Selective Image Encryption Using JBIG

Roman Pfarrhofer[1] and Andreas Uhl[1,2]

[1] School of Telematics & Network Engineering,
Carinthia Tech Institute (CTI),
A-9020 Klagenfurt, Austria
[2] Department of Scientific Computing,
Salzburg University,
A-5020 Salzburg, Austria

Abstract. Selective encryption techniques of JBIG encoded visual data are discussed. We are able to show attack resistance against common image processing attacks and replacement attacks even in case of restricting the amount of encryption to 1% – 2% of the data. The low encryption effort required is due to the exploitation of the interdependencies among resolution layers in the JBIG hierarchical progressive coding mode.

1 Introduction

Encryption schemes for multimedia data need to be specifically designed to protect multimedia content and fulfil the security requirements for a particular multimedia application [9]. For example, real-time encryption of an entire video stream using classical ciphers requires heavy computation due to the large amounts of data involved, but many multimedia applications require security on a much lower level (e.g. TV news broadcasting [17]). In this context, several selective encryption schemes have been proposed recently which do not strive for maximum security, but trade off security for computational complexity.

Several reviews have been published on image and video encryption including selective (or partial) encryption methods providing a more or less complete overview of the techniques proposed so far [24]. Kunkelmann [12, 11] and Qiao and Nahrstedt [22] provide overviews, comparisons, and assessments of classical encryption schemes for visual data with emphasis on MPEG proposed up to 1998. Bhargava et al. [1] review four MPEG encryption algorithms published by the authors themselves in the period 1997 – 1999. More recent MPEG encryption surveys are provided by But [2] (where the suitability of available MPEG-1 ciphers for streaming video is assessed) and Lookabaugh et al. [15] (who focus on a cryptanalysis of MPEG-2 ciphers; in [14] the authors discuss MPEG-2 encryption as an example for selective encryption in consumer applications, the paper having broader scope though).

Of course, other data formats have been discussed with respect to selective encryption as well (Liu and Eskicioglu [16] give an overview with focus on shortcomings of current schemes and future issues): coding schemes based on wavelets [21], quadtrees [4, 13], iterated function systems (fractal coding) [23], and vector quantization [3] have been used to create selective encryption schemes.

J. Dittmann, S. Katzenbeisser, and A. Uhl (Eds.): CMS 2005, LNCS 3677, pp. 98–107, 2005.

In case a selective encryption process requires a multimedia bitstream to be parsed in order to identify the parts to be subjected to encryption, the problem of high processing overhead occurs in general. For example, in order to selectively protect DC and large AC coefficients of a JPEG image (as suggested by some authors), the file needs to be parsed for the EOB symbols 0x00 to identify the start of a new 8×8 pixels block (with two exceptions: if 0xFF is followed by 0x00, 0x00 is used as a stuffbit and has to be ignored and if AC63 (the last AC-Coefficient) not equals 0 there will be no 0x00 and the AC coefficients have to be counted). Under such circumstances, selective encryption will not help to reduce the processing demands of the entire application [20].

A possible solution to this problem is to use the visual data in the form of progressive, scalable, or embedded bitstreams. In such bitstreams the data is already organized in layers according to its visual importance due to the compression procedure and the bitstreams do not have to be parsed to identify the parts that should be protected by the encryption process. In previous work, several suggestions have been made to exploit the base and enhancement layer structure of the MPEG-2/4 scalable profiles [5, 7, 8, 12, 25] as well as to use embedded bitstreams like SPIHT [4] and JPEG 2000 [10, 18] to construct efficient selective encryption schemes.

In this work we propose a selective encryption scheme with extremely low encryption demand focussed onto losslessly encoded imagery which is based on the hierarchical progressive coding mode of JBIG. In order to be able to process grayscale images with this JBIG based approach, we use a bitplane representation which has been discussed before in the context of selective bitplane encryption [6, 19]. The JBIG based approach improves the latter techniques significantly. Section 2 reviews the basic functionalities of the JBIG format. Section 3 explains how to exploit the JBIG format properties for selective encryption and provides experimental results showing evidence of our schemes' effectiveness and ability to withstand attacks. Concluding remarks are given in section 4.

2 JBIG Basics

Joint **B**inary **I**mage Experts **G**roup is an ITU standard (ITU recommendation T.82) finalized in 1993 for compressing binary images and was meant to improve the fax compression standards of that time especially with respect to the coding of halftoned images.

