COMPARISON OF JPEG AND JPEG 2000 IN LOW-POWER CONFIDENTIAL IMAGE TRANSMISSION*

Mara Rhepp[1,+]*, Herbert Stögner*[1]*, and Andreas Uhl*[1,2]

[1]School of Telecommunications & Network Engineering, Carinthia Tech Institute
Primoschgasse 8, A-9020 Klagenfurt, AUSTRIA

[2]Department of Scientific Computing, Salzburg University
Jakob-Haringerstr.2, A-5020 Salzburg, AUSTRIA
e-mail: uhl@cosy.sbg.ac.at

ABSTRACT

We compare JPEG and JPEG 2000 in the context of confidential image tranmission. Considering differend encryption techniques (AES, tripleDES) and transmission media (modem, Bluetooth, WLAN, ethernet), we derive under which circumstances the better compression performance of JPEG 2000 or the higher execution speed of JPEG leads to an overall time-optimal configuration of the entire compression-encryption-transmission chain.

1. INTRODUCTION

Visual content is exchanged over networks for many different application areas, many of them requiring confidentiality for sensitive data. For example, we mention distributed medical image databases (with patient related medical image meterial) or surveillance applications.

In the context of applications involving visual data transmission, we may distinguish whether the image data is given as plain image data (e.g. after being captured by a digitizer or CCD array) or in form of a bitstream resulting from prior compression. In recent work [5, 8] we have denoted the first application scenario as "on-line" (e.g. video conferencing, surveillance applications) and the latter "off-line" (since the respective applications like video on demand or photo CD-ROM are purely retrieval based). Note that the involvement of lossy compression technology is usually mandatory in the on-line scenario due to bandwidth restrictions. Consequently, for an on-line imaging application requiring confidentiality during data transfer, the processing chain involves aquisition, compression, encryption, and transmission.

Images are a type of data which require a large processing capacity or transmission bandwidth. In case that one or more parties which are involved in an imaging application have strong limits on their processing capacities (e.g., a mobile device with a small battery and a slow processor) or their network link (e.g., a wireless channel), the application needs to be carefully optimized to guarantee minimal energy or bandwidth consumption.

Guaranteeing minimal bandwidth consumption is easy – the image data needs to be compressed to the smallest possible amount of data which often requires high computational effort. In this work we focus on minimal energy consumption in the sense of minimizing processing time. Energy minimization for wireless image transmission has been already discussed in the literature [1, 9]. In [4] it has been found that in the case of the availability of low tranmission power it is advantageous to use a less efficient source coder which consumes less power under certain circumstances. In recent work [3], we have discussed the case of confidential transmission of lossless image data and have found that the optimal employment of compression depends on the execution speed of the cryptographic cipher in use. In this work, we investigate computationally efficient schemes to provide confidentiality for the transmission of visual data in a lossy on-line scenario. In particular, we seek to optimize the interplay of the three main steps of such a scheme, i.e. lossy compression, encryption, and transmission in the sense of minimal computational effort and energy consumption. Based on exemplary experimental data, we model the costs of the three involved processing steps and subsequently derive cost optimal strategies for employment of confidential visual data transmission in the target environment. Specifically, we aim at answering the question whether JPEG or JPEG 2000 is the optimal lossy compression scheme for this application area.

Section 2 provides an introduction to principles of confidential transmission of visual data. In Section 3 we present the building blocks of our target environment and model the respective behaviour (in terms of rate-distortion performance and computational costs) based on experimental data. Several different configurations of confidential visual data transmission are analyzed in Section 4. In the conclusion we summarize the main results and give an outlook to further work in this direction.

2. PRINCIPLES OF CONFIDENTIAL TRANSMISSION OF VISUAL DATA

There are two ways to provide confidentiality to a transmission application. First, confidentiality is based on mechanisms provided by the underlying computational infrastructure. The advantage is complete transparency, i.e. the user or a specific application does not have to take care about confidentiality. The obvious disadvantage is that confidentiality is provided for all applications, no matter if required or not, and that it is not possible to exploit specific properties of certain applications. To give a concrete example, consider the distributed database infrastructure mentioned in the introduction. If the connections among the components are based on TCP/IP internet-connections (which are not confi-

[+]Mara Rhepp is an artificial name representing a group of students working on this project in the framework of the Multimedia I laboratory (winterterm 2003/2004): R. Angermann, G. Auner, W. Ehrreich, T. Habersatter, O. Moser, D. Petanjek, A. Pressien, R. Rauter, M. Reschreiter.

