Parameterized Biorthogonal Wavelet Lifting for Lightweight JPEG 2000 Transparent Encryption*

Dominik Engel and Andreas Uhl
Department of Scientific Computing
Salzburg University, Austria
{dengel,uhl}@cosy.sbg.ac.at

ABSTRACT

Lightweight encryption offers a cogent alternative to full encryption of visual content in application settings with clients of low processing power, e.g. mobile applications, as it counterbalances security demands and computational demands. We present a lightweight transparent encryption scheme for JPEG 2000 that is based on and integrated into the wavelet lifting scheme. Keys are constructed from parameterized biorthogonal filters. The proposed method comes at extremely low computational cost and provides natural support for transparent encryption. We discuss the advantages and disadvantages of this encryption scheme with respect to keyspace, computational demands, compression performance, and security.

Categories and Subject Descriptors

I.4.2 [**Image Processing and Computer Vision**]: Compression (Coding); E.3 [**Data**]: Data Encryption

General Terms

Security, Performance

Keywords

JPEG 2000, lightweight encryption, parameterized biorthogonal wavelet lifting, transparent encryption

1. INTRODUCTION

Against the background of the finalization of JPEG 2000 [23] and the rising usage of this standard in the digital community, it becomes crucial to address issues of security and protection of intellectual property in JPEG 2000. In this respect, the diverse security needs of different applications are addressed in the framework of JPEG 2000 part 8 (JPSEC).

*Funding by the Austrian Science Fund (FWF), project number P15170, is gratefully acknowledged.

MM-SEC'05, August 1–2, 2005, New York, New York, USA

Full encryption of a JPEG 2000 bitstream (e.g. using AES) may be feasible for some settings, where there is sufficient computing power available on both, the encoder and the decoder side, and where an application demands security in the sense of complete protection of the visual content. There are other settings, however, in which other requirements are more important than those provided by complete encryption with a traditional cipher. JPEG 2000 performs exceptionally well at low bitrates and is thus well suited for mobile applications. In a mobile environment typically at least on one side there is low computing power. If visual content is to be transferred securely from one mobile device (like a mobile phone or a PDA) to another such device, computing power is restricted on the encoding and the decoding side, which could rule out full encryption as a feasible option for providing confidentiality. Furthermore, in such settings, there is often no need for complete protection of the visual content (cf. the notion of "hard" vs. "soft" encryption in [26]). In some application scenarios a degradation of quality (in terms of resolution or quality) for wrong keys is sufficient, as long as the full quality visual data can only be accessed with the unique correct key. In commercial scenarios access to a degraded version of the visual content often is a desired effect as an incentive for buying the full quality version ("transparent encryption"). Another consideration is that with full bitstream encryption, standard bitstream compliance is lost. A method for lightweight encryption that produces standard compliant bitstreams is preferable. We can phrase requirements for lightweight encryption in the presented setting:

- low demands on computational power
- retain compression performance comparable to the standard CDF 9/7 biorthogonal wavelet filter in JPEG 2000
- provide sufficient security with respect to target application
- support transparent encryption
- retain standard JPEG 2000 bitstream compliance

In this paper we present a method that involves practically no additional computational costs and fulfills the above requirements, especially the support for transparent encryption. To achieve this, we propose to use a wavelet parameterization based on the lifting scheme [22, 2] to produce a family of biorthogonal wavelet filters and construct a key from the parameters. The employed filters significantly improve the compression performance as compared to previously suggested parameterization types. Additionally, we increase the

size of the available keyspace by using secret non-stationary and inhomogeneous wavelet decompositions. This method, which produces a bitstream compliant to JPEG 2000 part 2, can be regarded as a special kind of header encryption since only the definitions of the filters used during wavelet decomposition need to be encrypted, the data itself (i.e. packet bodies, packet headers) remain in plaintext. As a consequence, only minimal computational encryption effort is required. In terms of realizing transparent encryption, the proposed approach produces bitstreams from which images of degraded visual quality can be decoded with any JPEG 2000 part 1 compliant codec. In order to get the full quality version, the correct key has to be obtained and a JPEG 2000 part 2 compliant codec has to be used for decoding.

2. PREVIOUS WORK

Macq and Quisquater [13, 14] introduce the term "transparent encryption" mainly in the context of digital TV broadcasting: they propose to use line permutations in the transform domain of a lossless multiresolution transform. The permutations are only applied in the region of the transform domain corresponding to fine grained details of the data. Droogenbroeck and Benedett [6] propose to encrypt the LSB bitplanes of the binary representation of raw image data. With respect to JPEG encoded images, the authors suggest to encrypt sign and magnitude bits of medium and high frequency DCT coefficients. Droogenbroeck [5] extends the latter idea to "multiple encryption", where different sets of DCT coefficients are encrypted by different content owners, and "over encryption", where these sets do not have an empty intersection (i.e. coefficients are encrypted twice or even more often). In the context of scalable or embedded bitstreams transparent encryption is achieved by simply encrypting the enhancement layer(s). This has been proposed by Kunkelmann and Horn using a scalable video codec based on a spatial resolution pyramid [11, 12] and by Dittmann and Steinmetz [4] using a SNR scalable MPEG-2 encoder/decoder. Yuan et al. [28] propose to use MPEG-4 FGS for transparent encryption in the same manner.

