LIGHTWEIGHT JPEG 2000 CONFIDENTIALITY FOR MOBILE ENVIRONMENTS

Thomas Köckerbauer\textsuperscript{1}, Michael Kumar\textsuperscript{1}, and Andreas Uhl\textsuperscript{1,2}

\textsuperscript{1}Institut für Praktische Informatik, Gruppe Software, Johannes Kepler University Linz
Altenbergerstr. 69, A-4040 Linz, AUSTRIA
e-mail: koe@aon.at, m.kumar@gmx.at
\textsuperscript{2}Department of Scientific Computing, Salzburg University
Jakob-Haringerstr.2, A-5020 Salzburg, AUSTRIA
e-mail: uhl@cosy.sbg.ac.at

ABSTRACT

A lightweight JPEG 2000 encryption scheme for mobile environments based on wavelet filter parametrization is discussed. Being a special variant of header encryption, the technique has an extremely low computational demand. Compression quality and security assessment show that the scheme may be employed in applications requiring a low to medium security level, provided the conditions for a secure use discussed in this work are obeyed.

1. INTRODUCTION

Encryption schemes for multimedia data need to be specifically designed to protect multimedia content and fulfill the security requirements for a particular multimedia application. 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 [1]). 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. For example, we mention selective encryption of MPEG streams [2] and of wavelet encoded data [3].

In this work, we focus onto encryption schemes for mobile environments which have to be extremely low-cost in terms of computational demand due to the limitations of the involved hardware devices (i.e. low power resources, low computing capabilities). We propose a lightweight JPEG 2000 encryption scheme based on wavelet filter parametrization for applications requiring a low to medium security level. In Section 2, we shortly review important JPEG 2000 features and a wavelet filter parametrization scheme. Section 3 introduces the encryption scheme and evaluates the resulting compression quality and security.

2. WAVELET COMPRESSION FUNDAMENTALS

2.1. JPEG 2000

The JPEG 2000 image coding standard [4] is based on a scheme known as EBCOT (“embedded block coding with optimized truncation”). The major difference between previously proposed wavelet-based image compression algorithms such as EZW or SPIHT (see [5]) is that, after performing a global wavelet transform, EBCOT as well as JPEG 2000 operate on independent, non-overlapping blocks of transform coefficients which are coded in several bit layers to create an embedded, scalable bitstream.

Whereas in JPEG 2000 Part I a fixed set of wavelet filters is defined, JPEG 2000 Part II allows the employment of user-defined filters which are signalled in specific fields of the bitstream. The background is to allow custom designed filters for special applications. We will exploit this freedom in filter choice for our lightweight encryption scheme.

2.2. Wavelet Filter Parametrization

For the construction of compactly supported orthonormal wavelets, solutions for the dilation equation have to be derived, satisfying two conditions on the coefficients $c_k (\phi(t) = \sum_{k \in \mathbb{Z}} c_k \phi(2t - k)$, with $c_k \in \mathbb{R}$). In our work we use parameterised filters generated according to an algorithm proposed by Scheid and Pittner [6]:

Given $N$ parameter values $-\pi \leq \alpha_i < \pi$, $0 \leq i < N$, the following recursion

$$c_0^0 = \frac{1}{\sqrt{2}} \quad \text{and} \quad c_1^1 = \frac{1}{\sqrt{2}}$$

$$c_k^0 = \frac{1}{2} \left( (c_{k-2}^0 + c_{k-2}^1) \cdot (1 + \cos \alpha_{n-1}) + (c_{2(n+1)-k}^1 - c_{2(n+1)+k}^1)(-1)^k \sin \alpha_{n-1} \right)$$

can be used to determine the filter coefficients $c_k^N$, $0 \leq k < 2N + 2$. We set $c_k = 0$ for $k < 0$ and $k \geq 2N + 2$.

Example filters which can be generated using this formula
are the Daubechies-6 filter, which can be constructed using the parameters \((0.6830127,-0.1830127)\), or the Haar filter which is generated with the parameter 0.

