A Hierarchical Selective Encryption Technique in a Scalable Image Codec

Cyril Fonteneau, Jean Motsch, Marie Babel, Olivier Déforges

A Hierarchical Selective Encryption Technique in a Scalable Image Codec

C. Fonteneau[a], J. Motsch[ab], M. Babel[a], and O. Déforges[a]
[a] IETR/INSA Image Group, Rennes, France
[b] IETR/LEST/CREC-Saint-Cyr, Coetquidan, France

Abstract

Modern still image codecs furnish more than just good distortion-rate performances. They must also provide some services. Scalability in resolution and quality, error resilience and embedded bitstreams were among the first one to be available. There is still room for enhancement, especially when it comes to security-oriented features. Image encryption is one of the aspect of image security. This paper presents the embedding of an encryption service in a multiresolution lossless codec. Partial encryption is performed using ciphering only the keystone part of the codec algorithm, a quadtree decomposition. This results in a hierarchical encryption scheme, showing to be a good tradeoff between encryption speed, selective access and robustness.

1 Selective image encryption

Nowadays, huge amount of digital visual data are stored on different media and are exchanged over various networks . Often, these visual data contain private, confidential or proprietary informations or are associated with economical interests. As a consequence, techniques especially designed for these data are required so that to provide security functionalities such as privacy, integrity, or authentication. Multimedia security[3] is aimed towards these technologies and applications.

Besides watermarking, steganography, and techniques for assessing data integrity and authenticity, providing confidentiality and privacy for visual data is among the most important topics in the area of multimedia security. Applications range from digital rights management to secured personal communications.

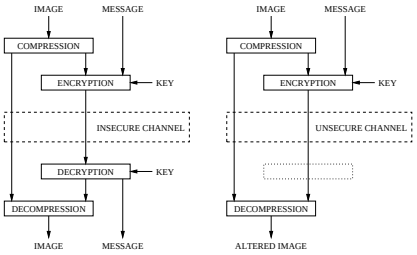
Contrary to classical encryption[2], security may not be the most important aim for an encryption system for images. Depending on the type of applications, other properties (such as speed or bitstream compliance after encryption) might be equally important as well. In that context, naive or hard encryption consists in putting in the whole image data bitstream into a standard encryption system, without taking care of its nature. However, considering the typical size of a digital image compared to that of a text message, the naive algorithm usually cannot meet the speed requirements for real-time digital image processing or transmission applications. In contrast, soft or selective encryption trades off security for computational complexity. They are designed to protect multimedia content and fulfil the security requirements for a particular multimedia application. Research is focused on fast encryption procedures specifically tailored to the target environment.

There are two levels of security for digital image encryption: low level and high-level security encryption. In low-level security encryption, the encrypted image[1] has degraded visual quality compared to that of the original one, but the content of the image is still visible and understandable to the viewers. In the high-level security case, the content is completely scrambled and the image just looks like random noise. In this case, the image is not understandable to the viewers at all.

Selective encryption [4]aims at avoiding the en-

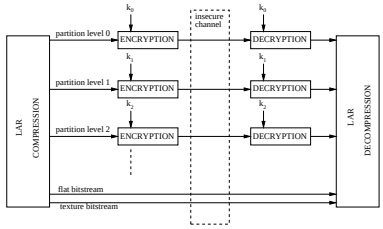
[1] the image decrypted without the decryption key

cryption of all bits of a digital image and yet ensuring a secure encryption. The key point is to encrypt only a small part of the bitstream to obtain a fast method. The canonical framework for selective encryption is presented on figure 1a. The image is first compressed. Afterwards, the algorithm only encrypts part of the bitstream with a well-proven ciphering technique: incidentally, a message (a watermark) can be added at this step. To ensure full compliance with any decoder, the bitstream should only be altered at carefully chosen places. With the decryption key, the receiver decrypts the bitstream and decompresses the image. When the decryption key is unknown, the receiver will still be able to decompress the image, but this image will significantly differs from the original, as depicted in figure 1b.



