SELECTIVE BITPLANE ENCRYPTION FOR SECURE TRANSMISSION OF IMAGE DATA IN MOBILE ENVIRONMENTS

Martina Podesser, Hans-Peter Schmidt, and Andreas Uhl

School of Telematics & Network Engineering
Carinthia Tech Institute, Klagenfurt, AUSTRIA

ABSTRACT

We propose selective bitplane encryption to provide secure image transmission in low power mobile environments. Two types of ciphertext only attacks against this scheme are discussed and we use the corresponding results to derive conditions for a secure use of this technique.

1. INTRODUCTION

In the area of multimedia security, the terms "selective encryption" or "soft encryption" are sometimes used as opposed to classical "hard" encryption schemes like the Advanced Encryption Standard (AES [5]). Such schemes do not strive for maximum security and trade off security for computational complexity. They are designed to protect multimedia content and fulfil the security requirements for a particular multimedia application. For example, real-time encryption for an entire video stream using classical ciphers requires much computation time due to the large amounts of data involved, on the other hand many multimedia applications require security on a lower level (e.g. TV broadcasting [9]). Therefore, the search for fast encryption procedures specifically tailored to the target environment is mandatory for multimedia security applications. An overview about current requirements and implementations of contents protection systems for digital multimedia data is given in [6].

Selective or partial encryption (SE) of visual data is an example for such an approach. Here, application specific data structures are exploited to create more efficient encryption systems (see e.g. encryption of MPEG video streams [13]). Consequently, selective encryption only protects the visually most important parts of an image or video representation relying on a secure but slow "classical" cipher. See [16] for a discussion of sensible application scenarios for this approach. The first attempts in this direction have been made to secure DCT-based multimedia representations (see e.g. [1, 2, 8, 10, 13, 14, 15, 17, 22, 23]), wavelet based [7, 11, 12, 19, 23] and quadtree based representations [3, 4] have been considered also. Recently, selective video encryption schemes resistant to bit errors [18] and compliant to video formats [20] have been proposed for wireless environments.

In this work we propose and evaluate selective bitplane encryption for confidential transmission of image data in mobile environments. In section 2 we introduce the main ideas and discuss a possible application scenario. The security of the suggested approach is evaluated in section 3 by discussing the effectiveness of two ciphertext-only attacks against our scheme. In the conclusion we summarize the main results and give recommendations for a save use of the proposed technique.

2. SELECTIVE BITPLANE ENCRYPTION

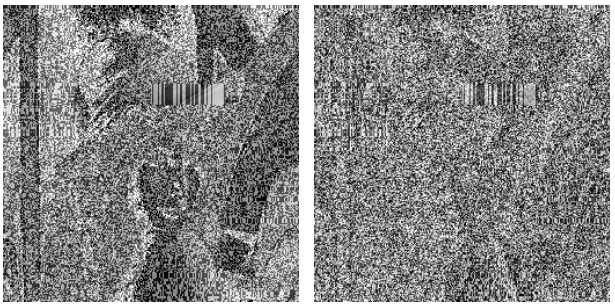
Intuitively, SE seems to be a good idea in any case since it is always desirable to reduce the computational demand involved in image processing applications. However, the security of such schemes is always lower as compared to full encryption. The only reason to accept this drawback are *significant* savings in terms of processing time or power. Therefore, the environment in which SE should be applied needs to be investigated thoroughly in order to decide whether its use is sensible or not.