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

dential by themselves of course), confidentiality can be provided by creating a Virtual Private Network (VPN) using IPSec (which extends the IP protocol by adding confidentiality and integrity features). In this case, the entire visual data is encrypted for each transmission which puts a severe load on the encryption system. The second possibility is to provide confidentiality on the application layer. Here, only applications and services are secured which have a demand for confidentiality. The disadvantage is that each application needs to take care for confidentiality by its own, the advantage is that specific properties of certain applications may be exploited to create more efficient encryption schemes or that encryption is omitted if not required.

In order to provide reasonable execution performance for encrypting the large amounts of data associated with imaging applications, usually symmetric encryption is used in practical applications. The Advanced Encryption Standard AES [2] is a recent symmetric block cipher which is going to replace the Data Encryption Standard DES very soon in all applications where confidentiality is really the aim. AES operates on 128-bit blocks of data and uses 128, 196, or 256 bit keys. It is the natural candidate for encrypting image data. For more information including links to various source code see the official NIST AES-page[1]. Despite of its known security deficiencies and low execution speed, many applications still use tripleDES [7] which operates on 64-bit blocks of data and employs a 56 bit key in each of its three DES usages.

3. BASIC BUILDING BLOCKS: COMPRESSION, ENCRYPTION, AND TRANSMISSION

In any (storage or) transmission application, compression has always to be performed prior to encryption since the statistical properties of encrypted data prevent compression from being applied successfully. Moreover, the reduced amount of data after compression decreases the computational demand of the subsequent encryption stage and lossy compressed encrypted data cannot be decrypted any more. Therefore, the processing chain has a fixed order (compression – encryption – transmission). In the following subsections, we introduce the basic technology and model the costs in terms of rate-distortion performance and computational demand of the stages in the processing chain of the target environment.

3.1 Lossy Compression

JPEG and JPEG 2000 are the most common techniques to compress grayscale or color images in lossy manner nowadays. They have been already compared with respect to many different aspects [6]. In the context of our work the two interesting aspects are rate-distortion performance and computational demand. It is generally known that the rate-distortion performance of JPEG 2000 is significantly better, especially at low bitrates.

However, this improvement comes at an increased computational cost. The question in the context of our target application is as follows. Given a fixed target quality, does the lower amount of data as produced by JPEG 2000 (which causes the subsequent encryption and transmission stages to be executed with lower computational demand) justify the higher cost as compared to JPEG ? To answer this question, knowledge about the relation of computational costs

[1] http://csrc.nist.gov/encryption/aes/

Figure 1: Testimages used to evaluate the rate distortion performance.

(i.e. timing behaviour) of the three stages of the processing chain is the key issue.

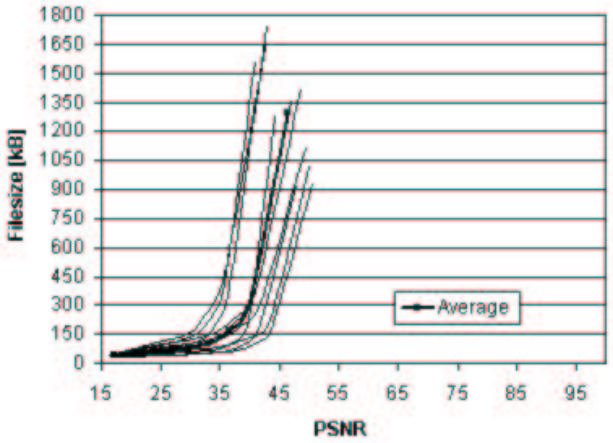


Figure 2: Rate-distortion performance of JPEG.

