© IEEE. Personal use of this material is permitted. However, permission to reprint/republish this material for advertising or promotional purposes or for creating new collective works for resale or redistribution to servers or lists, or to reuse any copyrighted component of this work in other works must be obtained from the IEEE.

This material is presented to ensure timely dissemination of scholarly and technical work. Copyright and all rights therein are retained by authors or by other copyright holders. All persons copying this information are expected to adhere to the terms and constraints invoked by each author's copyright. In most cases, these works may not be reposted without the explicit permission of the copyright holder.

# Security Enhancement for Lightweight JPEG 2000 Transparent Encryption

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

***Abstract*— We present improvements in lightweight transparent JPEG 2000 encryption with lifting parameterized biorthogonal wavelet filters. Security is further enhanced by a combination with the wavelet packet transform. Different methods for the selection of a suitable wavelet packet basis are presented, which also make a certain amount of control in the trade-off between security and computational complexity possible. The combined approach of parameterized filters and wavelet packets is evaluated with regard to compression performance, complexity and security.**

***Keywords*—JPEG 2000, lightweight transparent encryption, parameterized wavelet packets**

## I. Introduction

In recent years multimedia security has matured into a central and important research topic. The need for privacy and confidentiality in multimedia applications that are becoming increasingly popular and widespread, and efficient access control to secure revenue streams by preventing unauthorized access to multimedia content, are just two reasons for this development. With the increasing use of the JPEG 2000 standard [1], the need arises for methods that provide confidentiality and access control in JPEG 2000, as addressed in part 8 (JPSEC) of the standard. In this paper, we discuss techniques to enhance the security of JPEG 2000 lightweight encryption, based on parameterized wavelet filters and the wavelet packet transform.

When visual content is to be encrypted, a possible approach is the full encryption of the compressed bitstream with a traditional cipher, such as AES. The high level of security that this approach warrants comes at the cost of high computational demands and loss of functionality, such as retaining bitstream compliance and scalability [2]. Lightweight encryption aims at trading security for other functionality and/or decreasing computational complexity. In the context of wavelet coded image data, various methods have been proposed for lightweight encryption: securing coefficients by encrypting sign bits and by scrambling refinement bits [3], partial encryption of significance information [4], scrambling coefficient signs in code-blocks or entire layers in a JPEG 2000 bitstream [5], [6], and random permutations of coefficients and code-blocks [7]. All of these approaches aim at providing full confidentiality, i.e. completely blocking access to the encrypted data for users who lack key data. However, especially in the area of multimedia there are applications which do not require strict confidentiality. Such decreased requirements in security allow a controlled trade-off between security, complexity and functionality.

Macq and Quisqater [8] introduce the term "transparent encryption" to refer to encryption schemes in which portions of the original data are accessible in degraded quality even without key. The full quality version is restricted to legitimate users. Transparent schemes are applied in try-and-buy scenarios, in which access to the lower quality data may serve as an incentive for purchasing the full quality version. For transparent encryption of JPEG images, [9] suggest to encrypt sign and magnitude bits of medium and high frequency DCT coefficients. [10] extends this 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). Transparent encryption based on the encryption of enhancement layers is proposed by [11], [12] using a scalable video codec based on a spatial resolution pyramid and by [13] using a SNR scalable MPEG-2 encoder/decoder.

We present methods for lightweight transparent JPEG 2000 encryption, that allow a controlled adjustment of the balance between security and complexity. Vulnerability to some attacks that exists for previously suggested approaches is decreased or completely avoided.

## II. Security Issues for Lightweight Encryption with Parameterized Filters

In a previously suggested approach [14], secret parameterized biorthogonal wavelet filters are used for lightweight transparent encryption. The idea of this method is to keep the parameters that are used for creating the wavelet filters secret, either by making them the secret key or by encrypting the relevant portion of the header with a traditional cipher. In this way, the properties of the transform domain are hidden and reconstruction of the full quality image is restricted to legitimate users. Transparent encryption is supported in that reconstruction can be performed with filters that are parameterized with values different from the parameter used for encoding, but distortion is introduced for the images obtained in this manner. The produced bitstream is compliant to the JPEG 2000 standard, so a lower quality version of the original image can be obtained with a standard JPEG 2000 part 1 decoder. In order to get access to the full quality

0-7803-9282-5/05/$20.00 ©2005 IEEE

version, the correct key data has to be obtained and a JPEG 2000 part 2 codec has to be used. The approach, which integrates encryption with compression, has the advantage that the overhead in computational complexity is low and the amount of information to be encrypted is small.

