeds the watermark into the image content without the necessity of selection of content dependent embedding positions or segments. The watermark is embedded in the geometric structure with the common advantage of high robustness to lossy compression. The basis of our approach is a filter that can be implemented with low computational complexity. The results of the filter process can be interpreted as geometric structure of an image and can be used as embedding domain. For watermark embedding, we present an efficient algorithm with low computational complexity to change the embedding domain.

This paper is organized as follows. In section 2 the fundamentals of our approach are presented. Afterwards we propose an efficient realisation of our filter that is used to describe the geometric structure. In section 4 our embedding and extracting theory, which bases on the filter results, is introduced. Additionally, we propose a scheme to compute the warping field that is required to embed the watermark by geometric warping. Finally, our results are presented and discussed.

2. Fundamentals

In [3] we explain and show that the geometric structure is a suitable embedding domain for watermark information. The watermark is robust to strong lossy compression and can be embedded without significant quality degradations.

The basis to describe the geometric structure is the block-based Normed Centre of Gravity (NCG) and the mapping of the NCG x,y -coordinates on a content adaptive quantization lattice [3]. The values L and s are the result of the NCG calculation and mapping process. L delivers information about the “amount” of geometric structure (e.g. edged strength) in the processed block. The value s is a reduced description of the geometric structure (e.g. edge positions).

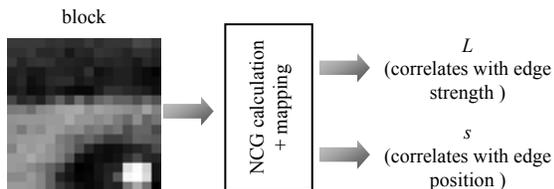


Figure 1. Using L and s to describe the geometric structure

As proposed in [6] the NCG can be used as a filter to compute for each pixel a value for L (matrix LFM –

Locator-Feature matrix) and for s (matrix CFM – *Carrier-Feature matrix*). The filter results describe the geometric structure of an image and are used for watermark embedding and extraction.

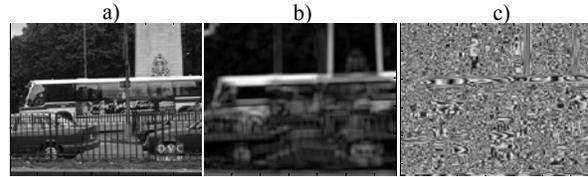


Figure 2. Original frame a) matrix LFM b) and matrix CFM c)

For practical applications, an efficient realisation of the filter is advantageous, which is proposed in the next section.

3. Efficient Filter Realisation

The simplest way to realise the filter process is to perform the NCG calculation for each pixel surrounding block (see Figure 3). More computing power than necessary is required using this way. Redundant steps in the filter process (e.g. averaging columns and rows of the blocks) are reasons for this.

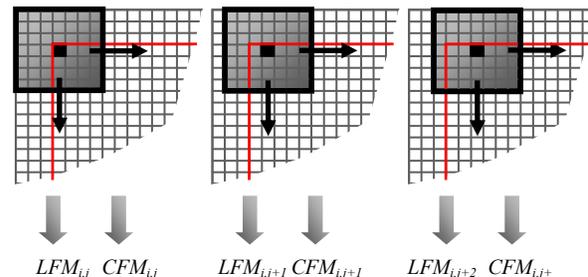


Figure 3. Simple NCG filter

To reduce the required computing power, we reduce the redundant steps as follows: The independent successive calculation of the NCG of the single blocks is split to dependent concurrent calculations of neighbouring blocks. The calculation bases on one vertical and one horizontal vector with length n , which are shifted over the image (instead one block with the size $n \times n$). On each position the mean values of the two vectors are computed and multiplied with the constant vectors $\bar{c}1$ and $\bar{c}2$, which have the length n .

$$c1_i = \cos\left(\frac{\pi}{n} \cdot (2 \cdot i + 1)\right) \quad (1)$$

$$c2_i = \sin\left(\frac{\pi}{n} \cdot (2 \cdot i + 1)\right) \quad (2)$$

The resulting vectors are collected by adding them to the temporary matrices $M1$, $M2$, $M3$ and $M4$ as shown exemplarily in Figure 4. $M1$ to $M4$ are

initialised with zero. The values of these matrices on position i,j are used to create the vectors \vec{v}_x and \vec{v}_y :

$$\vec{v}_x = \begin{pmatrix} M1_{i,j} \\ M2_{i,j} \end{pmatrix} \quad (3)$$

$$\vec{v}_y = \begin{pmatrix} M3_{i,j} \\ M4_{i,j} \end{pmatrix} \quad (4)$$

With these vectors, the values for L and s on position i,j can be computed using the known equations (see [3], equations (2) to (6)). Hence, we get the values $LFM_{i,j}$ and $CFM_{i,j}$ of the matrices LFM and CFM .