Fig. 1 shows the 1780×1308 pixels 24bpp color testimages used to rate the compression performance. We use the Jasper JPEG 2000 reference implementation and the IJG JPEG C implementations in order to compress the images to various bitrates. Figs. 2 and 3 plot PSNR versus filesize for all ten images and show also an average curve obtained by spline approximation.

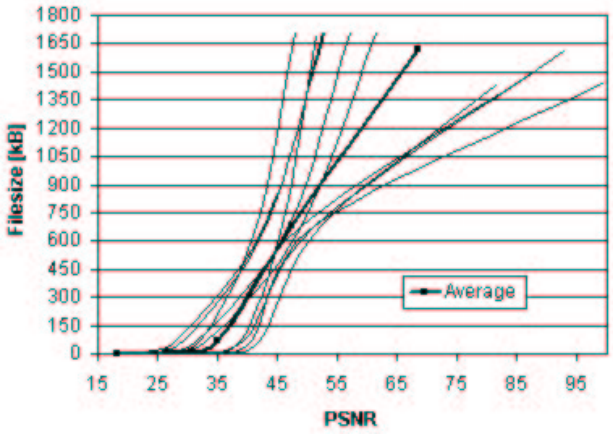


Figure 3: Rate-distortion performance of JPEG 2000.

The better rate distortion performance of JPEG 2000, especially at low bitrates, is clearly confirmed. But also the significant differences in execution speed are confirmed exerimentally. On average, Jasper requires 6.12 sec for compress-

ing an image whereas the IJG implementation suffices with 0.51 sec on an Intel Pentium III with 996MHz and 256MB SDRAM (this architecture is used for all subsequent measurements as well).

3.2 Encryption and Transmission

In order to model encryption behaviour, we use C++ implementations of AES[2] and tripleDES[3]. Fig. 4 plots the size of the data to be encrypted versus the time demand for doing this.

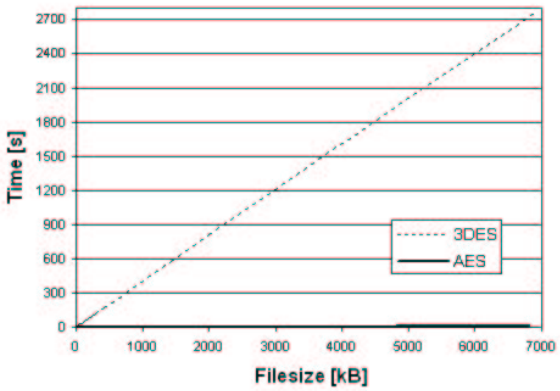


Figure 4: Time demand of encryption.

It is obvious that tripleDES is much slower as compared to AES. Whereas the amount of difference is partially due to the less efficient implementation of tripleDES, the trend is of course correct in general.

Finally, the transmission stage is modeled by five different transmission media: 56kBit modem, 1MBit Bluetooth, 10MBit ethernet, 11MBit IEEE802.11b WLAN, and 100MBit ethernet. We use a client-server application which transfers data to the client as soon as the connection has been set up. The client measures the time required to transmit the data after the connection is established.

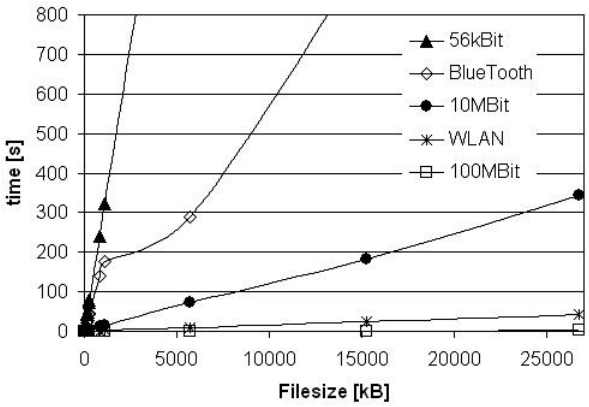


Figure 5: Time demand of transmission.

In Fig. 5 we plot the size of the data to be transmitted versus the time demand. It is clearly visible that the actual tranmission rates are much lower as predicted by the specification. However, the "theoretical" ranking among the different media is maintained in the experiments.