The used parameterization for biorthogonal wavelet filters is integrated with the wavelet lifting scheme [15]. It is based on the combination of the lifting steps of the 9/7 wavelet [16] with conditions of the perfect reconstruction theorem [17] and the symmetric properties of the 9/7 wavelet. Parameterization is only dependent on a single parameter $\alpha$. The keyspace spanned by the discretization of the available parameter range of $\alpha$ is quite limited. To increase the number of possible keys, the use of "inhomogeneous" and "non-stationary" variation in the used parameterized wavelet filters is proposed. "Non-stationary" variation refers to the use of differently parameterized wavelet filters for each resolution level. In the case of "inhomogeneous" variation, differently parameterized wavelet filters are used for horizontal and vertical wavelet decomposition.

Some attacks on this scheme are discussed in [14]. If inhomogeneous and non-stationary variation are used, the parameter space is of dimension $2l$ where $l$ is the number of wavelet decomposition levels. A full search of all discrete parameter values (the exact number of which depends on the discretization function used) in this space is not feasible. Only a search with larger discretization bins can be performed, but as shown in the results in [14], such a search technique cannot be used to obtain the full quality version of the image. However, for encoding values at the border of the parameter range, close hits in the attack achieve results that are near the original quality, which rules out application scenarios that require a guaranteed degradation in image quality. To enhance security in this respect, we propose the use of non-uniform discretization and wavelet packets.

## III. Improving Security

### A. Tuning the Parameter Range

The possible range for $\alpha$ that yields good compression results and maximizes keyspace size is given as $[-6, -1.4] \cup [0.2, 6.0]$ in [14]. Discretization is performed in intervals of equal size. The admissible size of the intervals depends on the quality degradation required by the application. In our tests we use 255 bins for discretization. We have found that compression performance for the parameterized filters is influenced by the quantization step signalling strategy chosen for JPEG 2000 encoding. JPEG 2000 part 1 defines two strategies: if *expounded* signalling is used then quantization steps are coded for each subband individually, whereas if *derived* is used, quantization step signalling is only done for the approximation subband, and the step size is inferred from this value for the detail subbands. As illustrated by Figure 1, low positive parameter values generate filters for which *derived* signalling fails. If this strategy has to be used (which is the case for complex wavelet packet decompositions at low bitrate), then the parameter range has to be adapted accordingly.

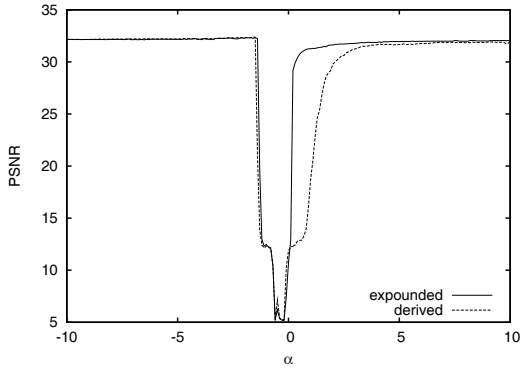



Fig. 1. Compression performance of parameterized filters for different JPEG 2000 quantization signalling strategies ("Lena", rate 0.25bpp)

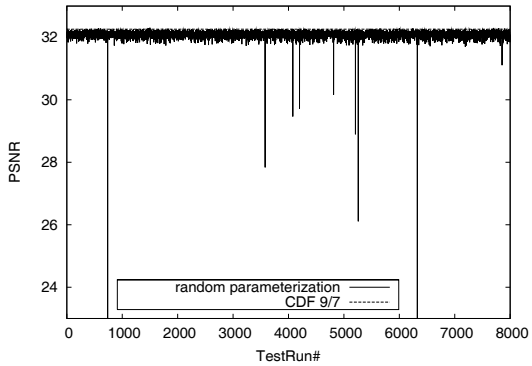
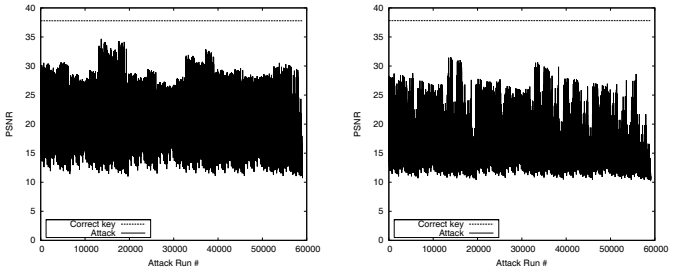