JBIGs core coding engine is a binary context-based adaptive arithmetic coder similar to the IBM Q-coder. In this section we will mainly focus on the hierarchical progressive coding mode of JBIG since the understanding of the associated techniques is crucial for the selective encryption technique described subsequently. As a first step a binary multiresultion hierarchy is being constructed as shown in Fig. 1.

Simple downsampling by two violates the Nyquist sampling theorem and leads to severe artifacts especially for typed documents and halftoned images. Therefore, a linear recursive IIR filter employing a 3×3 window in the higher re-

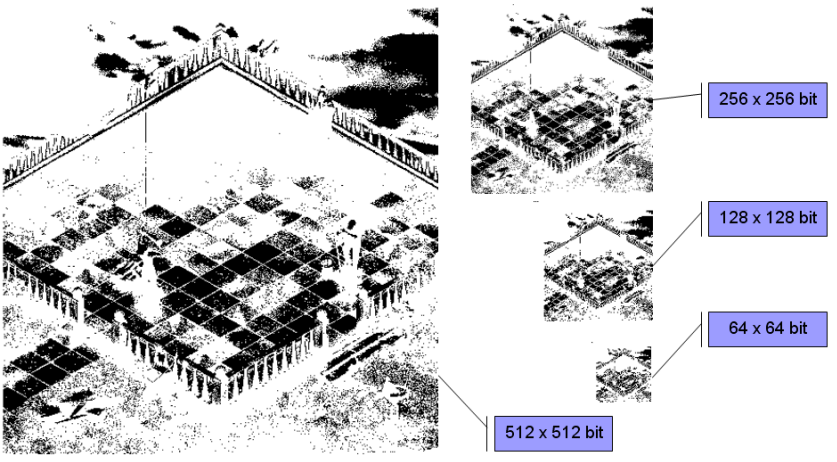


Fig. 1. Resolution layers of JBIGs hierarchical progressive mode

sulution level and 3 neighbouring samples from the already filtered low resolution image is used to create the low-pass filtered versions of the binary image.

When feeding these binary images into the arithmetic coder, for all resolution layers except the lowest one the context used within the coder consists of 6 neighbouring pixels of the currently encoded resolution layer and employs as well 4 neighbouring pixels of the already encoded layer with lower resolution to exploit the correlations among the resolution layers. This leads to significantly lower entropy values for the pixels to be coded in the higher resultion layers. Additionally, two strategies bypass the arithmetic coder if pixel values may be determined without encoding the actual values:

- Deterministic prediction (DP): based on knowledge about neighbouring pixel values of the current resolution layer, neighbouring pixel values of the layer with lower resolution, and the rule how the multiresolution hierarchy has been built, some pixel values are known without explicitely encoding them, the values may be derived from the other data.
- Typical prediction (TP): in the lowest resolution layer this means that identical lines are coded only once. A following identical line is labelled as being "typical" by setting a corresponding flag and the content is not fed into the coder. In the remaining layers, for a "typical" pixel being surrounded by pixels of the same colour follows that the corresponding four pixels in the next higher resolution layer have the same colour. A line is labelled as "typical" if it entirely consists of typical pixels and a corresponding flag is being set. Based on this technique, large homogeneous regions may be reconstructed without actually decoding a single pixel.

Note that by using cross-layer contexts, DP, and TP a high amount of dependency among resolution layers is used for encoding the data. As a consequence,

if parts of the data are lost for some reason, the errors caused by the missing data are propagated into the other resolution layers originally not affected by data loss.

In addition to the hierarchical layer structure, JBIG supports to partition the input image and all lower resolution layers into equally sized horizontal stripes. Accordingly, the entities encoded independently into the bitstream are denoted "stripe data entities" (SDE) which may be ordered in different manners. This has to be synchronized between encoder and decoder of course.

