On JPEG2000 Error Concealment Attacks

Thomas Stütz and Andreas Uhl *

University of Salzburg, Department of Computer Sciences, Jakob-Haringerstr. 2,
Salzburg, Austria
{tstuetz, uhl}@cosy.sbg.ac.at

Abstract. In this work, JPEG2000 error resilience options and error concealment strategies are discussed and evaluated. Error resilience options and error concealment strategies have been employed to mimic attacks against selective / partial JPEG2000 encryption schemes. Thus the security evaluation of these selective / partial encryption schemes relies on the proper working of the JPEG2000 error concealment. Recommendations for JPEG2000 encryption given in previous work have to be reassessed on the basis of our results. Improvements to the error concealment code of the JPEG2000 reference software JJ2000 are presented.

1 Introduction

Today visual data are predominantly present in digital form. Current threats to these data are on the one hand transmission and storage errors that may render the entire data useless and the illegitimate distribution of these data on the other. In order to protect the visual data and fulfill application requirements specifically tailored encryption approaches are necessary [1–3]. Especially JPEG2000 encryption has been the subject of a considerable amount of research [4–12]. Many of the proposed encryption schemes can be applied in a selective / partial way. There is a close connection between selective / partial encryption and an error-prone communication channel or storage device, as in all these cases compressed visual data is damaged. An overview of the involved processes is given in figure 1. In [2, pp.107–114] selective encryption of the JPEG2000 codestream is discussed and analyzed in terms of security. It is proposed to employ the JPEG2000 built-in error resilience tools to mimic attacks against selective encryption (therefore this attack is called error concealment attack). The main idea is that an attacker can identify the encrypted portions in the codestream and reconstruct the image on the basis of the unencrypted data. This idea of a distinct cryptanalytic model for selective encryption has later been formulated more explicitly [13]. If parts of the JPEG2000 codestream are encrypted, these parts introduce noise into the reconstructed image. An attacker is interested in increasing the image quality and therefore needs to identify and conceal the encrypted parts (thereby exploiting all available information). These attacks can be

* This work has been partially supported by the Austrian Science Fund, project no. 15170.

mimicked by JPEG2000 compression of the image with error resilience options enabled, which enable the JPEG2000 decoder to perform the appropriate error concealment. In [2] the authors conclude that on the basis of their experimental evaluations, it is sufficient to encrypt the leading 20% of the codestream in order to confidentially hide all image information. In this paper, we will show that this rule of thumb does not hold if the JPEG2000 reference software's error concealment is improved. In the technology examples of [3], confidentiality is claimed if only 1% of the JPEG2000 codestream is encrypted – a claim that that will have to be reconsidered. Additionally, several concealment strategies are evaluated.

The focus of previous contributions to JPEG2000 error resilience [14, 15] has been the comparison of JPEG2000 with MPEG-4, which has revealed that JPEG2000 offers superior error resilience tools compared to MPEG-4. Apart from the reference software [16], namely JJ2000 (http://jj2000.epfl.ch) and JasPer, only few implementations are available, e.g., Taubman's Kakadu and an implementation distributed by the company Luratech. However, those implementations and their source codes are not publicly available and therefore of limited interest to the research community. JasPer does not conceal detected bitstream errors (in fact, only the error detection mechanism is standardized, not the concealment), but JJ2000 offers error concealment.

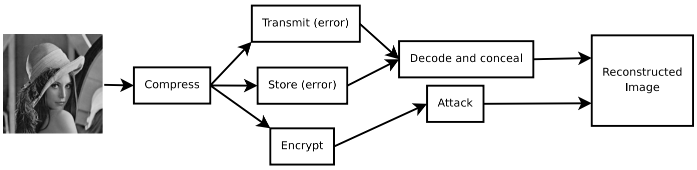


Fig. 1. Overview of the processes.

JPEG2000 will be briefly reviewed in section 2. In section 2.1 the JPEG2000 error resilience options and error concealment strategies are discussed in more detail. Improvements to the JJ2000 error concealment code are discussed in section 3. Experimental results for the different error resilience and concealment strategies are presented in section 4. Furthermore we will show that selective JPEG2000 encryption preserves considerable amount of visual information. Finally we conclude in section 5.