Fig. 2. Compression performance for random parameterization with *expounded* signalling, ("Lena", rate 0.25bpp)

Interestingly, we also found combinations of parameterized filters, that when used together (by non-stationary and inhomogeneous combination) produced non-competitive results for the expounded signalling strategy. Each of these filters achieves normal compression quality when used "alone" in a classical DWT. Surprisingly, the combinations also work fine with the *derived* strategy. Apparently the combination of these filters produces coefficient data that makes the analysis of the *expounded* strategy fail. In all of these combinations at least one positive filter value is contained, but not necessarily of low value. This gives two options: (a) One option is to check the quality of the reconstructed image after encryption. This introduces computational overhead, but preserves keyspace size. If an unsuitable combination occurs, encryption has to be repeated. This event is unlikely, but still the potential overhead in computational complexity might make this option infeasible in some scenarios. (b) Discarding the positive range leads to a severe reduction in keyspace, but this option completely avoids the unsuitable parameter combinations.

In our tests, we use equal sizes for the negative and positive range, $[-6, -1.4] \cup [1.4, 6.0]$. For this range, Figure 2 shows the results of 8000 test runs with randomized non-stationary and inhomogeneous variation for the pyramidal wavelet decomposition with *expounded* signalling. It can be seen that the combinations for which this strategy fails are rare (about $0.1\%$).

Large absolute values of $\alpha_{\text{enc}}$ used for encoding have been




(a) Uniform discretization (b) Square discretization

Fig. 3. Examples of discretization strategies, "Lena", rate 1

shown to be vulnerable to attacks that try to approximate $\alpha_{\text{enc}}$. The environment of values near $\alpha_{\text{enc}}$ that yield results of high quality when used for decoding increases in size with larger absolute value of $\alpha_{\text{enc}}$. In order to make the encryption scheme more robust and have parameter values with similar security, we use the square function to partition the range of $\alpha_{\text{enc}}$. Figure 3 shows that by this measure, simple attacks like probing the keyspace with a number of values for each of the parameters become less effective. The results shown are for "Lena" at rate 1 bpp, with the attack using three guesses for each parameter. Figure 3 also shows that the scheme cannot be used for providing strict confidentiality, as any combination of parameters will yield images in which the original content is discernible. For some combinations quality degradation is small, which is not acceptable for most application scenarios.

### B. Wavelet Packets

The wavelet packet (WP) transform [18] is a generalization of the pyramidal (or Mallat) wavelet transform. In the case of the wavelet packet transform, recursive decomposition is not restricted to the approximation subband, but can also be applied to any of the detail subbands. This results in a larger space of possible decomposition structures, of which the pyramidal decomposition structure is only one element. In combination with the best basis algorithm [18], wavelet packets have successfully been employed for compression of visual data with unusual properties in the frequency domain, such as textures with oscillatory patterns [19]. Secret wavelet packet decompositions have been proposed for lightweight encryption by [20].

To enhance encryption security, we extend the concepts of non-stationary and inhomogeneous variation in parameters to wavelet packets. Using a pseudo-random number generator, for each subband we create one parameter value for horizontal decomposition and one value for vertical decomposition. For a full level $l$ wavelet packet decomposition this leads to $\sum_{i=1}^{l} 2 \cdot 4^{(i-1)}$ parameters involved, e.g. 682 parameters for level 5. In the pyramidal case there are only $2l$ parameters, i.e. 10 parameters for level 5. The advantage of using wavelet packets is a massive increase in keyspace size. The drawback of using wavelet packets is an increase in computational complexity: Each additional parameter comes at the cost of a wavelet decomposition of a detail subband. The balance between security and complexity can be regulated by choosing more or less complex wavelet packet decompositions. There are several ways to select a wavelet packet decomposition. Each has different implications for compression performance, complexity and security, which is discussed in the following.