(a) Selective encryption mechanism

(b) Decryption without decryption key



(c) LAR hierarchical selective encryption

Figure 1: Selective encryption frameworks

Methods for selective encryption[5] proposed recently include DCT-based methods, Fourier-based methods, SCAN-based methods, chaos-based methods and quadtree-based methods. These methods have to be fast to meet the applications requirements and try to keep the compression ratio as good as without encryption.

In this paper, we introduce a hierarchical encryption technique using the compressed bitstream produced by a scalable lossless codec. It allows selective access management and low level security. Encryption is fast and provide a good trade-off between security, visual quality and distortion. Section 2 introduces the technique while section 3 shows experimental results. Finally, section 4 presents briefly future work.

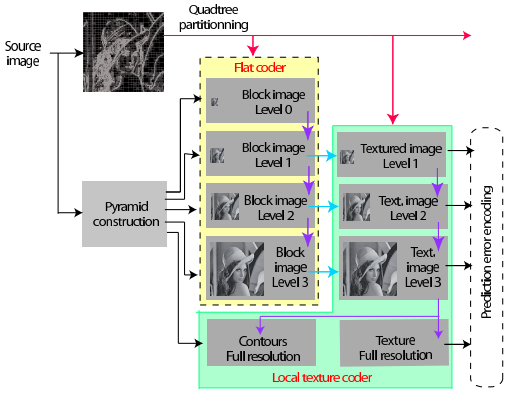
2 Selective encryption of LAR-compressed images

The LAR codec is a multipurpose coding solution for still images. It provides scalability both in resolution and quality, embedded bitstream from lossy to lossless coding, with computational low complexity, using grayscale and color imaging with state-of-the-art distortion-rate performances. This codec adapts resolution to the local activity of the image. Low resolutions correspond to smooth areas, and high resolutions correspond to high frequency areas (edges). That adaptation is described by a block-based quadtree partition, with block size from 2x2 to 64x64 pixels. A hierarchical decomposition framework allows scalability in quality and resolution, as depicted in figure 2a, where a conditional pyramid is used.

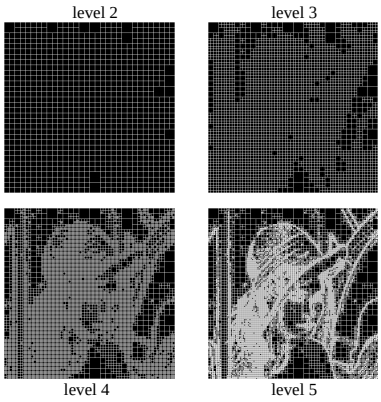
From a selective encryption point of view, the emphasis will be put on the description of the LAR bitstream. This bitstream embodies 3 interleaved components:

- The quadtree partition bitstream. A binary information is required at the decoder in order to construct the quadtree partition. This data is progressively sent level by level. Figure 2b illustrates that progressive coding.
- The flat LAR bitstream used to reconstruct an image of variable-size blocks. This bitstream is constructed during a first descent of the pyramid, conditioned by the quadtree partitioning.
- The texture bitstream that encodes the remaining details. This bitstream is built during a sec-

ond descend of the pyramid, conditioned by the quadtree partition of remaining undecomposed blocks and the flat bitstream.



(a) Hierarchical LAR decomposition for image coding



(b) Quadtree partition progressive coding

Figure 2: Hierarchical LAR

As the conditional pyramid relies on a quadtree partition, this partition needs to be transmitted without error. Previous work on error resilience dealt with that aspectand showed that the decoder was still able to decode erroneous bitstream. In that case, visual quality was very low, even when few bits of the quadtree were wrongly transmitted. Further work introduced a zero cost security mechanism, relying on the size of the quadtree partition search space.

Following that path, we propose to selectively encrypt different levels of the quadtree partition description, as depicted on figure 1c. One typical use-case of that scheme is selective access to an image database.