2 An Overview of the JPEG2000 Compression Pipeline

JPEG2000 [17] employs a wavelet transform; Part I of the standard [18] specifies an irreversible 9/7 and a reversible integer 5/3 wavelet transform. An image may consist of several components, which may be subject to an optional multiple component transform. The components are further subdivided into tiles, which are independently wavelet transformed. After the wavelet transform the coefficients are quantized and encoded using the EBCOT scheme, which renders distortion scalability possible. Thereby the coefficients are grouped into codeblocks and these are encoded bitplane by bitplane. The first non-zero bitplane is only coded with a cleanup pass, while every other bitplane is coded with three coding passes, namely significance propagation, magnitude refinement and cleanup pass. The JPEG2000 codestream – the standard's term for a JPEG2000 coded image – consists of headers (main header, tile headers, tile part headers) and packets, which are further subdivided into a packet header and a packet body. The packet header contains vital information for the decoding process, such as the number of leading zero bitplanes of a codeblock (all coefficients of the codeblock have a zero bit in these MSB bitplanes and only the remaining bitplanes are entropy coded). The packet bodies contain the entropy coded coefficient data of the codeblocks (also denoted the codeblock's bitstream). The codeblock's bitstream is partitioned such that each partition corresponds to the contribution of the codeblock to a certain quality layer. A packet body consists of the CCPs (codeblock contribution to a packet) of a certain resolution, quality layer and precinct (a spatial inter-subband partitioning structure that contains one to several codeblocks) of a tile of a component. The ordering of the packets defines the progression order of the JPEG2000 codestream.

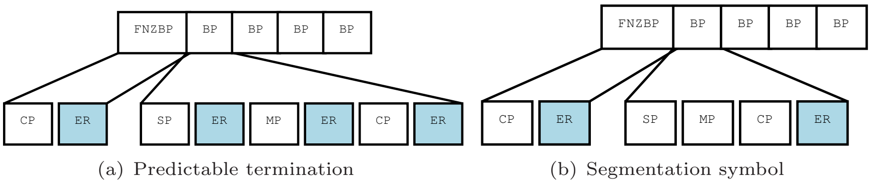
2.1 JPEG2000 Error Resilience Options

There are several options of strengthening robustness of JPEG2000 against transmission errors, e.g., the insertion of start of packet (SOP) and end of packet header (EPH) marker sequences, the resetting of the contexts after each coding pass, the insertion of a segmentation marker after each cleanup pass and the predictable termination of each coding pass. Only the segmentation symbol and predictable termination are capable of the detection of bitstream errors, i.e., of errors in the entropy coded coefficient data.

The coding of an additional segmentation symbol at the end of the cleanup pass protects the bitstream on a bitplane basis. Thereby the four bit sequence "1010" is coded in uniform context at the end of each cleanup pass (the last pass of each bitplane). If we assume that errors randomly generate a "1010" sequence at the end of a cleanup pass (approximately following a uniform distribution), the occurrence of an error is detected with a probability of $15/16 = 0.9375$. This strategy is very well-performing in terms of compression efficiency (only a very slight compression overhead is introduced, as shown in figure 6). However, it is only capable of detecting errors on a bitplane basis and hence undamaged coding passes may also be discarded.

The employment of predictable termination of each coding pass is an improvement in the following sense: Every erroneous coding pass can be separately identified and concealed. Any bit error is likely to result in an arithmetic decoder state that is not consistent with the predictable termination policy. A detailed description of the detection of termination inconsistencies can be found in [17]. About 3.5 bit of error resilience information are left on the spare least significant bits of a coding pass (according to the JJ2000 documentation and backed