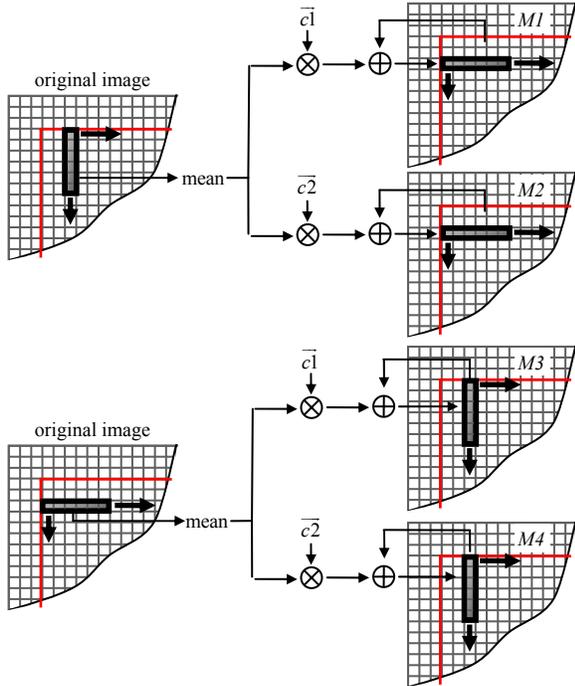


Figure 4. Advanced filter scheme with reduced redundant steps

As shown in Figure 5 the required computing power of the advanced filter process (based on a 3 GHz Intel E6850) is lower than the required computing power of the simple filter process. The proposed filter process can also be divided into several independent processes for a more efficient filtering on multi-core systems.

An implemented version of our advanced filter can be downloaded at [5].

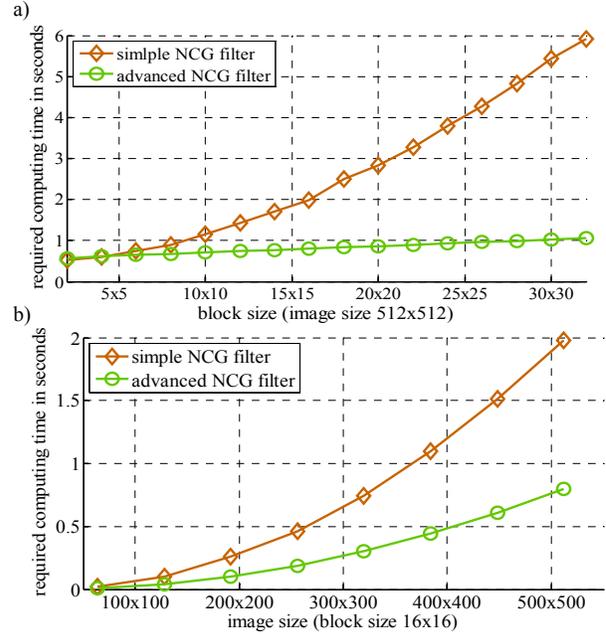


Figure 5. Required computing power for different filter realisations with different block sizes a) and different image sizes b)

4. Watermark Embedding and Extraction

Our watermarking embedding and extraction process is based on the matrices LFM and CFM of the filter process. CFM (correlation with edged positions) is used to carry the watermark information bits. LFM (correlation with edge strength) is used as indicator which elements of CFM are suitable and robust, respectively, to carry the watermark information. High values of LFM (strong edges) results in robust values of CFM (robust edge positions).

This section is divided into two sub-sections. In the first sub-section, the theory of embedding and extraction is explained. Afterwards we propose an efficient algorithm to compute the warping field that is required to change the geometric structure for embedding.