Recent work by Köckerbauer et al. [10] assesses the feasibility of using parameterized orthogonal filters (adapted from [20]) for lightweight encryption within JPEG 2000. The compression performance of the obtained orthogonal filters remains markedly below the established biorthogonal filters and varies considerably over the range of parameter values. To overcome the latter deficiency, a heuristic is proposed to avoid filters with low compression performance. Uhl and Pommer [25] use a parameterization of biorthogonal filters (as proposed by Hartenstein [8]) which yields some filters that can compete with the established filters. Still the parameterization is ill-suited for the aforementioned purpose as the variation of the obtained filters with regard to their compression performance is even worse than in the orthogonal case, with the worst filters going down below 5dB in a PSNR comparison. In all of the above approaches, the algorithm for parameterization of the wavelet filters introduces significant computational overhead and cannot be run jointly with JPEG 2000 compression in an integrated manner. Furthermore, with their focus on providing privacy and confidentiality rather than realizing transparent encryption they differ from the approach presented here.

Other approaches for lightweight encryption of JPEG 2000 include selective encryption of a certain amount of the packet data using a traditional cipher [7, 27, 16] or to permute the order of wavelet coefficients during compression [17]. All these approaches introduce significant computational overhead compared to the operation of unencrypted JPEG 2000, but stay below the computational demands of full AES encryption.

In the domain of watermarking, parameterized wavelet filters have also been proposed for increasing watermarking security [3, 9]. The lifting scheme has been used in constructing a watermarking scheme for JPEG 2000 [21].

3. PARAMETERIZED WAVELET LIFTING IN JPEG 2000

In our approach we use a lifting parameterization of the well-known CDF 9/7 wavelet filter that is presented by Zhong, Cheng, and Chen [29] and is based on work by Daubechies and Sweldens [2]. The authors use the construction theorem presented by Cohen, Daubechies, and Feauveau [1] to formulate conditions for the lowpass and highpass filter taps, h and g, respectively,

$$h_0 + 2\sum_{n=1}^{4} h_n = \sqrt{2},\ g_0 + 2\sum_{n=1}^{3} g_n = \sqrt{2} \tag{1}$$

$$h_0 + 2\sum_{n=1}^{4} (-1)^n h_n = 0 \tag{2}$$

$$g_0 + 2\sum_{n=1}^{3} (-1)^n g_n = 0 \tag{3}$$

$$2\sum_{n=1}^{3} n^2 (-1)^n g_n = 0. \tag{4}$$

A possible transformation of the CDF 9/7 wavelet into lifting steps is presented in [2].

$$s_n^{(0)} = x_{2n} \tag{5}$$

$$d_n^{(0)} = x_{2n+1} \tag{6}$$

$$d_n^{(1)} = d_n^{(0)} + \alpha(s_n^{(0)} + s_{n+1}^{(0)}) \tag{7}$$

$$s_n^{(1)} = s_n^{(0)} + \beta(d_n^{(1)} + d_{n-1}^{(1)}) \tag{8}$$

$$d_n^{(2)} = d_n^{(1)} + \gamma(s_n^{(1)} + s_{n+1}^{(1)}) \tag{9}$$

$$s_n^{(2)} = s_n^{(1)} + \delta(d_n^{(2)} + d_{n-1}^{(2)}) \tag{10}$$

$$s_n = \zeta s_n^{(2)} \tag{11}$$

$$d_n = d_n^{(2)}/\zeta \tag{12}$$

These lifting steps can be used to express the filter taps of h and g as functions of the four parameters $\alpha, \beta, \gamma, \delta$ and a scaling factor ζ. By combining these functions with conditions (1)-(4), [29] derive a parameterization that is only dependent on a single parameter α.

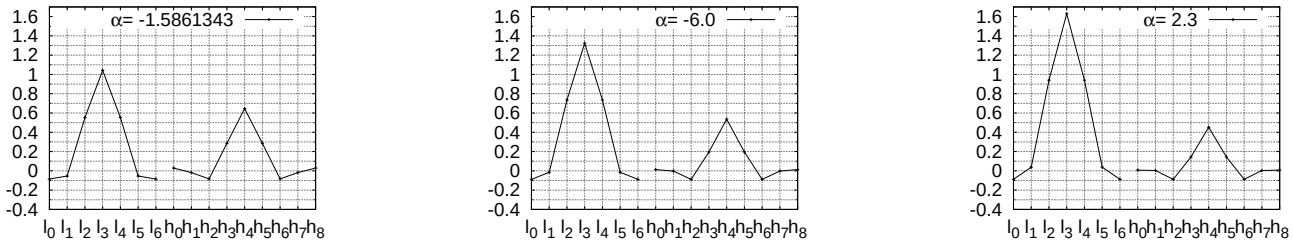
$$\beta = \frac{-1}{4(1+2\alpha)^2} \tag{13}$$

$$\gamma = \frac{-1-4\alpha-4\alpha^2}{1+4\alpha} \tag{14}$$

$$\delta = \frac{1}{16}\left(4 - \frac{2+4\alpha}{(1+2\alpha)^4} + \frac{1-8\alpha}{(1+2\alpha)^2}\right) \tag{15}$$

$$\zeta = \frac{2\sqrt{2}(1+2\alpha)}{1+4\alpha} \tag{16}$$

Figure 1 shows examples of parameterized biorthogonal filter taps. By setting α to the value originally proposed by [2], $-1.58613\ldots$, the original 9/7 wavelet is obtained.