[2]http://fp.gladman.plus.com/AES/index.htm
[3]http://www.ntecs.de/old-hp/s-direktnet/crypt/de/index.html

4. COST OPTIMAL CONFIGURATION OF CONFIDENTIAL VISUAL DATA TRANSMISSION

The aim of this section is to combine the performance results given in the last section in order to finally answer the question under which "environmental conditions" JPEG or JPEG 2000 might be preferable. This is done as follows. Rate-distortion performance (for fixed sized input images) of JPEG and JPEG 2000 is modeled by two functions $data_i(quality)$, $i = 1,2$, which require PSNR in decibel (dB) as input and deliver data size in kiloByte (kB) as output (see Figs. 2 and 3). The input PSNR is the target quality of the transmitted images, $data_i(quality)$ output the resulting file size for JPEG and JPEG 2000, respectively. The average rate-distortion curves as depicted in the figures are used for $data_i(quality)$. Since the aim is to assess the time bahaviour of the entire system to identify the least energy consuming setting, we model the overall time function $time(data)$ (input is data size in kByte, output is time in seconds) as the sum of $comptime_i$ (time in seconds required for compression, constant since not dependent on the output bitrate of the codecs), $enctime_j(data)$, $j = 1,2$ (time required for encryption with AES or tripleDES, input is data size in kByte, output is time in seconds, see Fig. 4), and $transtime_k(data)$, $k = 1,\ldots,5$ (time required for transmission over one of the five media considered, input is data size in kByte, output is again time in seconds, see Fig. 5). Note that spline approximation to measurement data is used for encryption and transmission timings as well. Twenty different functions $time(data)$ are obtained by combining two compression techniques, two encryption modes, and five transmisison media.

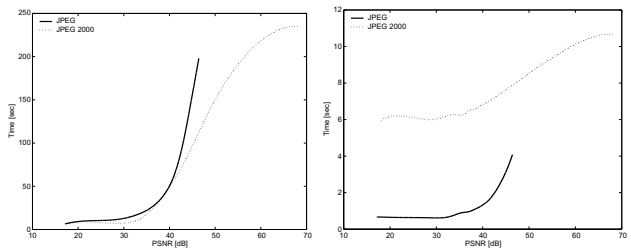
Finally we obtain functions which output the time demand of the entire processing chain upon input of the desired target quality ($time_l(quality)$) by inserting $data_i(quality)$ into $time(data)$:

$$time_l(quality) = comptime_i + enctime_j(data_i(quality)) + transtime_k(data_i(quality)) \text{ for } l = 1,\ldots,20$$

The spline approximations and the resulting twenty functions $time_m(quality)$ are all generated using MATLAB.

In the following, we always combine the two functions $time_l(quality)$ which correspond to employing JPEG and JPEG 2000 in the same environment (i.e. the same encryption and transmission techniques) into one plot in order to facilitate direct comparison. Fig. 6.a shows that in case of AES encryption and Bluetooth transmission the use of JPEG 2000 is faster as JPEG across the entire target quality range. Note that this is also true for all configurations using tripleDES as encryption technique and for all configuarations where modem is the transmission medium. In fact, all those plots (which are not shown) actually show the same shape which is very similar to the shape of the rate-distortion curves of JPEG and JPEG 2000. This result corresponds well to the intuitive expectations – if the time demand of encryption plus transmission is very high (as it is of course the case if tripleDES encryption or modem transmission is used), the lower time demand of JPEG as compared to JPEG 2000 is of no relevance for the overall timing behaviour. The final result only reflects the difference in the output bitrate as produced by

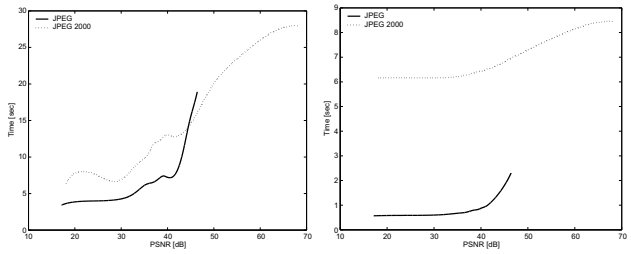
JPEG and JPEG 2000 and since the timings of encryption and transmission are almost linear in the amount of data, the output bitrate curves are simply linearly upshifted when the functions are combined.