Due to requirements of certain applications a loss of image quality may not be acceptable during transmission or storage (e.g., in medical applications because of reasons related to legal aspects and diagnosis accuracy [21]). Therefore, lossless compression schemes need to be employed for such applications. We assume a target environment, where due to the low processing power of the involved hardware not even lossless compression and decompression of visual data is reasonable or possible (e.g. mobile clients). Additionally, due to the increasing bandwidth available at mobile communication channels, compression seems not to be mandatory in any case, which is especially true for lossless applications. The reason is that the data reduction of lossless compression schemes is much lower as compared to lossy ones making the respective application less profitable. Note also that the time demand for compression is significantly higher as the time demand for encryption for almost all high quality codecs and symmetrical ciphers (which is mostly due to the efficient cache use of block-based encryption). For example,

Corresponding author, e-mail: uhl@cosy.sbg.ac.at

lossless compression with JPEG2000 takes a factor 100 (!) longer as compared to AES encryption (both executed in software). Therefore, it makes no sense to apply compression before encryption if the aim is to reduce computational demand (unless compression is executed in hardware and encryption in software). In applications where image data is acquired the plain image data may be accessed directly after being captured by a digitizer without being compressed. We assume the pictures to be captured by a hand-hold device with mounted digital camera and subsequently transmitted via a wireless channel. A concrete sample application for this scenario is teleradiology with mobile image capturing clients to enable fast and exact on-site diagnosis after an accident. Obviously, securing of patient related pictorial data is important.

For simplicity, we assume an 512×512 pixels image to be given in 8bit/pixel (bpp) precision. We consider the 8bpp data in the form of 8 bitplanes, each bitplane associated with a position in the binary representation of the pixels. The SE approach is to AES encrypt a subset of the bitplanes only, starting with the bitplane containing the most significant bit (MSB) of the pixels. Each possible subset of bitplanes may be chosen for SE, however, the minimal percentage of data to be encrypted is 12.5 % (when encrypting the MSB bitplane only), increasing in steps of 12.5 % for each additional bitplane encrypted. We use an AES implementation with blocksize 128 bit and a 128 bit key. The 128 bit block is filled with a quater of a bitplane line ($512/4 = 128$ bits). The encrypted bitplanes are transmitted together with the remaining bitplanes in plain text.

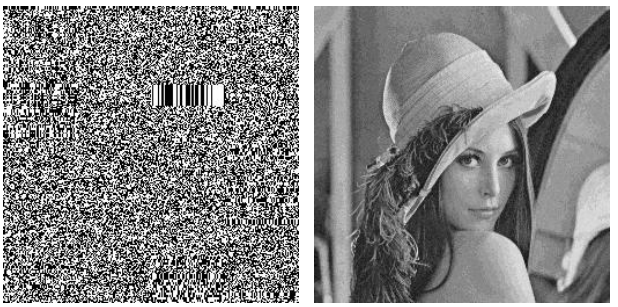


(a) 12.5% encrypted (b) 25% encrypted, 9.0dB

Figure 1: Visual examples for selective bitplane encryption, direct reconstruction.

Fig. 1 shows two examples of directly reconstructed images after selectively encrypting 1 and 2 bitplane(s). Whereas in the case of encrypting the MSB only structural information is still visible, encrypting two bitplanes leaves no useful information in the reconstruction, at least when directly reconstructing the image data.

Note the pattern reminiscent of a bar code in the upper right quater of the image. Fig. 2.a shows the encrypted MSB of the Lena image where this pattern is exhibited even clearer. This phenomenon due to the fact that AES encryption is used with identical key for all blocks in the image. Consequently, if there are identical plain text quater-lines directly situated above each other which also adhere to the AES block-border (i.e. starting at pixel positions 0, 128, 256, or 384), these data produce identical ciphertext blocks. Identical blocks of ciphertext are again arranged as identical quater-lines thereby generating the barcode effect. For the corresponding region with identical quater-lines starting at pixel position 128 in the MSB of the Lena image refer to Fig. 5.a.



(a) encrypted MSB (b) 50% encrypted, 31.8dB

Figure 2: Further visual examples for selective bitplane encryption.