(a) CDF 9/7 (b) α = -6.0 (c) α = 2.3

Figure 1: Examples of Parameterized Biorthogonal Wavelet Filter Taps

As the parameterization is based on the lifting scheme, it comes at virtually no computational cost. The only computations needed are the evaluations of the four functions for the scaling factor and the parameters other than α, and the calculation of the lowpass and highpass synthesis filter taps for normalization.

Since one of the stated requirements is the retention of compression performance that is comparable to the performance of the original 9/7 wavelet, we first assess the potential range that can be used for α. As illustrated by Figure 2, we found that with the exception of the open interval $]-1.4, 0.2[$ the filters produced by the 9/7 parameterization all achieve compression results that are competitive with the original CDF 9/7 wavelet. The filters within the interval $]-1.4, 0.2[$ are not stable and do not achieve highpass and lowpass separation. Therefore they are not suitable for compression, independent of the visual data to be transformed.

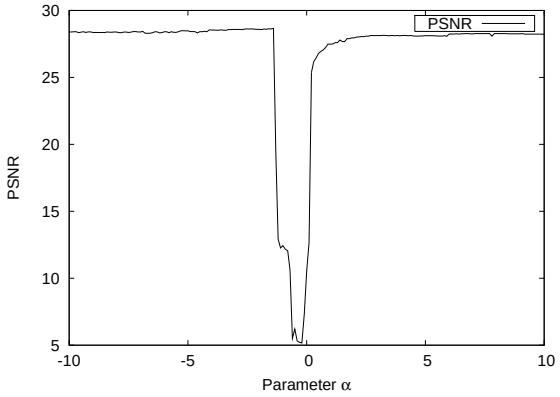


Figure 2: Compression performance (PSNR) of parameterized 9/7 wavelet filters for "Lena", rate 0.1 bpp

The peak-signal-to-noise-ratio (PSNR), as plotted in Figure 2, is by far no optimal choice to assess the quality of low quality images. Mao and Wu [15] propose an alternative measure that separates evaluation of luminance and edge information into a *luminance similarity score* (LSS) and an *edge similarity score* (ESS), reflecting properties of the human visual system. According to the authors, this measure is well suited for assessing distortion of low quality images, which are typically obtained by attacks on encrypted visual data. The more similar two images are in terms of their luminance information, the closer LSS is to 1. Negative values of LSS reflect significant dissimilarities in luminance. ESS is computed by block-based gradient comparison and ranges, with increasing similarity, between 0 and 1. We use the weights and block-sizes proposed by [15] in combination with Sobel edge detection. Figure 3 shows the compression performance for parameterized filters in terms of the LSS/ESS measure. For the evaluation of the compression performance of the parameterized wavelet filters both measures behave similar to the PSNR measure. In the next section we employ the measure for the evaluation of attacks.

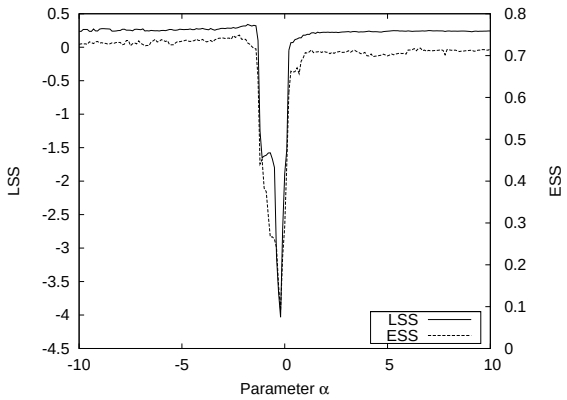


Figure 3: Compression performance (LSS/ESS) of parameterized 9/7 wavelet filters for "Lena", rate 0.1 bpp

4. KEYSPACE

The potential range for α is further restricted by the fact that in both positive and negative direction the variation of the produced filters drops rapidly with higher α. Figure 4 illustrates the problem for encryption. If the source image has been encrypted with a small absolute value for α, the PSNR curve of the reconstructed image with different parameters shows a steep peak for the correct value. Obviously an isolated peak is a favorable situation for encryption as only the correct parameter value will yield the full quality image, while even with small deviation the quality is reduced considerably. With increasing absolute parameter values the peak flattens, making larger absolute values for α increasingly less useful for encryption. These results are in contrast to the results reported by Huang et al. [9], who use