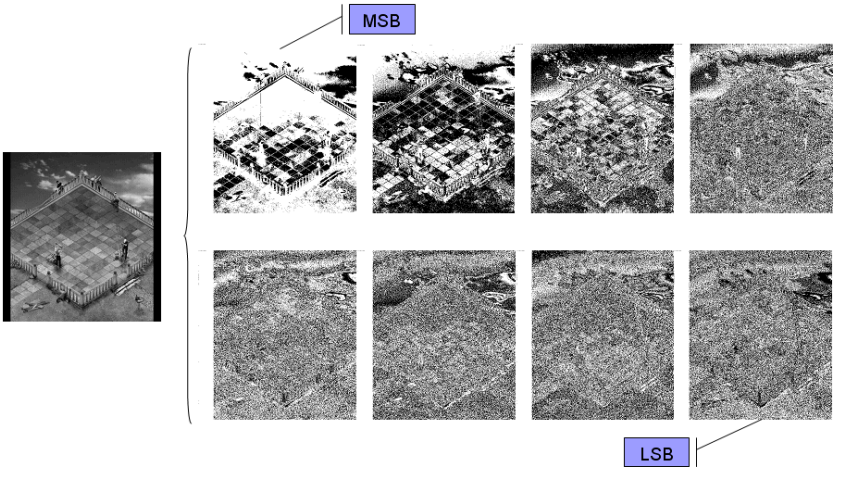


Fig. 2. Splitting an 8bpp image into its 8 bitplanes

In order to be able to compress grayscale images with JBIG, the grayscale images are split into a bitplane representation (e.g. 8 bitplanes for a 8bpp grayscale image as shown in Fig. 2), subsequently the bitplanes are JBIG compressed independently.

3 Selective Encryption Using JBIG

In previous work we have used the bitplane representation as described in the last section for selective encryption [19] – after splitting a grayscale image into its bitplanes, only a fraction of these planes (starting with the MSB) can be encrypted. It turns out that this approach is vulnerable by replacement and reconstruction attacks and therefore a secure setting requires up to 50% of the data to be encrypted. This approach is shown in the upper half of Fig. 3 (note that the processing of 4 bitplanes requires only the encryption of 35% of the JBIG encoded image in this case since planes close to the MSB can be compressed more efficiently of course).

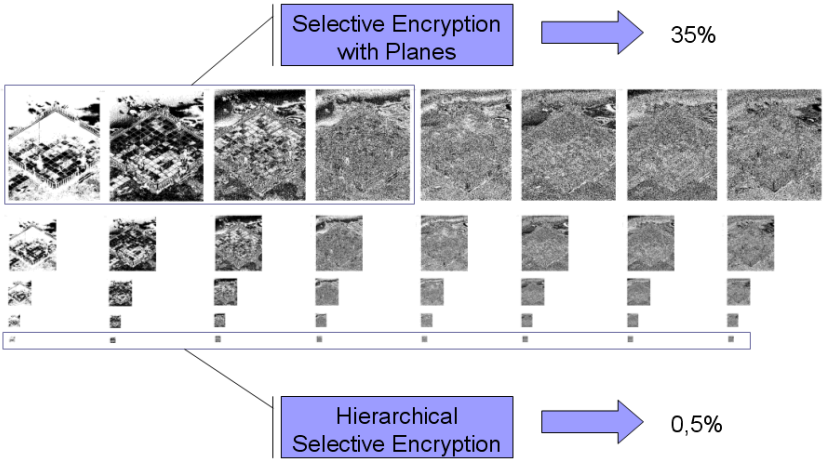


Fig. 3. Selective bitplane encryption vs. JBIG based encryption

When using the JBIG hierarchy for selective encryption only the lowest resolution of 5 layers may be encrypted, in this case for all bitplanes. This results in encrypting 0.5% of the original data only. These two principles may be mixed additionally: it is possible to limit encryption to a subset of reslution layers of a selected set of bitplanes only. In the following subsections, we will evaluate this idea and we will assess the robustness of this scheme against attacks.

We use the C JBIG implementation of M. Kuhn available via *anonymous ftp* from `ftp.uni-erlangen.de` in the directory `pub/doc/ISO/JBIG/`. This software has been extended to support encryption of arbitrary SDEs, for encryption we use the C++ AES implementation of B. Gladman[1] in CFB mode to avoid data padding for block completion. Our software avoids unwanted marker emulation by simply skipping parts of the encryption keystream in that case. For the subsequent experiments, we use 8bpp 512×512 grayscale images (see Fig. 4) and set the lowest resolution in JBIG to 32×32 pixels.