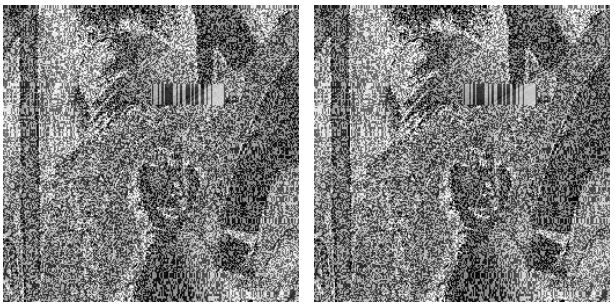
Note that it is of course important to encrypt the MSB first and continue with the bitplanes corresponding to the next bits in the binary representation. Fig. 2.b shows the case where the image is directly reconstructed after 4 bitplanes have been encrypted starting from the least significant bit (LSB). Almost no degradation is visible here – consequently it hardly makes any sense at all to encrypt these data. Table 1 gives the PSNR values of images subjected to the SE approach. Whereas the PSNR is constant 9 dB when encrypting the MSB first, PSNR decreases steadily from 51 dB to 14 dB for each additional bitplane encrypted and reaches 9 dB when encrypting all bitplanes after all in the case when the LSB bitplane is encrypted first.

# Bitplanes	1	2	3	4	5	6	7	8
First: LSB	51	44	38	32	26	20	14	9
First: MSB	9	9	9	9	9	9	9	9

Table 1: PSNR of images after direct reconstruction related to the number of encrypted bitplanes and to the ordering of the bitplanes.

A technique to eventually increase the security could be not to disclose which bitpanes have been subjected to

encryption besides the MSB. Fig. 3 shows directly reconstructed images where the MSB and n-th most significant bitplanes have been encrypted. Clearly, the visual quality is comparable to encrypting the MSB alone (compare Fig. 1.a).



(a) MSB + 4th (b) MSB + 5th

Figure 3: Visual examples for encryption of MSB and one additional bitplane.

Additionally, the statistical properties of bitplanes of natural images and encrypted bitplanes are fairly different. Table 2 compares the number of runs consisting of 5 identical bits contained in bitplanes (plaintext and ciphertext). All but the three less significant bitplanes show a much higher value of runs in the plaintext version. Therefore, the "secret" which bitplanes have been encrypted can be immediately solved using simple statistics.

Bitplane	MSB	2	3	4	5	6	7	LSB
Plain	45	39	32	20	11	5	4	4
Encrypted	4	4	4	4	4	4	4	4

Table 2: Number of runs consisting of 5 identical bits (rounded to thousand, Lena image).

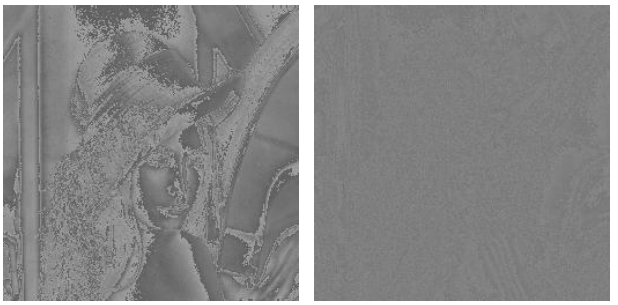
As a consequence, the most secure way to perform selective bitplane encryption is to encrypt the MSB bitplane and subsequently additional bitplanes in the order of decreasing significance with respect to their position in the binary representation.

3. EVALUATION OF SELECTIVE BITPLANE ENCRYPTION

The aim of this section is to assess the security of selective bitplane encryption by conducting two types of simple ciphertext-only attacks. A shortcoming of many SE investigations is the lack of quantifying the quality of the visual data that can be obtained by attacks against SE. Mostly visual examples are provided only. The reason is the poor correlation of PSNR and other simple quality measures and perceived quality especially for low-quality images [16]. Note for example that the PSNR computed between the image Lena and its entirely AES encrypted version is 9.2 dB whereas PSNR between Lena and an image with constant grayvalue 128 is 14.5 dB ! Both images do not carry any structural information related to Lena, however, the PSNR values differ more than 5 dB. However, for the most simple attack we may even relate the visual examples to meaningful numerical values.

