Assessing JPEG2000 Encryption with Key-Dependent Wavelet Packets

In [39] the authors suggest to use secret Fourier-based transforms for the encryption of visual data. Other proposals in the area of lightweight encryption [40] propose the encryption of the filter choice used for a wavelet decomposition. However, this suggestion remains vague and is not supported by any experiments, while [22,26] propose encrypting the orthogonal filterbanks used for an non-stationary multi-resolution analysis (NSMRA) decomposition. The use of concealed biorthogonal parametrized wavelet filters for lightweight encryption is proposed by [38]. The use of key-dependent wavelet packet decompositions is proposed first by [24,25]. The latter work [25] evaluates encryption based on key-dependent subband structures in a zerotree-based wavelet codec. Parametrized wavelet filters have been employed for JPEG2000 lightweight encryption by [17,5], however, this approach was shown to be insecure in later work [3]. The scrambling of DCT (discrete cosine transform) and DWT (discrete wavelet transform) coefficients is proposed in [44]. Recently secret DCT-based transforms have been proposed for image and video encryption [43].

In the context of JPEG2000, the degrees of freedom in the wavelet transform are a prime candidate for constructing a secret transform domain. JPEG2000, Part 2, allows the definition of custom wavelet filters and user-defined isotropic and anisotropic wavelet packet subband structures [13]. Exemplary wavelet packets are shown in figure 1. Key-dependent wavelet packets in JPEG2000 have been proposed for a lightweight encryption scheme in earlier work [7, 6,8]. This approach is in the focus of interest in this work. The suggested scheme can be seen as a form of header encryption, as only the information pertaining to the transform domain needs to be encrypted, the rest of the data remains in plaintext. This approach has the advantage that only the parameters of the secret transform domain need to be kept secret. Therefore the demands for the encryption stage are minimal as compared to a more traditional, bitstream-oriented encryption approach [7]. Due to the shift in com-

Fig. 1 Exemplary wavelet packet decompositions and test image.