*a) Pyramidal wavelet decomposition:* The pyramidal wavelet decomposition is low in computational demands and yields good compression results for natural images. As discussed above, when parameterized filters are used for lightweight transparent encryption, the level of security is significantly lower than for wavelet packet decompositions.

*b) Full wavelet packet decomposition:* In the full wavelet packet decomposition recursive decomposition is applied to each subband. If the full wavelet packet decomposition is used, the size of the keyspace is maximized. At the same time, the decomposition and reconstruction of this approach are computationally demanding: The order of complexity for a level $l$ full wavelet packet decomposition of an image of size $N^2$ is $\mathcal{O}(\sum_{i=1}^{l} 2^{2(i-1)} \frac{N^2}{2^{2(i-1)}})$ compared to $\mathcal{O}(\sum_{i=1}^{l} \frac{N^2}{2^{2(i-1)}})$ for the pyramidal decomposition. A drawback with using the full WP-decomposition is that compression performance drops for most images.

*c) Best basis:* The best basis algorithm (BBA) applies an additive costfunction to find an optimal wavelet packet decomposition structure for a target image. Because for this purpose first a full wavelet packet decomposition has to be created which is then successively pruned, this method has the highest complexity of all. The advantage of this method lies in the wavelet packet structured being tailored to the source image, which leads to increased compression performance. The size of keyspace depends on the source images used. This fact makes using the best basis an interesting option for databases of images that typically show oscillatory patterns, such as fingerprints or textures. For such images, the wavelet decomposition structures found with the best basis algorithm typically differ markedly from the pyramidal decomposition and compression performance is increased.

*d) Randomized WP decomposition structure:* For natural images the marginal gains in compression performance do not justify the high computational demands of the best basis algorithm. To control the level of complexity in our scheme, we use randomized wavelet packet structures. The algorithm for creating randomized wavelet packet structures proposed by [20] allows to set requirements and limits for the complexity of the resulting wavelet packet structure. Furthermore, it allows to tune the properties of the randomized structures to work well with natural images (at the expense of keyspace size compared to a full decomposition). The set of parameters includes maximum global decomposition depth of all subbands, minimum and maximum decomposition depth of the approximation subband, as well as parameters influencing the probability of decomposition for a subband, based on its decomposition depth. It can been shown that the average compression quality for randomized wavelet packet structures with appropriate parameters is competitive with the pyramidal decomposition [20].

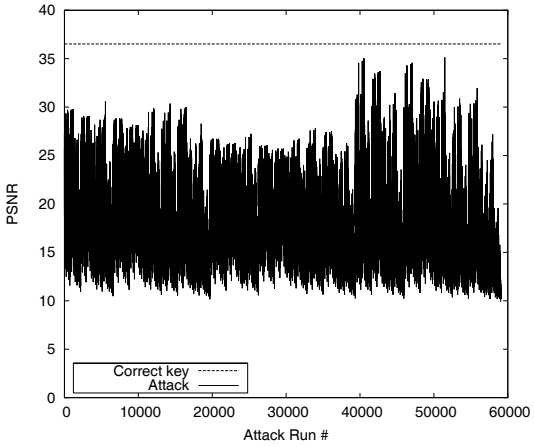



Fig. 4. Attack on "Barbara" (1bpp, uniform bins, pyramidal decomposition)

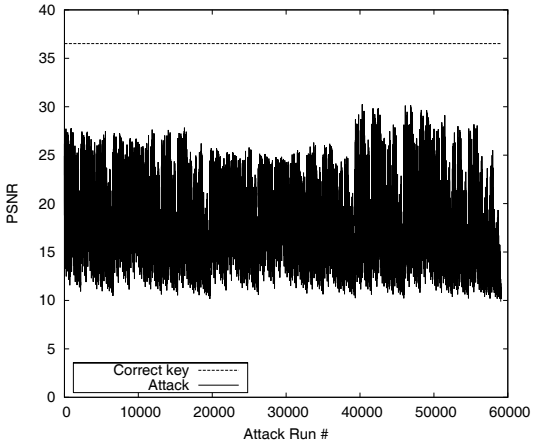



Fig. 5. Attack on "Barbara" (1bpp, uniform bins, randomized WP decomposition)