up by own experiments). Thus every error in a coding pass is detected with a probability of $1 - 1/2^{3.5} \approx 0.91$. Both methods can be combined to improve error detection. Figures 2(a) and 2(b) illustrate these two error resilience options; "FNZBP" denotes the first non zero MSB bitplane, which is only coded with a cleanup pass ("CP"). "BP" denotes the consecutive bitplanes , "SP" the significance propagation pass, "MP" the magnitude refinement pass, and "ER" the error resilience information.
[17, p.509] remarks on the propagation of bitstream errors: "Since code-blocks are coded independently, errors may not propagate beyond the code-block whose bit-stream is corrupted." The remaining codeblock data after an error generally is useless. In [17] it is pointed out that this is not only the case for arithmetically coded data, but may also occur for raw codeword segments, as a single symbol error in the significance propagation pass may corrupt the state array, thus rendering the remainder of the bitstream unusable. Further dependencies are introduced by the wavelet transform, e.g., an error in the lowest resolution LL subband will propagate to several pixels in the spatial domain.



(a) Predictable termination

(b) Segmentation symbol

Fig. 2. JPEG2000 error resilience options.

2.2 JPEG2000 Error Concealment

Note that only the detection of an error is standardized, the actual error concealment of the corrupted parts is a decoder choice.
A decoder has several possibilities when an error is detected:

1. truncate the JPEG2000 file at the position where the error has occurred (stop decoding immediately after the error),
2. set the corrupted coefficients to zero (as done in [14]), or
3. reset the coefficients to the last value before the detection of the error.

For the third strategy and predictable termination of each coding pass, the coefficient values can be saved before the decoding of a coding pass and can be reset to that values if an error is detected (reset on a coding pass basis). If the segmentation symbol is employed, the coefficients have to be saved after each successfully decoded cleanup pass (reset on a bitplane basis). It is a good idea to set all coefficient bits to the value before the detection of an error, and the bit (in the bitplane in which the error was detected) to one. If we assume that for all the remaining bits (which have not been decoded) every value is equally probable, this solution minimizes the average distortion.

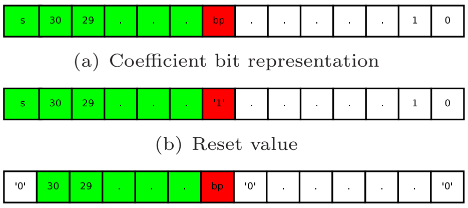
It is not certain which strategy performs best. In section 4.3 empirical results are presented.

3 Improving the JJ2000 Error Concealment Code

The JJ2000 decoder resets the coefficients on a bitplane basis, regardless of which error resilience options are enabled. We have modified the decoder in order to enable the reset on a coding pass basis.

Apart from that we noticed two bugs in the JJ2000 decoder that severely degrade the error concealment performance. The first one is rather subtle. A coefficient is only reset if non-zero bits have already been decoded. To test for the decoding of non-zero bits, a bitwise AND is applied to the coefficient and a resetmask. The resetmask is computed incorrectly, such that the bit of the erroneous bitplane is taken into account. This subtle difference is decisive, especially if the previously decoded bits are all zero, which is the case for the first non-zero bitplane of a codeblock. As wavelet coefficients tend to be distributed around zero, the majority of the coefficients will have a zero bit in the erroneous bitplane. Hence the probability that this coefficient (that is reset by JJ2000) actually has a one bit in this bitplane is very low. In the file StdEntropyDecoder.java line 2475 (4.1 unix release) it is therefore advisable to set: “resetmask = (-1)<<(bp+1);” instead of “resetmask = (-1)<<(bp);”. The JJ2000 comparison value is illustrated in figure 3(c); the corrected comparison value does not take the corrupted bit into account. A coefficient from an erroneous codeblock (an error has been detected in bitplane “bp”) is illustrated in figure 3(a), the value to which it is reset to is illustrated in figure 3(b).

The second bug occurs when the segmentation symbol and predictable termination are employed together. A correct termination of a coding pass overrides a previously detected error in the decoding of the segmentation symbol. Thus


s 30 29 . . . bp 1 0
s 30 29 . . . '1' 1 0
'0' 30 29 . . . bp '0' . . . . . '0'

(a) Coefficient bit representation

(b) Reset value

(c) JJ2000 comparison value

Fig. 3. Improvements for JJ2000.

employing both strategies leads to the same results as using only predictable termination of each coding pass. The bug can be corrected by changing the line 2439 in the file StdEntropyDecoder.java (4.1 unix release) from "error = mq.checkPredTerm();" to "error = error ‖ mq.checkPredTerm();".