3.1. Replacement Attack

Assuming the cipher in use is unbreakable we conduct the first attack by directly reconstructing the selectively encrypted images. However, the encrypted parts introduce noise-type distortions (see Fig. 1). Therefore, we replace the encrypted parts by artificial data mimicing typical images. The encrypted bitplane is replaced by a constant 0 bitplane and the resulting decrease in average luminance is compensated by adding 64 to each pixel if only the MSB bitplane was encrypted, 96 if the MSB and next bitplane have been encrypted, and so on. Subsequently, reconstruction is performed as usual, treating the encrypted and replaced parts as being non-encrypted.



(a) 25% encrypted, 13.2dB (b) 50% encrypted

Figure 4: Visual examples for the efficiency of the Replacement Attack.

Fig. 4 shows two visual examples of image reconstructions as obtained by the Replacement Attack (2 and 4 bitplanes are encrypted). Whereas a direct reconstruction of an image with 2 bitplanes encrypted suggests this setting to be "safe" (with 9.0dB quality, see Fig. 1.b), the Replacement Attack reveals that structural information is still present in the reconstructed image (with 13.2dB quality, see Fig. 4.a). However, the visual information is severely alienated. Obviously, not only the visual appearance but also the numerical PSNR values have been significantly improved by the Replacement Attack. In any case, even if a Replacement Attack is mounted, encrypting 4 bitplanes (i.e. 50% of the original data) leads to perfectly satisfying results (Fig. 4.b).

3.2. Reconstruction Attack

For the simplest case, we assume the MSB bitplane to be encrypted only. The idea of the Reconstruction Attack is to reconstruct the MSB data with the aid of the unencrypted remaining data. We exploit the well known property, that most regions of natural images are covered by areas with smoothly changing gray values (except edges, of course). In areas of this type, the MSBs of all pixels tend to be identical (except for the case of medium luminance). In order to automatically detect such areas we define a 2×2 pixels search window in which all 16 possible combinations of MSB configurations are tested. In this test, a certain set of differences among the 4 pixel values is computed for each of the 16 MSB configurations. Out of the set of differences, the smallest difference is selected and the corresponding configuration of the MSB bits in the search window is defined to be the reconstruction. Fig. 5.a shows the MSB of the Lena image and Fig. 5.b a reconstructed bitplane obtained as described above.

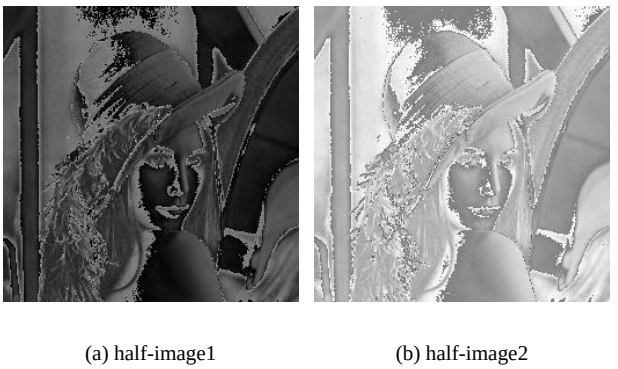
(a) original MSB (b) reconstructed bitplane

Figure 5: MSB of the Lena image and reconstructed Bitplane.

It is clearly visible that smooth areas are satisfactorily recovered (black=0) whereas edges are represented by white lines. This "edge-detection capability" is due to the fact that when the search window hits an edge, the difference operation leads to an attempt to compensate thereby setting the MSB to different values at both sides of the edge. Fig. 6.a shows an image resulting from the Reconstruction Attack where about 50% of the smooth areas are recovered correctly. A second difference exists with equally low value which is obtained as well by setting all MSB values constant (white=1) in smooth areas. Using this as additional information, a second reconstruction is obtained where the remaining 50% of the smooth areas are recovered correctly (see Fig. 6.b).

When combining these two reconstructed "half-images" the original may be obtained easily by choosing the correct areas from the respective half-images (see Fig. 7).