3.1 Reduction of Encryption Effort

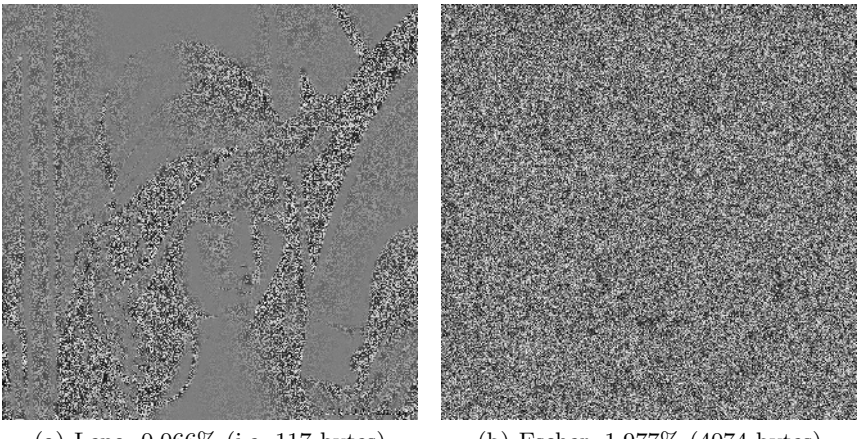
The most extreme case in our setting is to encrypt the lowest resolution layer of the MSB only. This corresponds to encrypting 0.056% and 0.066% of the JBIG encoded Escher and Lena images, respectively. Fig. 5(a) shows the directly reconstructed Lena image where a significant amount of high frequency information is still visible (see Fig. 7 left for the Escher image case). Additionally, we know from analysis in [19] that encrypting MSB data only is highly insecure against attacks.

We know furthermore from previous results that restricting the encryption operation to a low number of bitplanes does not lead to satisfying results with

[1] http://fp.gladman.plus.com/AES/index.htm

(a) Lena (b) Escher painting

Fig. 4. Test images



(a) Lena, 0.066% (i.e. 117 bytes) (b) Escher, 1.977% (4074 bytes)

Fig. 5. Encrypting different amounts of data

respect to securtiy. Therefore, we slightly increase the amount of data subject to encryption by protecting the lowest resolution layer of 4 bitplanes, starting from the MSB. This results in encrypting 0.265% of the JBIG encoded Escher image (see Fig. 8 left for a visual impression of the directly reconstructed data where no structures related to the image are visible any more). As we shall see later, this setting is already almost satisfactory from the security standpoint.

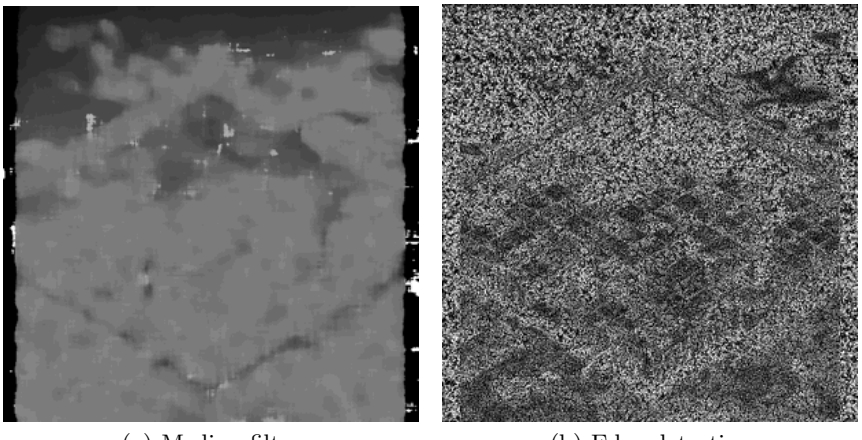
Finally, we look at the most secure setting considered in this context where we encrypt the two lowest resolution layers of all bitplanes. This still limits the amount of encrypted data to 1.977% and 2.292% for the Escher and Lena images, respectively. We show an example of a directly reconstructed Escher image in Fig. 5(b).

3.2 Attack Resistance

For testing attack resistance, we apply the following operations to the selectively encrypted images:

- Median filtering
- Edge detection (for the latter two attacks, we use the corresponding default Paint Shop Pro© algorithms)
- Replacement attack: the encrypted data used in the reconstruction process introduces a noise like pattern into the image. Therefore, we replace the encrypted data by constant zero data. We compensate for the change in average luminance as described in [19].

We first investigate the most extreme setting where only the lowest layer of the MSB bitplane is encrypted (compare Fig. 5(a) for the Lena case and Fig. 7 left for Escher). Neither median filtering nor edge detection do reveal the content of the image to a satisfying extent (see Fig. 6).