As we will see in section 4 these modifications dramatically increases the performance of the error concealment. An improved version of JJ2000 can be found at `www.wavelab.at/sources`.

4 Experimental Results

First we will present visual examples that reveal that visual information is preserved for selective JPEG2000 encryption. Then the influence on the compression performance of JPEG2000 is evaluated in order to show that the error resilience options are applicable. In section 4.3 error resilience options and concealment strategies are evaluated in a realistic scenario.

We assume that all headers (including packet headers) are well protected. The packet headers can be moved to the main header with the packed packet headers option, which may be treated with special care.

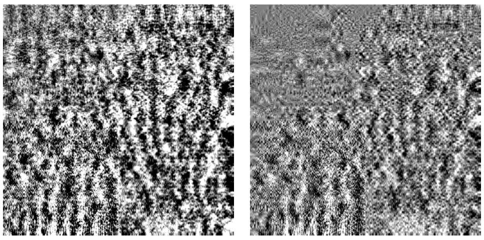
If not stated otherwise, JJ2000's default compression parameters have been employed, which include layer progression and 32 quality layers. The test sets have been derived from the freely available VQEG (video quality experts group) HDTV test set.

4.1 Visual Examples

Figures 4(a) and 4(b) illustrate that no concealment (decoding as if no error had been detected) and the JJ2000 concealment do not reveal any image information if the first 20% of the file (excluding headers) are encrypted or otherwise damaged. Additionally to the well-known PSNR (peak signal to noise ratio) the ESS (edge similarity score) as proposed in [19] is given in the figures. In the case of encryption one could assume that the image content is safely protected [2]. If the corrected concealment is applied, the image content (the Lena image) is clearly visible, as figure 5 reveals. Predictive termination and the segmentation symbol and error concealment on a coding pass basis have been applied. Decreasing the encryption percentage to 1% of the image data, as proposed in the technology examples of [3], will reveal even more visual information. From the encrypter's point of view, these results indicate that almost all of the JPEG2000 bitstream data has to be encrypted.

For partial encryption of the entire JPEG2000 codestream, i.e., including all headers, decoding the partially encrypted data may be hard, but the partial plaintext contains enough information to reconstruct the image obtained via the error concealment attack.

If the last 80% of the codestream (coded with 2bpp) are corrupted, the JJ2000 concealment, which achieves a PSNR of 23.77dB, performs better than no concealment (19.47dB), while the corrected error concealment increases the image



(a) No concealment: PSNR 8.4dB, ESS 0.23

(b) JJ2000 concealment: PSNR 9.7dB, ESS 0.23

Fig. 4. First 20% encrypted, 2bpp

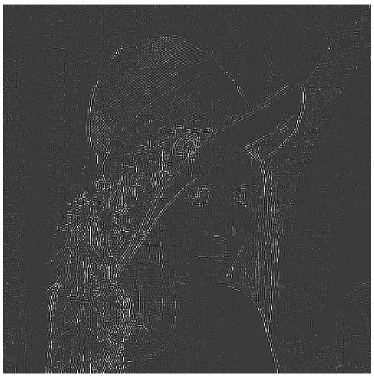


Fig. 5. First 20% encrypted, 2bpp, corrected concealment: PSNR 14.5dB, ESS 0.0

quality dramatically to a PSNR of 32.17dB. The corrected error concealment achieves 12.7dB more than no concealment and 8.4dB more than the default JJ2000 concealment, which is an enormous gain in image quality.