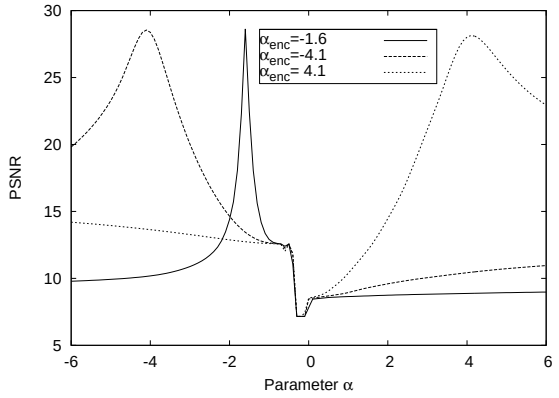


Figure 4: Attacks on "Lena" (PSNR), rate 0.1 bpp

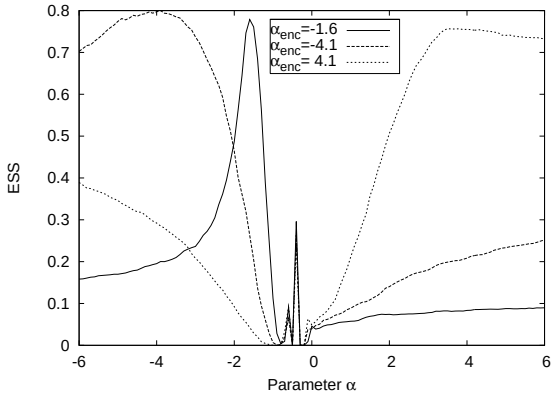


Figure 6: Attacks on "Lena" (ESS), rate 0.1 bpp

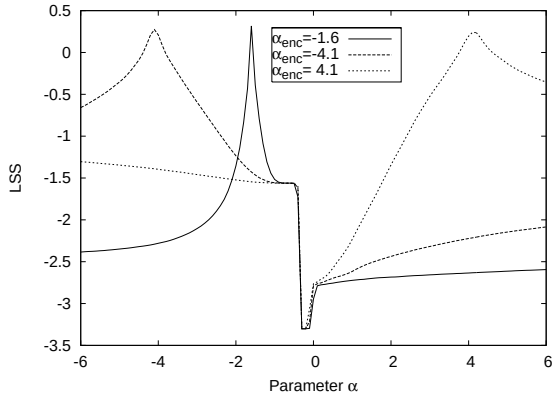


Figure 5: Attacks on "Lena" (LSS), rate 0.1 bpp

the same parameterized lifting scheme for watermark security and report that even a minute change in the value of α makes correct watermark detection virtually impossible.

In consideration of the transparent encryption scheme, the reduction in quality should not occur as high frequency distortions that alter the image beyond recognition. Figures 5 and 6 show the image quality for the same attacks as shown in the previous figure, but measured in LSS and ESS, respectively. Whereas the graph for LSS is very similar to that of PSNR, it can be seen that the peaks for ESS are less steep than those for LSS and PSNR. This means that distortion is introduced in terms of loss of luminance information rather than loss of structural (i.e. edge) information. Images obtained with a wrong parameter still contain most of the structure of the original image, but lack the correct luminance information. This interpretation is congruent with the visual impression, as illustrated by Figure 7, which shows some examples of reconstructed images for "Lena" encrypted with parameter $\alpha = 2.5$: (a) shows the image reconstructed with the correct parameter, (b), (c) and (d) show the image reconstructed with incorrect parameters.[1] For (b) and (c), both of which are reconstructed with a parameter that has the same sign as the parameter used for encryption, it can be seen that, while there is a definite loss of luminance information, much structural information is preserved. The reconstructed image shown in (d) illustrates the fact that for images encrypted with a negative parameter value, image reconstruction with a positive parameter value leads to severe distortion. Still, the little similarity to the original image that remains is structural.

In order to find a sensible range for α that uses as many values as possible while keeping vulnerability of individual values at a minimum, we introduce a measure for the usability of values of α. In the application setting described in the introduction, it is acceptable to gain access to the visual data with a wrong key, as long as the obtained version is sufficiently degraded in quality. In our test runs, we assume that it is acceptable if the quality of an image decoded with the wrong parameter is below 80% of the PSNR value of the image reconstructed with the correct key. Figure 8 show an evaluation of the parameter space, in which for each α used for encoding, we consider decoding values from the direct neighborhood in the interval $[-6 + \alpha, \alpha + 6]$ (with a sampling step size of 0.1). For all values in this interval for which the quality loss is less than 20%, the PSNR value above the 80% level of the correct value is added to the unweighted measure, which is plotted by the first line. The second line shows the same measure, but with the contributions of individual decoding values weighted by their distance from the correct value. While the unweighted measure reflects the overall performance of a single value, the weighted measure also reflects how fast the PSNR quality degenerates with the distance from the correct value. To a certain degree, the choice for the range of α to be used for encoding will depend on the security requirements of the actual application. In our test runs we use the interval $[-6, 6]$, which, as illustrated by Figure 8, comprises most of the usable keys.

As the employed measure is dependent on the properties of the filter rather than on the visual data to be encrypted, we can safely use this interval regardless of the source image. Considering the earlier evaluation of compression performance, we thus get a range of $[-6, -1.4] \cup [0.2, 6]$ that can be used for encryption. As parameters in the immediate vicinity of the value used for encoding still yield more

[1] In all of our test runs we use an adapted version of the JJ2000 reference implementation (`http://jj2000.epfl.ch/`) on 8 bpp grayscale bitmap images of 512^2 pixels.