4.1. Theory – Embedding and Extraction

The watermark information is spreaded to the whole image. Therefore, $m \cdot n$ different positions of LFM and CFM are selected to embed n watermark bits. The selection process is content independent and can be realized with a known or ciphered (key-controlled) process. As result we get the position matrix POS containing the vectors $pos_{i,j}$, which describes a position in LFM and CFM , respectively (following

LFM/CFM) (equation (5)). The parameter m defines the number of elements of *CFM/LFM* that are used to carry one watermark bit. m is limited by the size of *LFM/CFM* and the number of n bits.

$$POS = (\overline{pos}_{i,j}) = \begin{bmatrix} 1,1 & \cdots & 1,m \\ \vdots & \ddots & \vdots \\ n,1 & \cdots & n,m \end{bmatrix} \quad (5)$$

The relationship between the $m \cdot n$ chosen elements and the number of elements in *LFM/CFM* is *rel*:

$$rel = \frac{m \cdot n}{\text{number of elements in } LFM/CFM} \quad (6)$$

Based on *LFM*, *CFM* and *POS* the vector \bar{s}^* with length n is computed:

$$s_i^* = \frac{\sum_{j=1}^m (LFM_{pos_{i,j}} \cdot CFM_{pos_{i,j}})}{\sum_{j=1}^m LFM_{pos_{i,j}}}, s_i^* \in \mathbb{R} : [0,1] \quad (7)$$

\bar{s}^* represents for each watermark bit a value s^* . To embed a bit, s^* is changed so that $s^* < 0.5$ (ideal 0) to embed a bit value '0' or $s^* > 0.5$ (ideal 1) to embed a bit value '1'. s^* is changed by altering the position of edges and corners using warping (see next subsection). To extract the watermark bits, \bar{s}^* is computed and the threshold 0.5 is used to decide which bit values are embedded. Therefore, the original image or video is not necessary.

The robustness of s^* depends on two factors. The first factor is the embedding efficiency e . It depends on the ideal value s_{ideal}^* and the actual value s_{actual}^* after the warping process:

$$e = 1 - |s_{ideal}^* - s_{actual}^*| \quad (8)$$

With an increasing embedding efficiency e also the distance of s_{actual}^* to the threshold 0.5 increases. That results in a more robust watermark bit. The parameter m is the second factor. With higher m more values of *LFM* and *CFM* are used to compute s^* . Hence, s^* is more robust against alterations of single elements of *LFM* and *CFM*. The embedding efficiency e and the parameter m depend on each other. A higher value of m results in a lower embedding efficiency e . Reason for this is the dependence between spatial nearby elements of *LFM* and *CFM*. With higher m the spatial distance between the elements of *LFM* and *CFM* at position *POS* decreases. Hence, it is more difficult to change them independent on each other.

4.2. Practice – Computing the Warping Field

Aim of the warping process is to change the elements of *LFM* and *CFM* at position *POS* to reduce the difference of the elements of \bar{s}^* to the watermark bit values. To prevent visible quality degradations the warping field has to be limited.

The warping field W of an image with r rows and c columns is defined as follows:

$$W = (\bar{w}_{i,j}) \text{ with } i \in \mathbb{N} : [1,r], j \in \mathbb{N} : [1,c] \quad (9)$$

The warping vector $\bar{w}_{i,j}$ defines the warping in x ($w_{i,j}^x$) and the warping in y ($w_{i,j}^y$) direction. To reduce the computational complexity for computing the warping field, we describe the warping field W with a small set of sampling points P :

$$P = (\bar{p}_{i,j}) \quad (10)$$

Investigations have shown that a distance (independent of the host image) of 16 pixels between the sampling points results in a good balance between computational complexity and embedding efficiency e . To compute W out of P bilinear interpolation is used.

The scheme to compute P is described in the following: A single element $\bar{p}_{i,j}$ of P is computed by using an iterative gradient based search algorithm. Therefore, the values of $\bar{p}_{i,j}$ are varied, the warping field W is computed, the image is warped and filtered and the new values of \bar{s}^* are computed. The values that results in the highest embedding efficiency e are chosen for $\bar{p}_{i,j}$. This process is repeated with less variations of $\bar{p}_{i,j}$ until no significant increase of e can be observed. The maximal length of $\bar{p}_{i,j}$ is limited to p_{max} to control the influence of warping to the image quality. Because bilinear interpolation is used to compute W out of P , the influence of each sampling point on the warping field is spatial limited. Hence, each fourth sampling point can be computed by the search algorithm at the same time. As a result, the computational complexity is significantly reduced. All sampling points are computed in four steps. In each step another quarter of the sampling points is computed. These steps are repeated until no significant increase of e can be observed. The scheme is exemplarily shown in Figure 6.