However, the complexity of this attack increases significantly if more bitplanes are encrypted and also the reliability of the results is drastically reduced. Fig. 8 shows the result of this attack mounted against an encryption of two bitplanes where the attack is done in "separable" manner to save computational complexity (i.e. first the MSB is attacked and the second encrypted bitplane is treated is done in the Replacement Attack and then vice versa). The result is hardly more useful as the result of direct reconstruction (compare Fig 1.b).



(a) half-image1 (b) half-image2

Figure 6: Lena Image after Reconstruction Attack (two half-images).

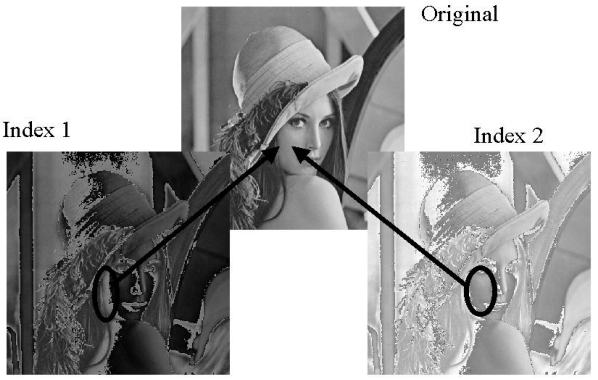


Figure 7: Combination of two half-images after Reconstruction Attack.

4. CONCLUSION

We have proposed selective bitplane encryption to secure image transmission in mobile environments where no compression is involved. Two types of ciphertext only attacks show clearly that encryption of the MSB bitplane only is not secure enough. However, selectively encrypting two bitplanes is sufficient if severe alienation of the image data is acceptable, whereas the encryption of four bitplanes provides high confidentiality.

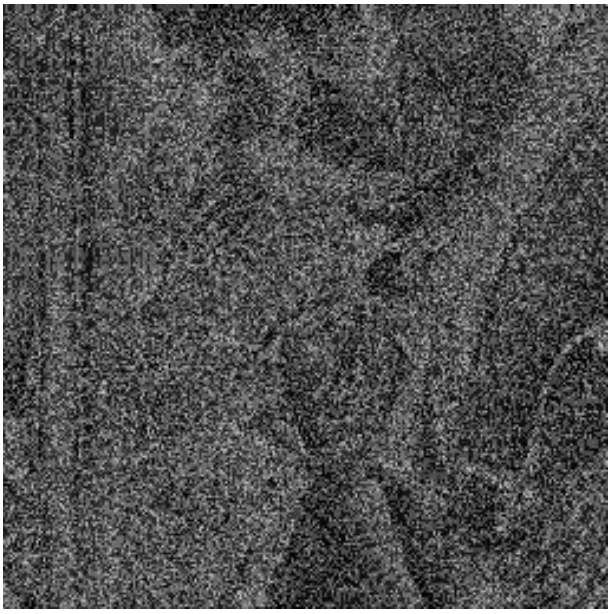


Figure 8: Lena Image after Reconstruction Attack, two bitplanes encrypted.

Acknowledgements

This work was completed in the context of the systems security lab and has been partially supported by the Austrian Science Fund (project FWF-15170).

5. REFERENCES

[1] I. Agi and L. Gong. An empirical study of secure MPEG video transmissions. In *ISOC Symposium on Network and Distributed Systems Security*, pages 137–144, San Diego, California, 1996.

[2] A. M. Alattar, G. I. Al-Regib, and S. A. Al-Semari. Improved selective encryption techniques for secure transmission of MPEG video bit-streams. In *Proceedings of the 1999 IEEE International Conference on Image Processing (ICIP'99)*. IEEE Signal Processing Society, 1999.

[3] H. Cheng and X. Li. On the application of image decomposition to image compression and encryption. In P. Horster, editor, *Communications and Multimedia Security II, IFIP TC6/TC11 Second Joint Working Conference on Communications and Multimedia Security, CMS '96*, pages 116–127, Essen, Germany, Sept. 1996. Chapman & Hall.