(a) Reconstruction with correct $\alpha_{\text{dec}} = -2.5$ (PSNR 38dB, LSS 0.997, ESS 0.95)

(b) Reconstruction with $\alpha_{\text{dec}} = -1.58613$ (PSNR 14.7dB, LSS -1.25, ESS 0.46)

(c) Reconstruction with $\alpha_{\text{dec}} = -6.0$ (PSNR 12.5dB, LSS -1.73, ESS 0.37)

(d) Reconstruction with $\alpha_{\text{dec}} = 2.5$ (PSNR 9.3dB, LSS -2.51, ESS 0.1)

Figure 7: Reconstructed images and quality measure results for "Lena" ($\alpha_{\text{enc}} = -2.5$), rate 1 bpp

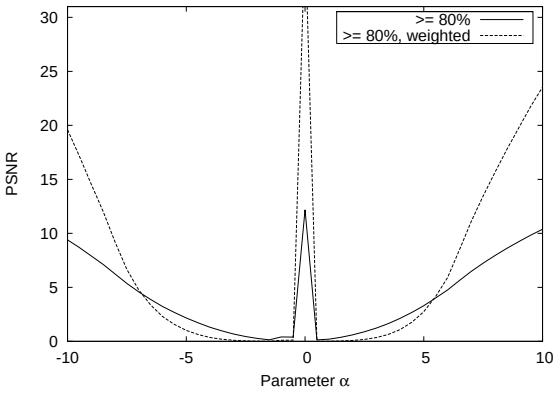


Figure 8: Accumulated quality measure of parameterized 9/7 wavelet filters, "Lena", rate 0.1 bpp

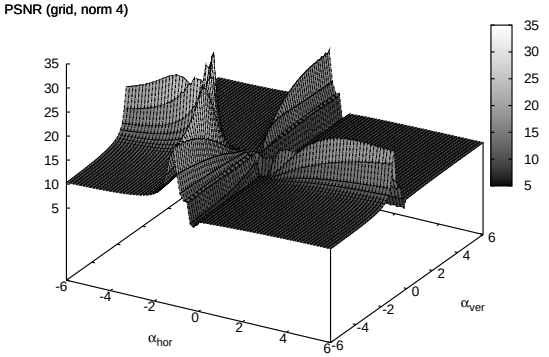


Figure 9: Inhomogeneous variation of lifting parameters for "Lena", rate 1 bpp

than the desired quality, a large enough stepsize between the discrete values of α has to be chosen.

Altogether, the obtained keyspace in one dimension is quite restricted and hardly suitable for real-life application. In order to enlarge the keyspace, we use different parameters for the horizontal and the vertical wavelet decomposition on different decomposition levels. These techniques have been called "non-stationary" (varying on each decomposition level) and "inhomogeneous" (varying in vertical and horizontal orientation) in the context of adaptive compression [24]. Pommer and Uhl [18] use this idea without parameterization for selective encryption. Neither of these methods results in a deterioration of compression performance. Similar to the 1D case we get steeper peaks for smaller absolute values. In order to show that non-stationary and inhomogeneous variations of parameters are principally useful, we present the results of test runs with relatively small values for α. For the inhomogeneous case, Figure 9 shows the results for encoding values of $\alpha_{\text{hor}} = -1.6$ and $\alpha_{\text{ver}} = -2.1$ on all decomposition levels and a step size of 0.1 in the interval $[-6, 6]$ in each direction for decoding. It can be seen that with one correct parameter, results of degraded quality can be obtained, but the full quality version can only be accessed with both parameters correct. Figure 10 shows the situation for non-stationary variation of α. The sequence of encoding parameters is shown in the caption of each plot.

For decoding, we left all parameters on the correct position and only varied the parameter α for levels 1, 3, and 5, respectively, with a stepsize of 0.1 in the interval $[-6, 6]$. Surprisingly, there is little difference between a variation of parameters on a low, medium or high subband. The fact that for all levels a clear peak is produced encourages the use of non-stationary variation. In both, inhomogeneous and non-stationary variation, images reconstructed with wrong parameters retain a certain quality. This is favorable for transparent encryption. However, the sign chosen for encoding has an important impact: if the image was encoded using a negative value for α, then decoding it with a positive value yields worse quality than any negative value. It depends on the requirements of the application, if decoding with an arbitrary parameter, especially the parameter for the original CDF 9/7 filter, is required to always produce an image above a minimum quality level. If this is the case, the parameter range may have to be restricted to negative values of α to ensure decodability with sufficient quality using JPEG 2000 part I codecs.