Note that similar parametrizations are available for bi-orthogonal filterbanks [7] and for the lifting scheme in the context of JPEG 2000 [8].

### 3. LIGHTWEIGHT ENCRYPTION FOR JPEG 2000

Selective encryption has been already discussed in the context of JPEG 2000. Among others, Norcen et al. [9] report that encrypting the first 15 - 20\% of the packet data is even resistant against an error-concealment attack. However, in case that one or more parties which are involved in an application have strong limits on their processing capacities (in our case, a mobile device with a small battery and a slow processor), even encrypting a small fraction of the image data may still be out of reach. In such environments, confidentiality may be provided by even more extreme selective encryption as follows.

Wavelet-based compression can be potentially performed using a wide variety of different wavelet transforms. This degree of freedom may be exploited to add security to wavelet-based applications by only encrypting the header information defining the wavelet transform in use and keeping the rest in plaintext. Following this general idea, selective encryption schemes based on encrypting the secret wavelet packet subband structure [3] or NSMRA decomposition scheme [10] have been proposed recently.

In this paper we investigate the properties of a header encryption variant where we keep the parameter to generate the filters for the wavelet transform secret. This can be easily achieved in the context of JPEG 2000 Part II by simply encrypting the corresponding field containing the custom filters in the header using a cryptographically strong cipher. As a consequence, the amount of data subject to encryption is minimal, since no actual image data but only filter coefficients are protected.

#### 3.1. Compression Quality

Whereas the traditional filters used for wavelet compression are tuned for optimal concentration of the energy contained in the image and the separation of high- and low-frequency parts, parameterised filters provide a wide quality range. The advantage as well as the disadvantage of parameterised filters is their variety, not all filters within such a family are equally suited for a specific purpose, in this case, image compression. Fig. 1 shows the resulting quality (PSNR in dB) when compressing the 8 bpp \(512 \times 512\) pixels Lena image using different parameter values with compression ratios 10 and 20, respectively.

It is clearly displayed that the compression quality of the filters resulting from the parametrization algorithm described in section 2.2 varies in the interval \([29.5dB, 35dB]\) for ratio 10 and \([25dB, 30dB]\) for ratio 20, respectively. Among other variations, obviously the left half of the parameter range leads to poor filter quality. As a consequence of these findings, a strategy is required to limit the possible compression quality loss introduced by randomly chosen parameters. The most desirable approach would be a heuristic which – given either the parameters to generate the filters or the actual filter coefficients themselves – could determine an approximation of the compression quality to be expected in advance (i.e. without performing the compression). A heuristic of this type would allow a parameter generation and evaluation on the fly, i.e. during the compression stage without significant increase of computational demand. Besides restricting the parameter to positive values no such heuristic could be found.

To avoid low-quality filters, two other approaches might be possibly used:

- Generate the parameters and the corresponding filter coefficients and perform the compression stage. The parameter is used only in case the quality turns out to be sufficient. As this technique is time consuming, it contradicts our goals we want to achieve with the entire system. Only one failure in parameter choice (i.e. one bad quality filter) makes the scheme significantly more expensive than full AES encryption of a JPEG 2000 Part I bitstream.

- Determine parameter values of good quality in advance and restrict the admissible parameters to regions close to that values. Fortunately, the quality of parameters is very much image independent, which makes this approach a feasible and efficient one. However, the decrease of the amount of admissible parameter values is known in advance (also to a potential at-
tacker) and needs to be considered. This fact reduces the overall security of the system since it corresponds to a smaller keyspace.