(a) Bluetooth (b) WLAN

Figure 6: Wireless connections, AES encryption.

The second wireless link shows a very different bahviour (Fig. 6.b). In case of WLAN transmission the use of JPEG is faster as JPEG 2000 across the entire target quality range, and at least five times faster up to 40 dB. This is due to the much transmission rate of WLAN as compared to Bluetooth which makes transmission faster and consequently compression speed more and output bitrate less important. Although 10MBit ethernet should deleiver almost the same transmission rate as WLAN (11MBit), this is not confirmed experimentally (compare Fig. 5). The actual transmission rate is much lower which results as well in a different relation of employing JPEG or JPEG 2000 in the entire processing chain as compared to WLAN. Fig. 7.a shows that JPEG is faster as JPEG 2000 only up to 44 dB, below that value JPEG outperforms JPEG 2000 by a factor of 2 at most.



(a) 10MBit (b) 100MBit

Figure 7: Wired connections (ethernet), AES encryption

Finally, in the case of 100MBit ethernet, JPEG again outperforms JPEG 2000 across the entire quality range and is more than six times faster up to 40dB. The difference to WLAN is not as pronounced as it would be expected considering the specification of the two transmission modes. This due to the reduced importance of the contribution of transmission as compared to encryption in case the transmission rate is very high.

5. CONCLUSIONS AND FUTURE WORK

In the context of confidential transmission of lossy encoded image data we have found that only in case of very slow encryption (tripleDES) and/or slow transmission (modem & Bluetooth) JPEG 2000 outperforms JPEG in terms of overall time demand of the entire processing chain. Only in such environments the data rate reduction of JPEG 2000 as compared to JPEG is significant enough to compensate for the higher time demand of JPEG 2000 compression. It is interesting to note that already in case of AES encryption and WLAN transmission JPEG is significantly faster. In future work we will focus also on GSM and UMTS wireless transmission systems and we will generalize the results for variably sized images.

REFERENCES

[1] S. Appadwedula, M. Goel, N.R. Shanbhag, D.L. Jones, and K. Ramchandran. Total system energy minimization for wireless image transmission. *Journal of VLSI Signal Processing*, 27:99–117, 2001.

[2] J. Daemen and V. Rijmen. *The Design of Rijndael: AES — The Advanced Encryption Standard*. Springer Verlag, 2002.

[3] Bubi G. Flepp-Stars, Herbert Stögner, and Andreas Uhl. Confidential transmission of lossless visual data: Experimental modelling and optimization. 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 252 – 263, Turin, Italy, October 2003. Springer-Verlag.

[4] T. Lan and A. Tewfik. Adaptive low power multimedia wireless communications. In *Proceedings of the Conference on Information Sciences and Systems*, pages 377–382, 1997.

[5] 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.

[6] Diego Santa-Cruz and Touradj Ebrahimi. A study of JPEG 2000 still image coding versus other standards. In *Proceedings of the 10th European Signal Processing Conference, EUSIPCO '00*, Tampere, Finland, September 2000.

[7] B. Schneier. *Applied cryptography (2nd edition): protocols, algorithms and source code in C*. Wiley Publishers, 1996.

[8] Champskud J. Skrepth and Andreas Uhl. Selective encryption of visual data: Classification of application scenarios and comparison of techniques for lossless environments. In B. Jerman-Blazic and T. Klobucar, editors, *Advanced Communications and Multimedia Security, IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security, CMS '02*, pages 213 – 226, Portoroz, Slovenia, September 2002. Kluver Academic Publishing.

[9] L.T. Smit, G.J.M. Smit, and J.L. Hurink. Energy-efficient wireless communication for mobile multimedia terminals. In *Proceedings of the International Conference on Advances in Mobile Multimedia (MoMM2003)*, pages 115–124. Austrian Computer Society, 2003.