(a) Median filter (b) Edge detection

Fig. 6. Attack results: Escher image, 0.056% encrypted

However, the replacement attack shows to be effective in this setting (based on the results in [19], this is not surprising of course) which means that this parameter choice is not secure enough – Fig. 7 clearly shows the main structures of the original image.

When increasing the amount of encryption to 0.265% (by encrypting the lowest resolution layer of 4 bitplanes), we realize that now not even the replacement attack is able to deliver results that give any detailed information about the encrypted image (see Fig. 8).

As a consequence, the scenario when encrypting the lowest two resolution layers of all bitplanes (as shown in Fig. 5(b)) can be considered secure in any case.

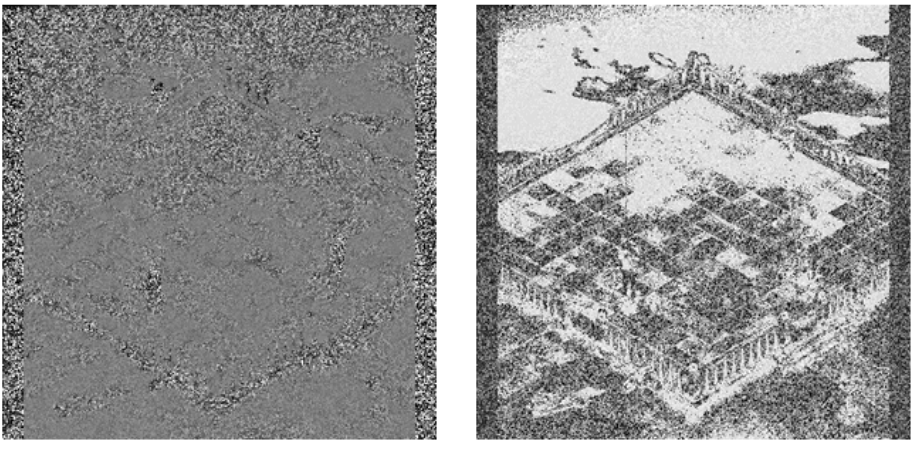


Fig. 7. Escher image (0.056% encrypted), direct reconstruction & replacement attack

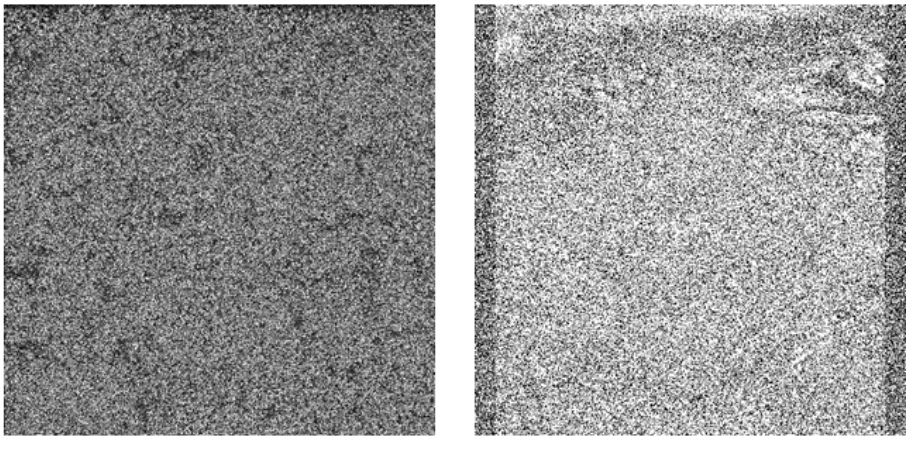


Fig. 8. Escher image (0.265% encrypted), direct reconstruction & replacement attack

4 Conclusion

We have discussed selective encryption of JBIG encoded visual data exploiting the interdependencies among resolution layers in the JBIG hierarchical progressive coding mode. Contrasting to earlier ideas when selectively encrypting a subset of bitplanes, we are able to show attack resistance even in case of restricting the amount of encryption to 1% – 2% of the data only. The extremely low amount of data required to be protected in our technique also allows the use of public-key cryptography thereby simplifying key management issues.

Acknowledgements

Most of this work has been done at CTI in the context of a system security lab in summer term 2003. Partial support by the Austrian Science Fund, project no. 15170, is acknowledged.

References

[1] B. Bhargava, C. Shi, and Y. Wang. MPEG video encryption algorithms. *Multimedia Tools and Applications*, 24(1):57–79, 2004.