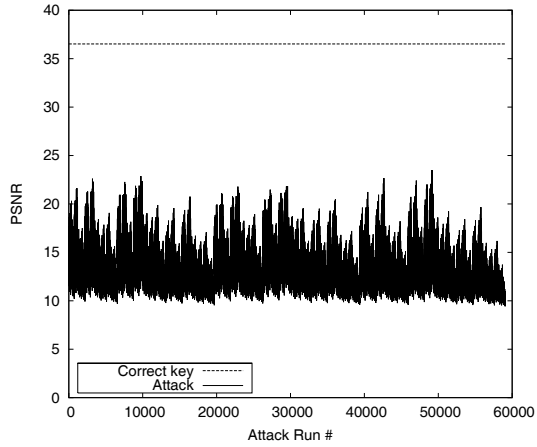



Fig. 6. Attack on "Barbara" (1bpp, square bins, randomized WP decomposition)

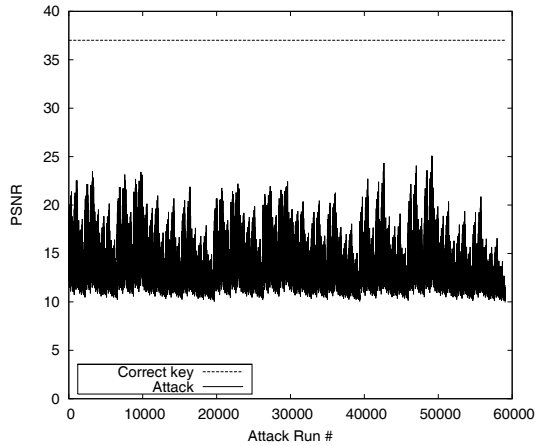



Fig. 7. Attack on "Lena" (1bpp, square bins, randomized WP decomposition)

For all wavelet packet decompositions it should be noted that for *expounded* quantization step size signalling, the information overhead increases exponentially. Therefore it is necessary to use *derived* signalling of quantization step sizes when complex wavelet packet decomposition with many subbands are used at low bitrates. As discussed above, this makes a reduction in the positive part of the parameter range necessary.

## IV. Security Evaluation

Attacks that try to search the parameter space become more difficult due to the increased number of parameters and the improved method of discretization. In the following simulated attacks we aim at assessing the contribution that is made to security by these two improvements, so we assume the packet decomposition structure is known to the attacker. Keeping the wavelet packet structure secret can be used to further increase security. If randomized wavelet packet structures are created with a pseudo-random number generator as the source of entropy, then the same seed as for the randomized filters can be used. Thus the amount of information to be encrypted does not increase. A discussion of attacks on secret wavelet packet scenarios can be found in [20].

Figures 4 to 7 illustrate the gain in security that can be achieved by using randomized wavelet filters in combination with wavelet packets. For Figure 4, the image "Barbara" was encoded with the pyramidal wavelet transform and uniform discretization was used for the randomized wavelet filters at each decomposition level. Figure 5 illustrates the increase in security that can be achieved with the introduction of randomized wavelet packets. Figure 6 and Figure 7 show the performance for randomized wavelet packet structures in combination with non-uniform discretization for "Barbara" and "Lena", respectively. The random structures were generated with a maximum global decomposition depth of five, a fixed decomposition level for the approximation subband of five, and decomposition probabilities that produce wavelet packet structures of medium complexity. For the pyramidal decomposition in combination with uniform discretization some results of the search attack are very near the full quality that should only be obtainable with the correct key (Fig. 4).

Wavelet packets lead to some improvement (Fig. 5). In the case of wavelet packets with non-uniform discretization, the quality degradation is most efficient, and quality for attacked images ranges in a band from about 10 to 23 and 25 dB for "Barbara" (Fig. 6) and "Lena" (Fig. 7), respectively. For transparent encryption this ensures discernibility, while maintaining a clear degradation of visual quality compared to the original image. Figure 8 gives visual examples for both images (attack run #20739).