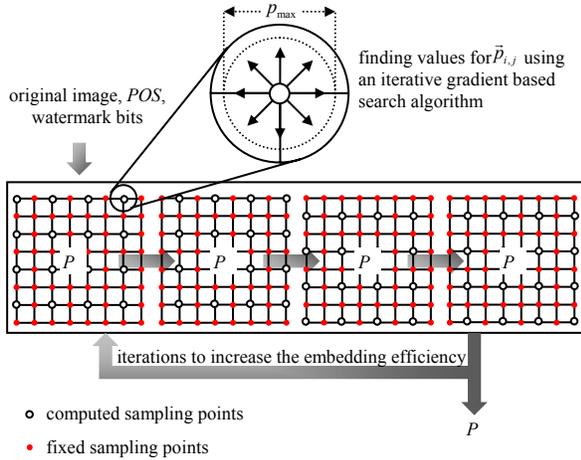


Figure 6. Scheme to compute P

Finally, the matrix P is used to compute the warping field W . An example is shown in Figure 7. For a better visualization P is gained by 15 and W is gained by 5.

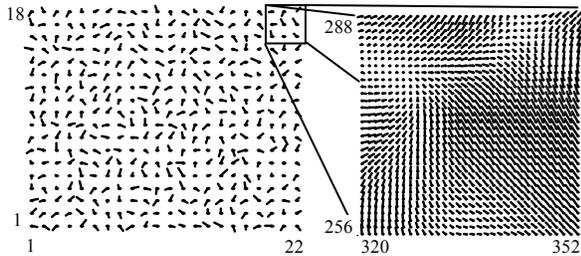


Figure 7. Sampling points P (left) and part of the resulting warping field W (right) of a 352x288 frame

Using the warping field W , an image or frame can be warped to embed the watermark bits. For example, see Figure 8. The maximal warping strength in this example is $p_{max} = 0.3$ pixel.

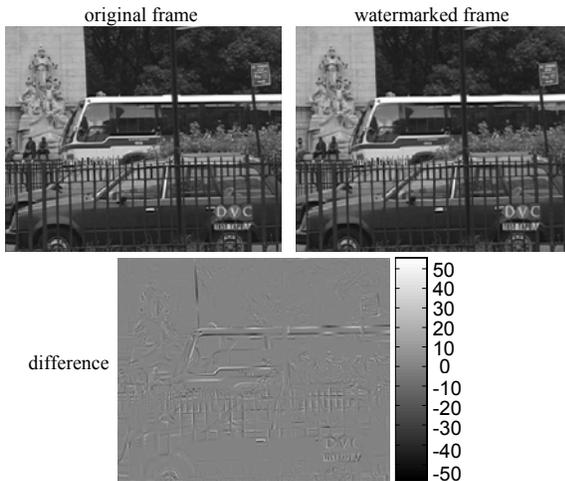


Figure 8. Example for embedding watermark bits by geometric warping

5. Results

The proposed watermark approach can be applied on images or frames of videos. Generally, strong lossy compression is more used in video processing instead in image processing. Because of this, the standard test videos “Bus”, “Horse”, “Horse2”, “Waterfall” and “Foreman” (gray scaled, resolution of 352x288 pixels, 930 frames in total) are used to analyse our approach. For compression the actual compression standard H.264/AVC and for the adaptive quantization lattice [3] $quant = 32$ is used.

5.1. Embedding Efficiency

The mean embedding efficiency e_{mean} is computed for different rel and different maximal warping strengths p_{max} . The results are shown in Figure 9. As expected, e_{mean} decreases with an increased rel (m , respectively).

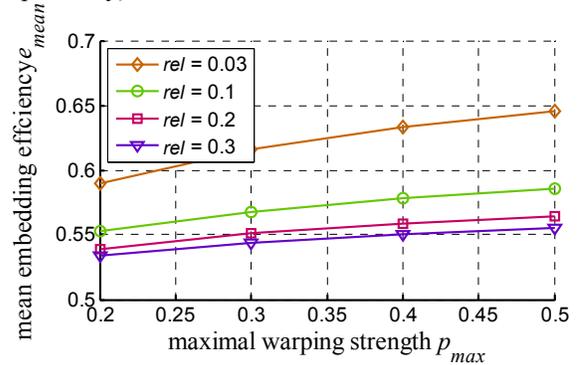


Figure 9. Mean embedding efficiency e_{mean}

5.2. Quality

The influence of the embedding and warping process, respectively, on the video quality can not be estimated by using common statistics such as Peak Signal to Noise Ratio ($PSNR$) or Structural Similarity Index ($SSIM$). In [7] we propose quality relevant warping parameters and evaluate them with a study. As parameters the mean spatial change of warping w_{smean} and the mean temporal change of warping w_{tmean} are proposed. Based on these parameters we can estimate the influence of the warping process of this work on the video quality. Out of the maximal warping strength p_{max} and the distance of 16 pixels between sampling points P of W , the mean spatial change of warping can be computed as follows:

$$w_{smean} = \frac{2 \cdot p_{max}}{16} \quad (11)$$

w_{mean} doesn't matter if $w_{smean} \leq 0.0375$ as can be seen in Figure 12 of [7]. Furthermore, the warping doesn't result in visible quality degradation at $w_{smean} \leq 0.0375$. For this work we can conclude:

1. The warping (watermark embedding) doesn't result in visible quality degradation for $p_{max} \leq 0.3$.
2. We can embed the watermark bits in each video frame (w_{mean} doesn't matter) without visible quality degradations for $p_{max} \leq 0.3$.

5.3. Watermark Robustness and Capacity

In this sub-section, the robustness of the embedded watermark bits to lossy compression is analysed. For compression the actual most efficient compression standard H.264/AVC [8] is used. The figures in this sub-section present the watermark Bit Error Rate (BER) of all videos in relationship to the compression strength. Because parameters of compression and resulting video data rates can not be interpreted without additional information we use the $PSNR$ to describe the compression strength.

As already stated, the watermark robustness depends on the embedding efficiency e and the amount of embedding positions per bit m and rel , respectively. In Figure 10 the Bit Error Rate (BER) of the embedded bits in relationship to the compression strength is plotted for different rel . Despite a decreased embedding efficiency e (see Figure 9) an increased rel results in a decreased Bit Error Rate. Hence, for further analyses $rel = 0.3$ is used.

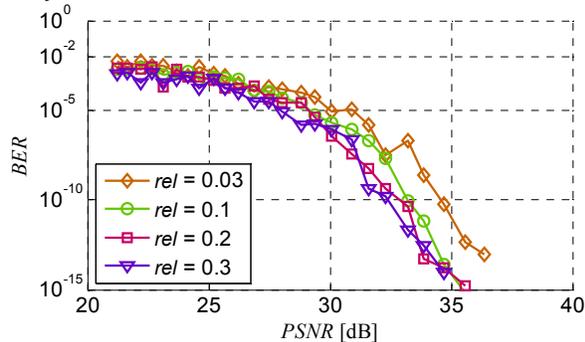


Figure 10. Watermark robustness for different rel with $p_{max} = 0.3$ and $n = 20$ embedded bits

A maximal warping strength $p_{max} \leq 0.3$ doesn't result in visible quality degradation (see last sub-section). To analyse the influence of the chosen warping strength p_{max} on the watermark robustness, also higher values are used. The results are shown in Figure 11. A higher warping strength results in a higher embedding efficiency (Figure 9) and in a higher watermark robustness.

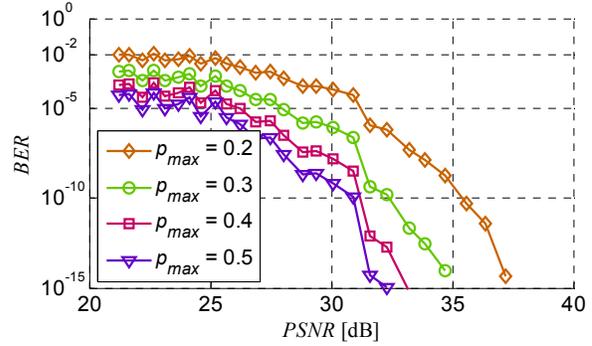


Figure 11. Watermark robustness for different p_{max} with $rel = 0.3$ and $n = 20$ embedded bits

Finally, it can be concluded that for maximal robustness the parameter rel and p_{max} has to be as high as possible. To prevent visible quality degradations p_{max} is limited to $p_{max} \leq 0.3$. Hence, for following analyses of the watermark capacity in relationship to the robustness we use $rel = 0.3$ and $p_{max} = 0.3$. Figure 12 shows the results. As expected, the watermark robustness decreases with an increasing watermark capacity (at the same quality). The results show that the robustness of the watermark to strong lossy compression is very high even at a relative high watermark capacity. In Figure 13, the influence of compression is illustrated to show the relationship between watermark robustness and degradation of video quality.

