MULTI–RESOLUTION ACCESS CONTROL ALGORITHM BASED ON FRACTAL CODING

S. Roche, J.-L. Dugelay and R. Molva

Institut EURECOM.
B.P. 193, F-06904 Sophia Antipolis Cedex
E-mail: {roche,dugelay,molva}@eurecom.fr
URL: http://www.eurecom.fr/~image

ABSTRACT

This paper presents, a new technique for compression and secure image coding that is based on IFS. A multi-resolution access control algorithm based on the convergence control of iterative image reconstruction process is investigated. For multimedia applications an icon representation of low image quality is extracted directly from the encrypted data flow thanks to the partial self-affinity properties inherent to Local-IFS. The robustness of our scheme is due to the inherent high correlation of image data and to the non-linear decoding process.

1. INTRODUCTION

The advent of multimedia applications has brought new requirements for a joint approach combining image processing and security techniques. Security becomes a mandatory component of commercial multimedia applications providing access to images through public channels. Typical security mechanisms required by such applications include encryption, digital signatures and fingerprinting. In this paper we present a new approach based on IFSC —Iterated Function System Coding— that provides both compression and hierarchical access control for images at various resolution levels.

The hierarchical access control scheme allows all the receivers of the broadcast channel to display a low resolution image with no commercial value. The scheme also allows image access at higher quality levels depending on each receivers access rights that usually are determined by the subscription agreement. The hierarchical access control mechanism is different from a classical encryption scheme in that the message received through the public channel is not totally hidden in order to attract potential customers who would apply for the commercial service to get the higher quality image. Hierarchical access control can be achieved through the serial combination of existing compression and encryption algorithms like the DES but several constraints due to performance limitations of a full-fledge encryption algorithm in the context of multimedia applications and to security exposures inherent to the high correlation akin to images prohibit the use of existing algorithms for the new applications [1]. The hierarchical access control scheme suggested in this paper provides both compression and security functions within a single algorithm. Since the protection mechanism is integrated with IFSC, specific properties of images are taken into account in the design of the access control mechanism as opposed to a general encryption algorithm. Thus, instead of the whole encoded image, only key parameters of the IFS code need to be encrypted.

2. A REVIEW OF FRACTAL IMAGE CODING

The basic idea about fractal image coding is to represent the image by a set of transforms associated with an iterated process [2]. The goal is to assure that this process converge towards a fixed point called attractor that is an approximation of the original image. The compression gain provided by this technique is due to the compact encoding of the set of transforms that represent the image data.

In order to formalize these concepts we introduce the following notations.

2.1. Notation

- x, y two generic images.
- x_c the image to be encoded.
- x_0 the initial image of the iterative process.
- $\mathcal{W}$ the image transform.
- x_a the attractor of $\mathcal{W}$.
- d a metric defined on the image space.

2.2. Collage theorem

If it exists $\mathcal{W}$ such as $d(x_c, \mathcal{W}(x_c)) \leq \epsilon$ and
$d(\mathcal{W}(x), \mathcal{W}(y)) \leq \sigma \cdot d(x, y)$ where $0 < \sigma < 1$
then
$d(x_c, x_a) \leq \lim_{n \to +\infty} \{ \frac{1-\sigma^n}{1-\sigma} \cdot \epsilon + \sigma^n \cdot d(x_c, x_0) \}$
with $x_a = \lim_{n \to +\infty} \mathcal{W}^{on}(x_0)$
and $\mathcal{W}^{on} = \underbrace{\mathcal{W}(\mathcal{W}(\cdots(\mathcal{W}(x_0))\cdots))}_{n \text{ terms}}$

Unfortunately the previous theorem does not give any clue on how to construct the global image transform $\mathcal{W}$. In spite of numerous attempts no general method for computing the global image transform $\mathcal{W}$ has so far seen discovered. Nevertheless, a way out has been proposed for still image coding by A. Jacquin who introduced the Local-IFS concept [3].