4.2 Compression Performance

The bitstream error resilience options in JPEG2000 are efficient in terms of compression performance (c.f. figure 6). These results were obtained by averaging a test set of 250 images with a resolution of 1024 times 576. Error resilience by means of the additional coding of the segmentation symbol (labeled "Seg avg." in figure 6) is most efficient in terms of compression performance, while predictable termination (labeled "Pterm avg.") is slightly more demanding at the cost of about 0.1dB for all bitrates.
Combining both methods (labeled "Combined avg.") adds the nearly negligible overhead of the coding of the segmentation symbol to the overhead of predictable termination.
In general, the bitstream error resilience options can be said to almost preserve JPEG2000's compression performance.

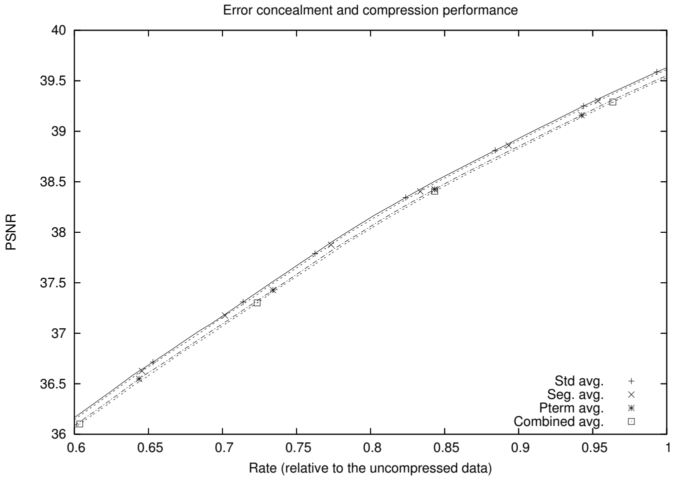


Fig. 6. Compression performance and error concealment strategies

4.3 Resilience Options and Concealment Strategies

The location where an error has occurred is the predominant influence on the visual quality of the decoded image. Hence we present an evaluation where each combination of error resilience options and error concealment strategy is evaluated for an error in a certain location in the file.

The analysis on the basis of network error simulations with a bit error rate in the range of 10^{-2} to 10^{-4} [14, 15, 20] is too coarse grain to show the subtle differences between the error concealment strategies. Commonly, errors occur due to hardware damage of disks; for magnetic disks, sectors of 512 bytes are damaged. Selective encryption is similar to the occurrence of random errors. The results of figures 7 and 8 show the averaged results for a test set of 100 images with a resolution of 512 times 288 each compressed with JJ2000 default parameters and a bitrate of 2bpp. The error location is given in percentage of the codestream length. One damaged sector with 512 byte is assumed (which are 1.39% of the JPEG2000 file).

Figure 7 evaluates the different concealment strategies for both bitstream error resilience options enabled (segmentation symbol and predictable termination). The best results in terms of PSNR are obtained by resetting the coefficients to their last value (before the detection of an error) on a coding pass basis and by employing both predictable termination and the segmentation symbol (labeled "Prior value with pterm, seg (coding pass)"). Interestingly, the JJ2000 concealment strategy (labeled "JJ2000 concealment with pterm, seg"), though obviously inaccurate, performs better than the other strategies, namely the ignorance of errors (labeled "Ignorance of errors with pterm, seg"), the truncation before the error (labeled "Truncation at error with pterm, seg") and setting the corrupted coefficients to zero (labeled "Zero with pterm, seg"). Compared to previously presented results (see section 4.1), where improvements up to 8.4dB could be reported, these results are surprising. As only a smaller portion of the codestream is affected, fewer CCPs are corrupted (in [10] an average CCP length