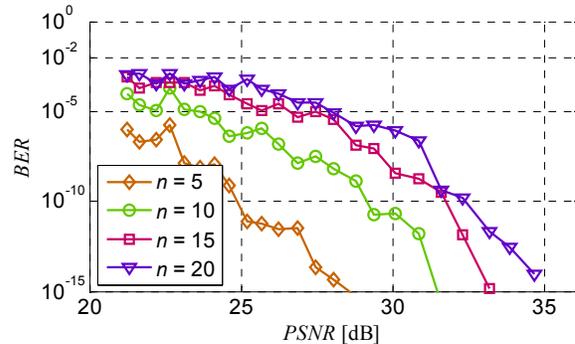


Figure 12. Watermark robustness to compression (H.264/AVC) for different embedded number of bits n with $rel = 0.3$ and $p_{max} = 0.3$

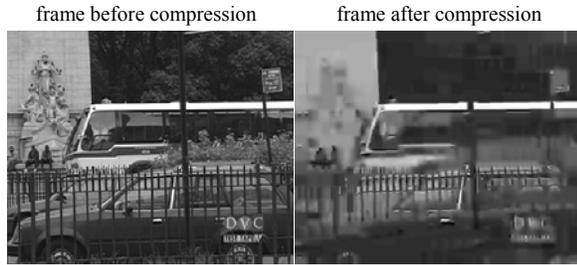


Figure 13. Influence of compression on the video quality ($PSNR = 20.6$ dB), the 20 embedded watermark bits can be extracted with a Bit Error Rate of $BER = 0.0013$

5.4. Further Analyses

Aim of the proposed watermarking approach is to achieve robustness to strong lossy compression. In the above sub-section we analyse this robustness. In this sub-section we analyse the robustness of the watermark bits to other kinds of typical distortions such as noise, scaling, cropping and geometric warping.

Noise: Noise is a distortion, which can be the result of converting videos from digital to analogue to digital. For our analyses we use Gaussian noise with a mean of zero. The strength of the noise is given by the standard deviation σ . Figure 14 shows the robustness of the watermark bits to noise. In Figure 15, the distortion of noise is exemplarily shown.

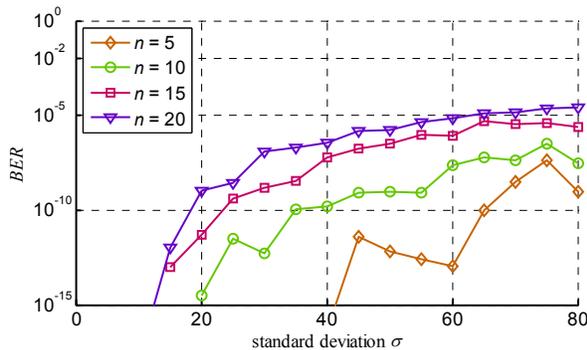


Figure 14. Watermark robustness to noise for different embedded number of bits n with $rel = 0.3$ and $p_{max} = 0.3$

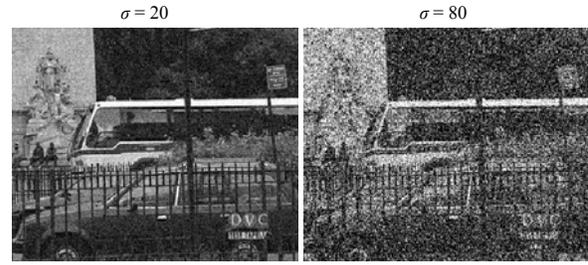


Figure 15. Influence of noise on the video quality, the 20 embedded watermark bits can be extracted with a Bit Error Rate of $BER = 0.00003$ at $\sigma = 80$

Scaling: Scaling is a typical operation in the field of image and video processing to adapt the resolution. For our analyses we use scaling where the scaling factor of the frames is the same for the height and for the width. We assume that the scaling factor is known during the watermark extraction. Figure 16 shows the robustness of the watermark bits to scaling. The strength of scaling is given in percent. For example, scaling of 10 % means that the frame size is reduced to 10 %. In Figure 17, some examples for scaling are shown.