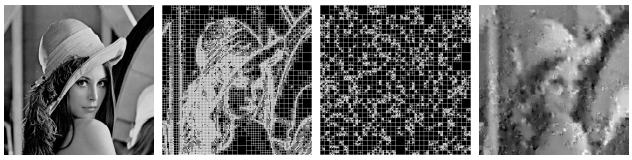
This hierarchical selective encryption technique has the following properties:

- Encryption is performed on a level basis. Different keys are used to encrypt each level of the quadtree partition, and one or several levels can be encrypted. This allows a fine management of the visual information revealed to the decoder.
- Encryption and decryption are performed using a classical cryptosystem, symmetric or asymmetric depending on the target application requirements, in speed or security. It allows for flexibility and standard compliance.
- Encryption can be performed offline on the compressed bitstream or online, during compression.
- Encryption is performed on a small part of the bitstram, especially when images are losslessly coded.

3 Experimental results

The selective encryption scheme has been applied to natural images, using the Advanced Encryption Standard (AES[1]) cryptosystem, with a key length of 256 bits, in ECB (Electronic CodeBook) mode. This system is a 128-bits block cipher adopted as a standard. It has been analyzed extensively and is now widely used worldwide as was the case with its predecesoor, the Data Encryption Standard (DES). AES is one of the most popular algorithms used in symmetric key cryptography. This part of the scheme furnished basic cryptographic security. The following results show the ability of our hierarchical selective encryption scheme.

Figure 3 shows an example of encryption, where the smallest block decomposition is encrypted. When small blocks are modified by the selective encryption, it appears that the overall quality is still acceptable. Nevertheless, the encrypted picture is of no use, as for printing.



(a) Image (b) Partition (c) Encr. Part. (d) Encr. Image

Figure 3: Selective encryption on `lena` at level 3.

Visual effect of encryption at different levels is shown on figure 4. Encrypting level corresponding to small blocks offers low level selective cryptography, whereas the image remains understandable, while encrypting level corresponding to big blocks offers high level selective encryption.

(a) Level 4 (b) Level 3 (c) Level 2 (d) Level 1

Figure 4: Selective encryption on `lena` at decreasing levels

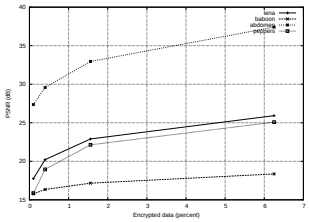


Figure 5: PSNR [dB] vs. relative data encrypted [%] for several images

Figure 5 presents the evolution of the PSNR versus the quantity of data encrypted, for different images. From a distortion point of view, it appears that encrypting higher level (smaller blocks) increases the PSNR, and at the same time, the encrypting cost. From a security point of view, as the level increases, the search space for a brute force attack increases drastically. In example, the entropy of the quadtree partition for `lena` at level 1 is 61 bits, resulting in a search space of 2^{61} differents partition, while at level 4, the entropy is 8886 bits. Encryption at level 1 is weaker than at level 4, but the obtainable quality after decryption is still bad, making that useless. Encryption at level 4 is stronger, but the visual quality is better. In that case, it is very difficult to break the encryption scheme to obtain the lossless image.

4 Future work

Our proposal of a hierarchical selective encryption based on LAR codec presents good results in terms of security, speed or any tradeoff between them. Nevertheless, some aspects need to be further investigated. As usual with cryptosystems, the possibility of attacks is to be considered, both on the underlying cryptosystem, as AES, or on the coding side. For that purpose, further work is necessary to evaluate the computing cost of brute force attacks, quantifying the information available to the attacker. Another point is encrypting the LAR flat bitstream instead of the quadtree partition bitstream. Last point is to develop a complete secure framework, from client to image database, with hierarchical key management.

References

[1] J. Daemen and V. Rijmen. *The desing of Rijndael AES – The Advanced Encryption Standard*. Srpinger, 2002.

[2] B. Schneier. *Applied Cryptography*. John Wiley and Sons, 2nd edition, 1996.

[3] A. Uhl and A. Pommer. *Image and Video Encryption*. Springer, 2005.

[4] M. Van Droogenbroeck and R. Benedett. Techniques for a selective encryption of uncompressed and compressed images. In *ACIVS Advanced Concepts for Intelligent Vision Systems*, pages 90–97, Ghent, Belgium, September 2002.

[5] M. Yang, N. Bourbakis, and S. Li. Data, image and video encryption. *IEEE Potentials*, 2004.