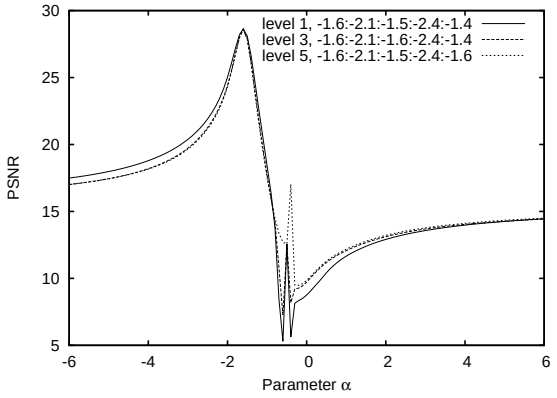


Figure 10: Non-stationary variation of lifting parameters for "Lena", rate 0.1 bpp

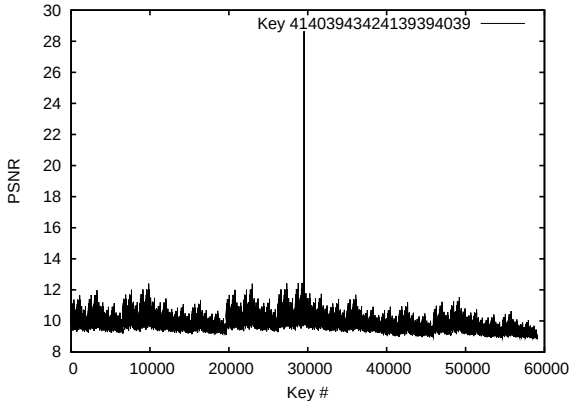


Figure 11: Brute force attack on "Lena", rate 0.1 bpp

The combination of non-stationary and inhomogeneous variation of α leads to $2l$ parameters from which the keyspace can be constructed, where l is the number of decomposition levels. Depending on the minimum acceptable quality degradation, the number of partitions p for each of these parameters can be chosen. The size s of the resulting keyspace is p^{2l}. Reversely, the size of the used keys is $\log_2(s)$ bit. For example, using a two-digit hexadecimal number to describe each parameter, we could construct an 80 bit key for a 5 level wavelet decomposition. The resulting discretization of the range of each individual parameter into 256 partitions leads to a step size of approximately 0.04 and largely avoids full quality results for similar values. However, near the edges of the parameter range, we found that this partitioning tends to be too fine. Possible solutions are a non-uniform partitioning, a restriction in parameter space, a higher number of wavelet decomposition levels, or the use of smaller partitions (a single hexadecimal number still yields 40 bit keys, inducing a step size of approximately 0.65).

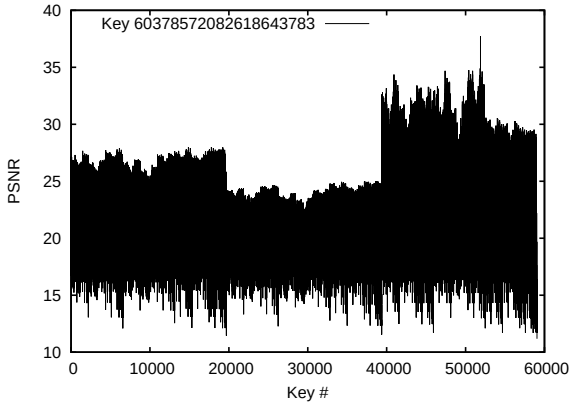
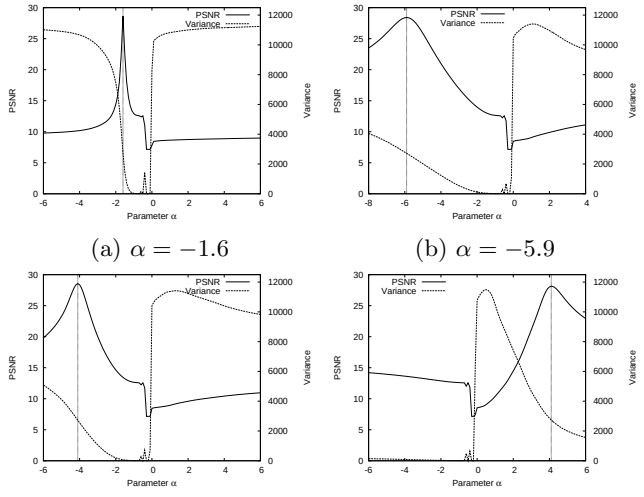


Figure 12: Brute force attack on "Lena", rate 1 bpp

5. SECURITY

Figure 11 shows the result of a brute force attack that uses three partitions for each parameter. The encryption was done using a key with two decimal digits per parameter, the compression result of the correct key was added for reference. For the attack shown in this figure, a key with individual parameters of low absolute values was chosen. For keys that contain more parameters at the border of the range, similar problems occur as in the 1D case and near-hits achieve high PSNR results. Figure 12 shows such a case for a bitrate of 1 bpp. The used key contains values near the border of the range, most notably $\alpha_{\mathrm{hor},2} = -4.1$, $\alpha_{\mathrm{ver},3} = 4.5$, $\alpha_{\mathrm{hor},5} = 4.3$ and $\alpha_{\mathrm{hor},5} = -5.1$. As compared to the previous key, the PSNR of the attacks is significantly higher over the whole range, and the quality of the reconstructed images for key values with many near-hits for the individual parameters (the last third in Figure 12) is just below the correct key.