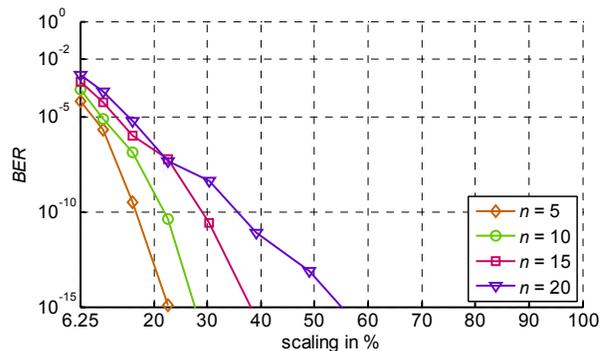


Figure 16. Watermark robustness to (known) scaling for different embedded number of bits n with $rel = 0.3$ and $p_{max} = 0.3$

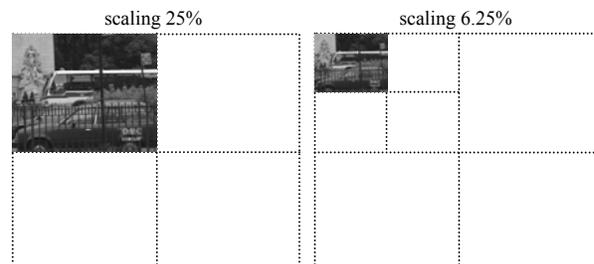


Figure 17. Scaling of frames, the 20 embedded watermark bits can be extracted with a Bit Error Rate of $BER = 0.0016$ after reducing the amount of pixels to 6.25 %

Cropping: An additional operation in the field of image and video processing is cropping. For our analyses we assume that the cropping parameters (but not more) are known. Figure 18 shows the robustness of the watermark bits to cropping. The cropping strength is given in percent. For example, cropping of 10 % means that 10 % of the frame is lost. In Figure 19, some examples for cropping are shown.

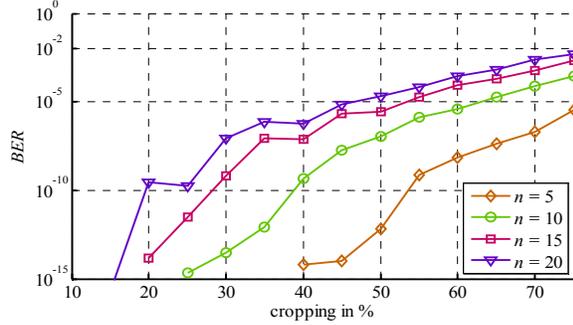


Figure 18. Watermark robustness to (known) cropping for different embedded number of bits n with $rel = 0.3$ and $p_{max} = 0.3$

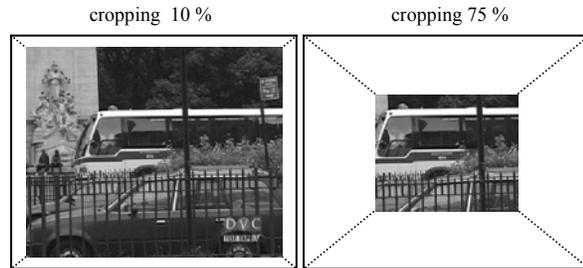


Figure 19. Cropping of video frames, the 20 embedded watermark bits can be extracted with a Bit Error Rate of $BER = 0.005$ after cropping of 75 %

Geometric warping: Geometric warping doesn't belong to the class of typical video processing operations. However, the proposed watermarking approach uses geometric warping for watermark embedding. An attacker could also use geometric warping to destroy the watermark. In the following we analyse the robustness of the watermark to geometric warping attacks. The used attack warping fields are constructed similar to the embedding warping fields. Because the attacker doesn't know the embedding positions POS , he can't attack the watermark bits directly. Hence, the attack warping fields are generated with a random set of parameters with a maximal warping strength p_{max} . The results are shown in Figure 20. The watermark bits are robust also if the warping strength of the attack is increased by factor 3 in comparison to the warping strength of the embedding ($p_{max} = 0.3$). Because geometric warping

with $p_{max} > 0.3$ results in visible quality degradations we can say that the watermark is robust to invisible geometric warping attacks. In Figure 21, some examples for warping attacks are shown.