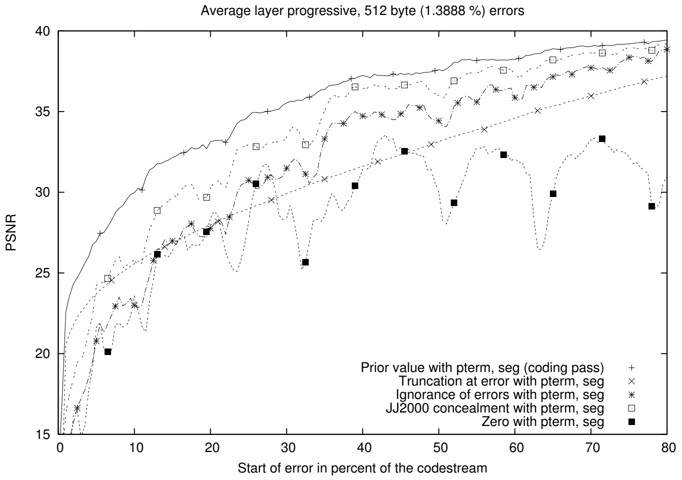


Fig. 7. Concealment strategies for combined bitstream resilience options

of 83 bytes is reported for JJ2000 default compression parameters and a test set of 1035 images). Hence, several codeblocks after the error will not be affected and contribute to the image quality (these are not taken into account if the codestream is truncated before the error). Another aspect is the probability of the corruption of the first contribution of a codeblock (the first contributions of codeblock are especially harmful for JJ2000 error concealment code), which decreases if the length of the corrupted segment is reduced, as well as with the position of the error. Furthermore, the affected codeblocks will likely not cover the same spatial area in different subbands (due to the order of the CCPs in the packets). Thus errors of different codeblocks will not accumulate in the wavelet transform.

The worst performance is achieved by resetting the corrupted coefficients to zero. With layer progression, less influential portions of a codeblock's compressed coefficient data are located at the end of the file. However, if an error occurs in these portions, the entire coefficients are set to zero.

In figure 8 error resilience options and concealment strategies are evaluated in more detail. Only errors in the first 35% of the codestream are examined, as errors in this part of the codestream introduce severe distortion. For predictable termination and the segmentation symbol enabled, resetting the coefficients on a coding pass basis is superior to the reset on a bitplane basis (labeled "Prior value with pterm, seg (bitplane)"). Employing the segmentation symbol and predictable termination separately leads to a slightly worse PSNR (labeled "Prior value with seg (bitplane)" and "Prior value with pterm (coding pass)"), but both perform better than the JJ2000 error concealment. It is notable that the image quality is significantly improved by working on a coding pass basis.

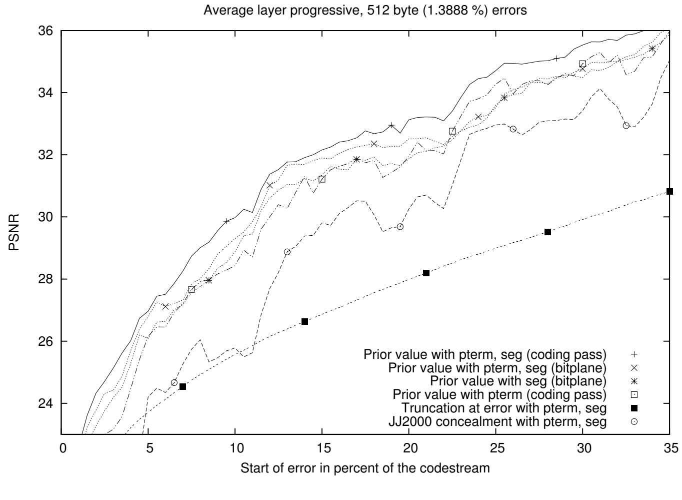


Fig. 8. Resilience options and concealment strategies

5 Conclusion

In this paper improvements for JPEG2000 reference software JJ2000 error concealment code have been presented, which increase the image quality dramatically (up to 8.4 dB in our evaluation). These improvements directly influence the applicability of selective JPEG2000 encryption for confidentiality: It can no longer be considered applicable. Empirical results for the influence on the compression performance of the bitstream error resilience options are presented. Additionally, different JPEG2000 resilience options and error concealment strategies have been evaluated. Our results show that the best results are achieved by resetting the coefficients on a coding pass basis.