An obvious problem with the presented encryption scheme is that the parameters that make up the key are independent and the searches for the right individual parameter values are separable. Keys that are congruent with the secret key in some positions yield degraded versions of the original visual data. This makes the scheme very vulnerable to known plain text attacks. If the target visual content is not known in plain text, the attack of the full quality version of the source image is more difficult. A conceivable attack is the use of a heuristic search that assesses the "perceptual quality" of reconstructed versions to find the parameters one by one in the relatively small 1D parameter space. A possible choice for such a heuristics is a measure for the smoothness of the reconstructed image, which has been reported to yield expedient attacks on images encrypted using parameterized orthogonal filters [19]. The implicit assumption of such an attack is that there is a strong correlation between PSNR and smoothness, and ideally a coincidence of a single maximum in PSNR with a single maximum in smoothness. This being the case would make a number of attacks based on this heuristics feasible, ranging from naive stepwise search for steepest descent to elaborate gradient techniques. Even a simple attack based on such a heuristics would reduce the complexity of the search considerably and could impose a significant degree of vulnerability on the presented approach. To assess the potential of such an attack, we use the sample variance s^2 as an inverse measure of smoothness to test the



(a) $\alpha = -1.6$ (b) $\alpha = -5.9$

(c) $\alpha = -4.1$ (d) $\alpha = 4.1$

Figure 13: Correlation of PSNR and Variance

validity of the correlation assumption,

$$s^2 = \frac{1}{N} \sum_{i=0}^{N-1} (x_i - m)^2,$$

where m is the mean pixel value in the reconstructed image and N is the number of pixels.

Figure 13 shows the correlation between PSNR and variance for a single parameter. It can be seen that the strong inverse correlation between a minimum in variance and a maximum in PSNR, which is necessary for the attack described above, does not exist. The attack can be adapted to use the weaker correlation that can be observed: the peak in PSNR never occurring in regions of relatively high variance. This can be used to make a few "guesses" for each parameter over the whole range and eliminate the ones with high variance to obtain a combination of parameters that will yield an image of comparatively good quality. For a scheme aiming at transparent encryption this vulnerability is not critical, as long as the obtained quality stays below the maximum acceptable quality. As can be seen in Figure 13, the correlation between smoothness and PSNR is not strong enough to substantially reduce search complexity for the full quality visual data. Other than for orthogonal filter parameterization, the lifting parameterization is not vulnerable to a heuristic using variance as a measure. This is due to the fact that in the former case, which aims at providing confidentiality rather than transparent encryption, images decoded with the wrong key contain a high amount of high frequency noise. For the presented approach, no such noise is added, rather luminance information (along with a portion of the edge information) is lost.

6. CONCLUSION

The main advantage of the presented lightweight encryption scheme is that, while maintaining competitive compression performance, it comes at extremely low computational overhead and innately supports transparent encryption. The relatively restricted keyspace that results from the lifting parameterization can be enlarged by using different parameter values for for the vertical and horizontal wavelet decomposition on each decomposition level. The main problem of our scheme is the separability of these parameters which allows relatively low-cost attacks. However, in many settings that require "soft" encryption, e.g. in the area of mobile multimedia applications, the level of security will suffice.

In future work, we will aim at enlarging the keyspace. A possible approach is a non-uniform partitioning of the possible range of α with more parameters of low absolute value, which produce filters that are less vulnerable to attacks. Another approach which we will investigate is to use wavelet packet decompositions in combination with the best basis algorithm and enlarge the keyspace by using a different parameterized filter for each individual subband. We will also investigate the merit of combining the presented approach with other low-cost approaches, like permutation of wavelet coefficients, in order to enhance security. Furthermore, higher dimensional parameter spaces will be considered and investigated with respect to their trade-off between compression performance and security.

7. REFERENCES

[1] A. Cohen, I. Daubechies, and J. Feauveau. Bi-orthogonal bases of compactly supported wavelets. *Comm. Pure and Appl. Math.*, 45:485–560, 1992.

[2] I. Daubechies and W. Sweldens. Factoring wavelet transforms into lifting steps. *J. Fourier Anal. Appl.*, 4(3):245–267, 1998.

[3] W. Dietl, P. Meerwald, and A. Uhl. Protection of wavelet-based watermarking systems using filter parametrization. *Signal Processing (Special Issue on Security of Data Hiding Technologies)*, 83:2095–2116, 2003.

[4] J. Dittmann and R. Steinmetz. A technical approach to the transparent encryption of MPEG-2 video. In S. K. Katsikas, editor, *Communications and Multimedia Security, IFIP TC6/TC11 Third Joint Working Conference, CMS '97*, pages 215–226, Athens, Greece, Sept. 1997. Chapman and Hall.

[5] M. V. Droogenbroeck. Partial encryption of images for real-time applications. In *Proceedings of the 4th 2004 Benelux Signal Processing Symposium*, pages 11–15, Hilvarenbeek, The Netherlands, Apr. 2004.

[6] M. V. Droogenbroeck and R. Benedett. Techniques for a selective encryption of uncompressed and compressed images. In *Proceedings of ACIVS (Advanced Concepts for Intelligent Vision Systems)*, pages 90–97, Ghent University, Belgium, Sept. 2002.

[7] R. Grosbois, P. Gerbelot, and T. Ebrahimi. Authentication and access control in the JPEG 2000 compressed domain. In A. Tescher, editor, *Applications of Digital Image Processing XXIV*, volume 4472 of *Proceedings of SPIE*, pages 95–104, San Diego, CA, USA, July 2001.