2.3. Jacquin's algorithm

Unlike IFS coding, Local-IFS coding does not search global self-affinity, i.e. smaller copies of the entire image buried in it at every scale. Instead, data redundancy is exploited through partial self-affinity. Thus the previous problem is split into several smaller problems leading to the implementation of a low complexity algorithm. In this algorithm x_c is partitioned at two different levels of resolution. The partitioning uses squared blocks of size $B \times B$, called range blocks, in the first level and squared blocks of size $2 \cdot B \times 2 \cdot B$, called domain blocks, in the second level —typically, B is fixed at 4 or 8 pixels—. For each range block, the algorithm searches the domain block for which the following local quadratic error is minimal:

$$\epsilon_k = \sum_{(i,j) \in R_k} \left((\mathcal{W}_k(D_k))(i,j) - R_k(i,j) \right)^2$$

where

- $R_k(i,j)$ designates the grey-value at pixel (i,j) in the range block indexed by k.
- $(\mathcal{W}_k(D_k))(i,j)$, designates the grey-value at pixel (i,j) in the transformed domain block D_k associated with R_k.

Before the matching stage, domain blocks are transformed as follows [4]:

- sub-sampling by a factor two —in each direction—
- geometric transformations —eight isometries are considered—
- scale and offset on the luminance value. These parameters are computed using a least square method based on the local criterion described previously.

For each range block R_k and its associated domain block D_k —written in vector form—, these operations can be expressed under the following matrix form:

$$\begin{pmatrix} r_{k\,1} \\ \vdots \\ r_{k\,B^2} \end{pmatrix} = [A_k]_{B^2 \times 4 \cdot B^2} \cdot \begin{pmatrix} d_{k\,1} \\ \vdots \\ d_{k\,4B^2} \end{pmatrix} + \begin{pmatrix} b_k \end{pmatrix}$$

with
$$(b_k) = (\ o_k, \quad \cdots \quad , o_k\ )^t$$

and
$$[A_k] = \begin{pmatrix} 0 \cdots 0\ s_k\ s_k\ 0 \cdots 0\ s_k\ s_k\ 0 \cdots 0 \\ s_k\ s_k\ 0 \cdots\cdots 0\ s_k\ s_k\ 0 \cdots\cdots 0 \\ 0 \cdots\cdots 0\ s_k\ s_k\ 0 \cdots\cdots\ 0\ s_k\ s_k \\ 0 \cdots\cdots 0\ s_k\ s_k\ s_k\ s_k\ 0 \cdots\cdots 0 \end{pmatrix}$$

with $-1 \leq s_k \leq 1$
In this representation the range block space is associated with the row space of the matrix A_k and the domain block space is associated with the column space of this matrix. The four $s_k \neq 0$ per line express the scale of the grey level transformation and the sub-sampling by average of 4 pixels of D_k. The distribution of s_k among the 0 represents the 8 isometries. Since all the range blocks R_k define a partition of the image, the set of local transforms $\mathcal{W}_k$ constitutes the local-IFS code. In the decoding place the attractor x_a of the original image x_c is obtained from its Local-IFS code and any initial image x_0 by the following algorithm: image x_0 is partitioned into a set of square-blocks. Each area R_k of the image is computed by taking the associated block D_k in image x_0 and applying the associated contractive local transformation $\mathcal{W}_k$ defined during the coding stage. The resulting image is called x_1. The algorithm iterates this process to obtain x_2 from x_1 and so on until it reaches x_a. In practice, less than ten iterations are needed.

3. FRACTAL CODING FOR MULTI-RESOLUTION ACCESS CONTROL

3.1. Access control principle

Our access control is based on the control of the reconstruction process —the iterated process—. As indicated in the collage theorem, the convergence parameter σ is very important in the IFSC because it controls the decoding process convergence and so the quality of the reconstructed image. Unfortunately, σ is not accessed directly in the Jacquin's model due to the local structure of the code. However we can modify σ efficiently through the luminance scale-parameters s_k of the matrices A_k [5]. By partially hiding the value of s_k through encryption several gradual access levels can be obtained. For instance, if s_k is quantized with 8 bits, each of this bits could be let readable (Fig.2*a*). In this case, the classical reconstructed image with highest resolution is obtained (Fig.3*d*). On the other extreme encrypting all 8 bits of s_k leads to the image of Fig.3*a* that is unreadable. During the decoding process the encrypted s_k bits can be affected by guessed values so that the value of s_k lies in the midrange —i.e. 0— of scale parameters. Then according to the Jacquin's transformation structure, the $[A_k]$ matrices become $[0]$ consequently range blocks and domain blocks become independent. Only one iteration is then enough to obtain the attractor that consisted on uniform blocks with the grey values equal to the offset values o_k (Fig.3*a*) — highest encryption—. Between these two extreme configurations, encryption of s_k at intermediate degrees leads to intermediate levels of visualization quality. It is important to notice that the iterated process is still convergent because even the guessed values of $|s_k|$ lie below 1. Note that any domain block can be view as a set of range blocks (Fig.1). Each range block of the decoded image x_a is thus highly dependent on the block mappings performed on a pyramidal fashion during the previous iterations. Hence the s_k values associated with each of the blocks involved with these mappings strongly affect the final decoded image. Thus s_k values appear to be the key parameter in order to provide access control.