[2] Jason But. Limitations of existing MPEG-1 ciphers for streaming video. Technical Report CAIA 040429A, Swinburne University, Australia, April 2004.

[3] T. S. Chen, C. C. Chang, and M. S. Hwang. Virtual image cryptosystem based upon vector quantization. *IEEE Transactions on Image Processing*, 7(10):1485–1488, October 1998.

[4] H. Cheng and X. Li. Partial encryption of compressed images and videos. *IEEE Transactions on Signal Processing*, 48(8):2439–2451, 2000.

[5] Jana Dittmann and Ralf Steinmetz. Enabling technology for the trading of MPEG-encoded video. In *Information Security and Privacy: Second Australasian Conference, ACISP '97*, volume 1270, pages 314–324, July 1997.

[6] Marc Van Droogenbroeck and Raphaël 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, September 2002.

[7] Ahmet Eskicioglu and Edward J. Delp. An integrated approach to encrypting scalable video. In *Proceedings of the IEEE International Conference on Multimedia and Expo, ICME '02*, Laussanne, Switzerland, August 2002.

[8] Mark M. Fisch, Herbert Stögner, and Andreas Uhl. Layered encryption techniques for DCT-coded visual data. In *Proceedings (CD-ROM) of the European Signal Processing Conference, EUSIPCO '04*, Vienna, Austria, September 2004. paper cr1361.

[9] B. Furht and D. Kirovski, editors. *Multimedia Security Handbook*. CRC Press, Boca Raton, Florida, 2005.

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

[11] T. Kunkelmann. *Sicherheit für Videodaten*. Vieweg Verlag, 1998.

[12] Thomas Kunkelmann. Applying encryption to video communication. In *Proceedings of the Multimedia and Security Workshop at ACM Multimedia '98*, pages 41–47, Bristol, England, September 1998.

[13] X. Li, J. Knipe, and H. Cheng. Image compression and encryption using tree structure. *Pattern Recognition Letters*, 18:1253–1259, 1997.

[14] T. D. Lookabaugh and D. C. Sicker. Selective encryption for consumer applications. *IEEE Communications Magazine*, 42(5):124–129, 2004.

[15] T. D. Lookabaugh, D. C. Sicker, D. M. Keaton, W. Y. Guo, and I. Vedula. Security analysis of selectiveley encrypted MPEG-2 streams. In *Multimedia Systems and Applications VI*, volume 5241 of *Proceedings of SPIE*, pages 10–21, September 2003.

[16] Xiliang Lu and Ahmet M. Eskicioglu. Selective encryption of multimedia content in distribution networks: Challenges and new directions. In *Proceedings of the IASTED International Conference on on Communications, Internet and Information Technology (CIIT 2003)*, Scottsdale, AZ, USA, November 2003.

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

[18] Roland Norcen and Andreas 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, October 2003. Springer-Verlag.

[19] M. Podesser, H.-P. Schmidt, and A. Uhl. Selective bitplane encryption for secure transmission of image data in mobile environments. In *CD-ROM Proceedings of the 5th IEEE Nordic Signal Processing Symposium (NORSIG 2002)*, Tromso-Trondheim, Norway, October 2002. IEEE Norway Section. file cr1037.pdf.

[20] A. Pommer and A. Uhl. Application scenarios for selective encryption of visual data. In J. Dittmann, J. Fridrich, and P. Wohlmacher, editors, *Multimedia and Security Workshop, ACM Multimedia*, pages 71–74, Juan-les-Pins, France, December 2002.

[21] 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.

[22] Lintian Qiao and Klara Nahrstedt. Comparison of MPEG encryption algorithms. *International Journal on Computers and Graphics (Special Issue on Data Security in Image Communication and Networks)*, 22(3):437–444, 1998.

[23] Stephane Roche, Jean-Luc Dugelay, and R. Molva. Multi-resolution access control algorithm based on fractal coding. In *Proceedings of the IEEE International Conference on Image Processing (ICIP'96)*, pages 235–238, Lausanne, Switzerland, September 1996. IEEE Signal Processing Society.

[24] 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.

[25] C. Yuan, B. B. Zhu, Y. Wang, S. Li, and Y. Zhong. Efficient and fully scalable encryption for MPEG-4 FGS. In *IEEE International Symposium on Circuits and Systems (ISCAS'03)*, Bangkok, Thailand, May 2003.