### 3.2. Security

The restriction in terms of filter quality values reduces the amount of admissible parameter values as seen in the previous subsection to 20 – 50% of the entire range, depending on the quality requirements of the target application. At first sight, there seem to be enough parameter values left since the data type of the parameters for this kind of filter is $\mathbb{R}$ (in theory), in practice it is $\mathbb{Q}$. However, close parameters lead to similar filters which in turn lead to similar wavelet transform coefficients. Of course, this might be a threat to the security of the system since an attacker does not need to know the compression parameter exactly to get a “decrypted” image with sufficient quality. In Fig. 2 we illustrate this problem. The Lena image is compressed with filters generated by the parameter 1.05841, and subsequently decompressed with a large number of different filters derived from parameters covering the entire possible range. We plot the PSNR of the resulting images against the parameter used for decompression. The desired result would be an isolated single PSNR peak at the position of the “correct” parameter (that one used for compression) and low values everywhere else.

![Fig. 2. Attack against a 1-D parameter scheme, JPEG 2000 compression at ratios 1:10 and 1:20](image)

The result of this experiment is not an isolated PSNR peak but an entire region centered around the correct parameter where the PSNR values are decreasing with increasing distance from the correct value. For example, the parameter range $[0.75, 1.25]$ (which covers about 8% of the entire parameter range) provides image quality above 20 dB. Fig. 3.a visualizes an image decompressed with a parameter displaced from the correct one by a distance of $\approx 0.2$ in terms of parameter value. Obviously, the quality of this (attacked) image is too high to provide any kind of confidentiality.

As a consequence, the number of admissible parameter values needs to be restricted to a rather sparse grid. Taken this fact together with the beforementioned restrictions due to low quality filters (subsection 3.1) the keyspace is too small for a reasonable application in case of the 1-D parameter scheme. However, when taking these restrictions into account the quality of encrypted and attacked images is low enough for applications where the size of the keyspace is not an issue (see Fig. 3.b).

In order to increase the available keyspace parametrizations with more parameters (leading to longer filters) can be used. This increases the number of high quality filters significantly if the percentage of good filters remains approximately constant in the entire set of filters, which turns out to be true. To compare the 1-D parametrization to the 2-D case, the Lena image is compressed with the filters generated by the parameters -1.69159 and -1.84159, and subsequently decompressed with a large number of different filters derived from parameters covering the entire possible range. In Fig. 4 we again plot the PSNR of the resulting images against the parameter used for decompression.

![Fig. 4. Attack against a 2-D parameter scheme, JPEG 2000 compression at ratio 1:10](image)
The result shows that still a sparse grid needs to be applied to this much larger parameter space. In the 2-D parameter scheme we do not result in the single isolated PSNR peak as well but we still face an entire region where the quality of the encrypted and attacked images is too high. Therefore, the resulting number of admissible parameters still remains rather small in the 2-D case, but the strategy to move to higher dimensional parametrization schemes turns out to be fruitful in principle and leads to reasonable keyspace sizes at least for low security applications. Fig. 5 shows two encrypted and attacked images using the same 2 parameters for compression as given before. The result suggests that a sufficient degree of confidentiality may be achieved with the proposed scheme, provided the limitations as discussed before are addressed properly.

\[\text{Fig. 5. Quality of attacked images, JPEG 2000 compression at 0.4 bpp}\]

\[\text{(a) 9.86 dB, parameters 1.00841 and 1.60841} \]
\[\text{(b) 11.76 dB, parameters - 3.04159 and 0.70841}\]

4. CONCLUSIONS AND FUTURE WORK

We have introduced a lightweight encryption scheme for JPEG 2000 using wavelet filter parametrization which is suited for mobile environments due to its extremely low computational demand. It turns out, that provided the restrictions concerning the amount of admissible parameter values are obeyed, the scheme can provide enough confidentiality for applications requiring a low to medium level of security. In future work we will focus on the precise size of the available keyspace in higher dimensional parameter systems and on the parametrization techniques directly related to the lifting scheme [8].

Acknowledgements

This work has been performed while Andreas Uhl was a guest professor at Johannes Kepler University Linz in the framework of a mobile multimedia students project, and has been partially funded by the Austrian Science Fund, project no. 15170.

5. REFERENCES