[8] F. Hartenstein. Parametrization of discrete finite biorthogonal wavelets with linear phase. In *Proceedings of the 1997 International Conference on Acoustics, Speech and Signal Processing (ICASSP'97)*, Apr. 1997.

[9] J. Huang, J. Hu, D. Huang, and Y. Q. Shi. Improve security of fragile watermarking via parameterized wavelet. In *Proceedings of the IEEE International*

Conference on Image Processing (ICIP'04), Singapore, oct 2004. IEEE Signal Processing Society.

[10] T. Köckerbauer, M. Kumar, and A. Uhl. Lightweight JPEG 2000 confidentiality for mobile environments. In *Proceedings of the IEEE International Conference on Multimedia and Expo, ICME '04*, Taipei, Taiwan, June 2004.

[11] T. Kunkelmann. Applying encryption to video communication. In *Proceedings of the Multimedia and Security Workshop at ACM Multimedia '98*, pages 41–47, Bristol, England, Sept. 1998.

[12] T. Kunkelmann and U. Horn. Partial video encryption based on scalable coding. In *5th International Workshop on Systems, Signals and Image Processing (IWSSIP'98)*, pages 215–218, Zagreb, Croatia, 1998.

[13] B. Macq and J. Quisquater. Digital images multiresolution encryption. *The Journal of the Interactive Multimedia Association Intellectual Property Project*, 1(1):179–206, Jan. 1994.

[14] B. M. Macq and J.-J. Quisquater. Cryptology for digital TV broadcasting. *Proceedings of the IEEE*, 83(6):944–957, June 1995.

[15] Y. Mao and M. Wu. Security evaluation for communication-friendly encryption of multimedia. In *Proceedings of the IEEE International Conference on Image Processing (ICIP'04)*, Singapore, Oct. 2004. IEEE Signal Processing Society.

[16] R. Norcen and A. Uhl. Selective encryption of the JPEG2000 bitstream. In A. Lioy and D. Mazzocchi, editors, *Communications and Multimedia Security. Proceedings of the IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security, CMS '03*, volume 2828 of *Lecture Notes on Computer Science*, pages 194 – 204, Turin, Italy, Oct. 2003. Springer-Verlag.

[17] R. Norcen and A. Uhl. Encryption of wavelet-coded imagery using random permutations. In *Proceedings of the IEEE International Conference on Image Processing (ICIP'04)*, Singapore, Oct. 2004. IEEE Signal Processing Society.

[18] A. Pommer and A. Uhl. Wavelet packet methods for multimedia compression and encryption. In *Proceedings of the 2001 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing*, pages 1–4, Victoria, Canada, Aug. 2001. IEEE Signal Processing Society.

[19] A. Pommer and A. Uhl. Selective encryption of wavelet-packet encoded image data — efficiency and security. *ACM Multimedia Systems (Special issue on Multimedia Security)*, 9(3):279–287, 2003.

[20] J. Schneid and S. Pittner. On the parametrization of the coefficients of dilation equations for compactly supported wavelets. *Computing*, 51:165–173, May 1993.

[21] Y.-S. Seo, M.-S. Kim, H.-J. Park, H.-Y. Jung, H.-Y. Chung, Y. Huh, and J.-D. Lee. A secure watermarking for JPEG-2000. In *Proceedings of the IEEE International Conference on Image Processing (ICIP'01)*, Thessaloniki, Greece, Oct. 2001.

[22] W. Sweldens. The lifting scheme: A custom-design construction of biorthogonal wavelets. *Appl. Comput. Harmon. Anal.*, 3(2):186–200, 1996.

[23] D. Taubman and M. Marcellin. *JPEG2000 — Image Compression Fundamentals, Standards and Practice*. Kluwer Academic Publishers, 2002.

[24] A. Uhl. Image compression using non-stationary and inhomogeneous multiresolution analyses. *Image and Vision Computing*, 14(5):365–371, 1996.

[25] A. Uhl and A. Pommer. Are parameterised biorthogonal wavelet filters suited (better) for selective encryption? In J. Dittmann and J. Fridrich, editors, *Multimedia and Security Workshop 2004*, pages 100–106, Magdeburg, Germany, September 2004.

[26] A. Uhl and A. Pommer. *Image and Video Encryption. From Digital Rights Management to Secured Personal Communication*, volume 15 of *Advances in Information Security*. Springer-Verlag, 2005.

[27] Y. Wu and R. H. Deng. Progressive protection of JPEG2000 codestreams. In *Proceedings of the IEEE International Conference on Image Processing (ICIP'04)*, Singapure, Oct. 2004. IEEE Signal Processing Society.

[28] C. Yuan, B. B. Zhu, M. Su, Y. Wang, S. Li, and Y. Zhong. Layered access control for MPEG-4 FGS. In *Proceedings of the IEEE International Conference on Image Processing (ICIP'03)*, Barcelona, Spain, Sept. 2003.

[29] G. Zhong, L. Cheng, and H. Chen. A simple 9/7-tap wavelet filter based on lifting scheme. In *Proceedings of the IEEE International Conference on Image Processing (ICIP'01)*, pages 249–252, October 2001.