(a) "Lena", Original Image

(b) Pyramidal decomposition, uniform discretization (22 dB)

(c) WP decomposition, non-uniform discretization (18.8 dB)

(d) "Barbara", Original Image

(e) Pyramidal decomposition, uniform discretization (23.3 dB)

(f) WP decomposition, non-uniform discretization (18 dB)

Fig. 8. Visual Examples of Attacks, 1bpp

## V. Conclusion

The proposed approach has the advantage of providing a handle for adjusting the balance between complexity and security. If the pyramidal decomposition is used, a minimum level of security can be achieved at a very low additional computational complexity. By adjusting the complexity of the used (randomized) wavelet packet structures, security can be increased at the cost of a rise in complexity. A drawback of this approach is that there is a significant amount of variation in the quality of images obtained with wrong keys.

In future work we will investigate into methods to influence and stabilize quality degradation. Furthermore, we will assess the advantages and disadvantages of introducing anisotropic wavelet packets, i.e. wavelet packets that produce subbands of non-uniform sizes, to further increase security.

## Acknowledgment

This work was partly funded by the Austrian Science Fund (FWF), project number P15170. Dominik Engel was supported by the Austrian Academy of Sciences.

## References

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

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

[3] W. Zeng and S. Lei, "Efficient frequency domain video scrambling for content access control," in *Proceedings of the seventh ACM International Multimedia Conference 1999*, (Orlando, FL, USA), pp. 285–293, Nov. 1999.

[4] H. Cheng and X. Li, "Partial encryption of compressed images and videos," *IEEE Transactions on Signal Processing*, vol. 48, no. 8, pp. 2439–2451, 2000.

[5] R. Grosbois, P. Gerbelot, and T. Ebrahimi, "Authentication and access control in the JPEG 2000 compressed domain," in *Applications of Digital Image Processing XXIV* (A. Tescher, ed.), vol. 4472 of *Proceedings of SPIE*, (San Diego, CA, USA), pp. 95–104, July 2001.

[6] R. Norcen and A. Uhl, "Selective encryption of the JPEG2000 bitstream," in *Communications and Multimedia Security. Proceedings of the IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security, CMS '03* (A. Lioy and D. Mazzocchi, eds.), vol. 2828 of *Lecture Notes on Computer Science*, (Turin, Italy), pp. 194 – 204, Springer-Verlag, Oct. 2003.

[7] 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), IEEE Signal Processing Society, Oct. 2004.

[8] B. M. Macq and J.-J. Quisquater, "Cryptology for digital TV broadcasting," *Proceedings of the IEEE*, vol. 83, pp. 944–957, June 1995.

[9] 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)*, (Ghent University, Belgium), pp. 90–97, Sept. 2002.

[10] M. V. Droogenbroeck, "Partial encryption of images for real-time applications," in *Proceedings of the 4th 2004 Benelux Signal Processing Symposium*, (Hilvarenbeek, The Netherlands), pp. 11–15, Apr. 2004.

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

[12] T. Kunkelmann and U. Horn, "Partial video encryption based on scalable coding," in $5^{\text{th}}$ *International Workshop on Systems, Signals and Image Processing (IWSSIP'98)*, (Zagreb, Croatia), pp. 215–218, 1998.

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

[14] D. Engel and A. Uhl, "Parameterized biorthogonal wavelet lifting for lightweight JPEG 2000 transparent encryption," in *Proceedings of ACM Multimedia and Security Workshop, MM-SEC '05*, (New York, NY, USA), pp. 63–70, Aug. 2005.

[15] H. Zhong and L. Jiao, "Novel secret key watermarking system," in *Proceedings of SPIE, International Symposium on Multispectral Image Processing and Pattern Recognition, Image Compression and Encryption Technologies*, vol. 4551, (Wuhan, China), Oct. 2001.

[16] I. Daubechies and W. Sweldens, "Factoring wavelet transforms into lifting steps," *Journal of Fourier Analysis Applications*, vol. 4, no. 3, pp. 245–267, 1998.

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

[18] M. Wickerhauser, *Adapted wavelet analysis from theory to software*. Wellesley, Mass.: A.K. Peters, 1994.

[19] D. Engel and A. Uhl, "Adaptive image compression of arbitrarily shaped objects using wavelet packets," in *Picture Coding Symposium 2003 (PCS'03)*, (Saint Malo, France), pp. 283–288, Apr. 2003.

[20] A. Pommer and A. Uhl, "Selective encryption of wavelet-packet encoded image data — efficiency and security," *ACM Multimedia Systems (Special issue on Multimedia Security)*, vol. 9, no. 3, pp. 279–287, 2003.