References

1. Furht, B., Muharemagic, E., Socek, D.: Multimedia Encryption and Watermarking. Volume 28 of Multimedia Systems and Applications. Springer-Verlag, Berlin, Heidelberg, New York, Tokyo (2005)
2. Uhl, A., Pommer, A.: Image and Video Encryption. From Digital Rights Management to Secured Personal Communication. Volume 15 of Advances in Information Security. Springer-Verlag (2005)
3. ISO/IEC 15444-8: Information technology – JPEG2000 image coding system, Part 8: Secure JPEG2000 (April 2007)
4. Grosbois, R., Gerbelot, P., Ebrahimi, T.: Authentication and access control in the JPEG2000 compressed domain. In Tescher, A., ed.: Applications of Digital Image Processing XXIV. Volume 4472 of Proceedings of SPIE., San Diego, CA, USA (July 2001) 95–104
5. Kiya, H., Imaizumi, D., Watanabe, O.: Partial-scrambling of image encoded using JPEG2000 without generating marker codes. In: Proceedings of the IEEE International Conference on Image Processing (ICIP'03). Volume III., Barcelona, Spain (September 2003) 205–208
6. Wu, Y., Deng, R.H.: Compliant encryption of JPEG2000 codestreams. In: Proceedings of the IEEE International Conference on Image Processing (ICIP'04), Singapure, IEEE Signal Processing Society (October 2004)
7. Wu, H., Ma, D.: Efficient and secure encryption schemes for JPEG2000. In: Proceedings of the 2004 International Conference on Acoustics, Speech and Signal Processing (ICASSP 2004). (May 2004) 869–872
8. Zhu, B., Yang, Y., Li, S.: JPEG2000 syntax-compliant encryption preserving full scalability. In: Proceedings of the IEEE International Conference on Image Processing (ICIP'05). Volume 3. (September 2005)
9. Fang, J., Sun, J.: Compliant encryption scheme for JPEG2000 image code streams. Journal of Electronic Imaging **15**(4) (2006)
10. Stütz, T., Uhl, A.: On format-compliant iterative encryption of JPEG2000. In: Proceedings of the Eighth IEEE International Symposium on Multimedia (ISM'06), Los Alamitos, CA, USA, IEEE Computer Society (2006) 985–990
11. Engel, D., Stütz, T., Uhl, A.: Format-compliant JPEG2000 encryption in JPSEC: Security, applicability and the impact of compression parameters. EURASIP Journal on Information Security (Article ID 94565) (2007) doi:10.1155/2007/94565, 20 pages

12. Yang, Y., Zhu, B.B., Yang, Y., Li, S., Yu, N.: Efficient and syntax-compliant JPEG2000 encryption preserving original fine granularity of scalability. EURASIP Journal on Information Security (2007)
13. Said, A.: Measuring the strength of partial encryption schemes. In: Proceedings of the IEEE International Conference on Image Processing (ICIP'05). Volume 2. (September 2005)
14. Moccagatta, I., Soudagar, S., Liang, J., Chen, H.: Error resilient coding in JPEG-2000 and MPEG-4. IEEE Journals of Selected Areas in Communications **18**(6) (June 2000)
15. Dufaux, F., Ebrahimi, T.: Error-Resilient Video Coding Performance Analysis of Motion JPEG 2000 and MPEG-4. In: Proceedings of Visual Communications and Image Processing, VCIP'04. Motion analysis and image sequence processing, SPIE (2004)
16. ISO/IEC 15444-5: Information technology – JPEG2000 image coding system, Part 5: Reference software (November 2003)
17. Taubman, D., Marcellin, M.: JPEG2000 — Image Compression Fundamentals, Standards and Practice. Kluwer Academic Publishers (2002)
18. ISO/IEC 15444-1: Information technology – JPEG2000 image coding system, Part 1: Core coding system (December 2000)
19. Mao, Y., Wu, M.: Security evaluation for communication-friendly encryption of multimedia. In: Proceedings of the IEEE International Conference on Image Processing (ICIP'04), Singapore, IEEE Signal Processing Society (October 2004)
20. Dufaux, F., Baruffa, G., Frescura, F., Nicholson, D.: JPWL - an Extension of JPEG 2000 for Wireless Imaging. In: Proceedings of IEEE Int. Symp. on Circuits and Systems, ISCAS'06, IEEE (May 2006)