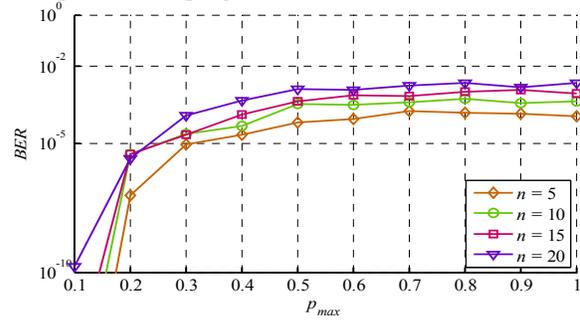


Figure 20. Watermark robustness to warping for different embedded number of bits n with $rel = 0.3$ and $p_{max} = 0.3$



Figure 21. Geometric warping attack of video frames, the 20 embedded watermark bits can be extracted with a Bit Error Rate of $BER = 0.0023$ after warping attacks with $p_{max} = 1$

5.5. Discussion

The embedded watermark bits achieve a high robustness to strong lossy compression, noise, (known) scaling, (known) cropping and geometric warping attacks. To get the parameter of scaling, cropping or other de-synchronizing distortions (rotation, skewing and so on), our watermark approach can be combined with re-synchronization templates [11]. These templates could be pseudo random noise, which is added on the images or frames. As shown in Figure 14 the watermark bits are very robust to noise. Hence, adding of invisible pseudo random noise-based templates after watermarking the images or frames doesn't affect the watermark bits significantly.

6. Conclusion

In this paper, we presented a blind uncompressed domain geometric warping-based watermarking approach for images and videos. The advantage of our

approach is the embedding of watermarks into the content of data without the necessity of using content dependent embedding positions. On this way, the watermark efficiency and security have been increased and the computational complexity has been decreased. For the watermark approach we developed an efficient filter algorithm to describe the geometric structure and we proposed the watermark embedding scheme. We show that the resulting watermark can be embedded without visible quality degradations and with high robustness to strong lossy compression, noise, (known) scaling, (known) cropping and geometric warping at a high watermark capacity.

This work is an important improvement of previous works and can be used as basis for further watermarking approaches that use the advantageous geometric structure as a new type of embedding domain.

7. References

- [1] F. Perez-Gonzales and J. R. Hernandez, *A tutorial on digital watermarking*, Proc. of International Carnahan Conference on Security Technology, pp. 286-292, Madrid Spain, 1999.
- [2] S. Voloshynovskii, S. Pereira, T. Pun, J. J. Eggers and, J. K. Su, *Attacks on Digital Watermarks: Classification, Estimation-based Attacks and Benchmarks*, In IEEE Communications Magazine, vol. 39, issue 8, pp. 118-126, 2001.
- [3] D. Pröfrock, M. Schlauweg, and E. Müller, *Video Watermarking by Using Geometric Warping Without Visible Artifacts*, Proc. of Information Hiding (8th IH 2006), Alexandria, USA, 2006.
- [4] M. J. J. B. Maes and C. W. A. M. van Overveld, *Digital watermarking by geometric warping*, Proc. of International Conference on Image Processing (ICIP), vol. 2, pp. 424-426, Chicago, IL, USA, 1989.
- [5] <http://www.mathworks.com/matlabcentral/fileexchange/1oadFile.do?objectId=18622>
- [6] D. Pröfrock, M. Schlauweg, and E. Müller, *Content-Based Watermarking by Geometric Warping and Feature-Based Image Segmentation*, In Signal Processing for Image Enhancement and Multimedia Processing, Vol 37, ISBN: 978-0-387-72499-7, 2007.
- [7] D. Pröfrock, M. Schlauweg, and E. Müller, *A Study of Video-Quality Relevant Warping Parameters*, Proc. of International Workshop on Multimedia Signal Processing (MMSP), Cairns, Australia, 2008.
- [8] Draft ITU-T recommendation and final draft international standard of joint video specification (ITU-T Rec. H.264/ISO/IEC 14486-10 AVC), in Joint Video Team (JVT) of ISO/IEC MPEG and ITU-T VCEG, JVT-G050, (2003).
- [9] M. Schlauweg, D. Pröfrock, and E. Müller, *Soft Feature-Based Watermark Decoding with Insertion/Deletion Correction*, In Proceedings of 9th Information Hiding Workshop (IH 2007). Saint Malo, France, 11 – 14, June 2007.
- [10] K. Solanki, N. Jacobsen, U. Madhow, B. S. Manjunath, and S. Chandrasekaran, *Robust Image-Adaptive Data Hiding Using Erasure and Error Correction*, IEEE Transactions on Image Processing, Vol. 13 (12), 1627-1639, 2004.
- [11] M. Barni, *Shedding light on some possible remedies against watermark desynchronization: a case study*. Proc. of SPIE, Security, Steganography, and Watermarking of Multimedia Contents 2005, vol. 5681, pp. 106-113, 200