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

[5] J. Daemen and V. Rijmen. *The Design of Rijndael: AES - the advanced encryption standard*. Springer Verlag, 2002.

[6] A. M. Eskicioglu and E. J. Delp. An overview of multimedia content protection in consumer electronics devices. *Signal Processing: Image Communication*, 16(7):681–699, 2001.

[7] R. Grosbois, P. Gerbelot, and T. Ebrahimi. Authentication and access control in the JPEG 2000 compressed domain. In A. Tescher, editor, *Applications of Digital Image Processing XXIV*, volume 4472 of *Proceedings of SPIE*, San Diego, CA, USA, July 2001.

[8] T. Kunkelmann. Applying encryption to video communication. In *Proceedings of the Multimedia and Security Workshop at ACM Multimedia '98*, pages 41–47, Bristol, England, Sept. 1998.

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

[10] T. Maples and G. Spanos. Performance study of a selective encryption scheme for the security of networked real-time video. In *Proceedings of the 4th International Conference on Computer Communications and Networks (ICCCN'95)*, Las Vegas, NV, 1995.

[11] A. Pommer and A. Uhl. Wavelet packet methods for multimedia compression and encryption. In *Proceedings of the 2001 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing*, pages 1–4, Victoria, Canada, Aug. 2001. IEEE Signal Processing Society.

[12] A. Pommer and A. Uhl. Selective encryption of wavelet packet subband structures for obscured transmission of visual data. In *Proceedings of the 3rd IEEE Benelux Signal Processing Symposium (SPS 2002)*, pages 25–28, Leuven, Belgium, Mar. 2002. IEEE Benelux Signal Processing Chapter.

[13] L. Qiao and K. 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.

[14] P. A. Schneck and K. Schwan. Authenticast: An adaptive protocol for high-performance, secure network applications. Technical report, Georgia Institute of Technology, Atlanta, GA, USA, 1997.

[15] C. Shi and B. Bhargava. A fast MPEG video encryption algorithm. In *Proceedings of the ACM Multimedia 1998*, pages 81–88, Boston, USA, 1998.

[16] C. J. Skrepth and A. Uhl. Selective encryption of visual data: Classification of application scenarios and comparison of techniques for lossless environments. In *Advanced Communications and Multimedia Security, IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security, CMS '02*, Portoroz, Slovenia, Sept. 2002. Kluver Academic Publishing. To appear.

[17] L. Tang. Methods for encrypting and decrypting MPEG video data efficiently. In *Proceedings of the ACM Multimedia 1996*, pages 219–229, Boston, USA, Nov. 1996.

[18] A. S. Tosun and W. chi Feng. On error preserving encryption algorithms for wireless video transmission. In *ACM Multimedia 2001*, pages 302–307, Ottawa, Canada, Oct. 2001.

[19] T. Uehara, R. Safavi-Naini, and P. Ogunbona. Securing wavelet compression with random permutations. In *Proceedings of the 2000 IEEE Pacific Rim Conference on Multimedia*, pages 332–335, Sydney, Dec. 2000. IEEE Signal Processing Society.

[20] J. Wen, M. Severa, W. Zeng, M. Luttrell, and W. Jin. A format-compliant configurable encryption framework for access control of multimedia. In *Proceedings of the IEEE Workshop on Multimedia Signal Processing, MMSP '01*, pages 435–440, Cannes, France, Oct. 2001.

[21] S. Wong, L. Zaremba, D. Gooden, and H. Huang. Radiologic image compression – a review. *Proceedings of the IEEE*, 83(2):194–219, 1995.

[22] T.-L. Wu and S. F. Wu. Selective encryption and watermarking of MPEG video (extended abstract). In H. R. Arabnia, editor, *Proceedings of the International Conference on Image Science, Systems, and Technology, CISST '97*, Las Vegas, USA, Feb. 1997.

[23] W. Zeng and S. Lei. Efficient frequency domain video scrambling for content access control. In *Proceedings of ACM Multimedia 1999*, pages 285–293, Orlando, FL, USA, Nov. 1999.