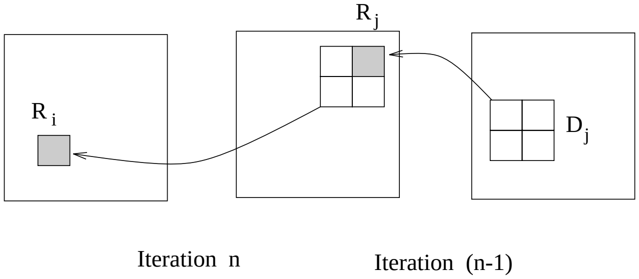

Figure 1: *Domain block as a set of* 4 range blocks

3.2. Icon representation

In multimedia applications, an icon representation is preferred to a low-resolution full size image. Thanks to its hierarchical structure, L-IFS provides a zooming capability [4] that allows for the construction of an icon from an L-IFS coded image even when the s_k values are unknown. Icon representation can be obtained directly from the ciphered data flow by choosing adequate range and domain block sizes. For instance, if the coding stage is performed with range blocks of size 4×4 and domain blocks of size 8×8, an icon representation — zoomed out by factor 16— is obtained by setting 1×1 as the range block size and 2×2 as the domain block size while decoding (Fig.4). Note that the Local-IFS data used at the decoding stage are the same ones that were computed during the coding stage. Only decoding algorithm parameters —block sizes— are modified in order to get an icon.

	MSB			s_k bits				LSB
a	**1**	**0**	**0**	**1**	**1**	**1**	**1**	**0**
b	**1**	**0**	**0**	**1**	**1**	×	×	×
c	**1**	**0**	**0**	**1**	×	×	×	×
d	**1**	**0**	**0**	×	×	×	×	×
e	**1**	**0**	×	×	×	×	×	×
f	**1**	×	×	×	×	×	×	×
g	×	×	×	×	×	×	×	×

Figure 2: s_k *parameters masking from no encryption (a) to full encryption (g)*

4. SECURITY EVALUATION

Here, we consider the security of the protection mechanism in the presence of possible attacks by malevolent intruders [6].

exhaustive search: the first attack consists in an exhaustive exploration of the set of possible values for secret data. The complexity of this attack is in the side of $O(2^{(4096 \cdots n)})$ where 4096 is the range block number, n is the number of s_k bits that are encrypted. This large combination is due to the interdependence of the range blocks (Fig.1).

s_k *auto-correlation*: the complexity of the search on s_k values in different blocks could be reduced based on the auto-correlation between s_k but no correlation exists even between two adjacent range blocks.

statistical cross-correlation: the attacks aiming at the guess of s_k values based on the statistical cross-correlation between s_k and other parameters like o_k are impossible because they would also require the knowledge of the original image.

filtering: filtering seems to be another potential means of restoring the original image at an acceptable quality. However the non-linear aspects of corruption due to the iterated coding process makes the design of a suitable filter extremely difficult.

5. CONCLUDING REMARKS

In this paper, a compression scheme for still images using IFS that provides a multi-resolution access control facility is described. Thanks to the properties of IFS, the multi-resolution access can be achieved without any degradation of compression performance. This scheme considers image data features in order to prevent some possible attacks. Using this scheme, the same public decoder could be used with or without protection. An extension of this scheme to moving picture is under investigation. The principle remains unchanged, except that 3-D cubes are used instead of 2-D block primitives in order to compress GoP —Groups of Picture— instead of still images [7]. An improvement of the basic scheme can be envisioned by focusing only on significant parts of the image data like the center of the image or the RoI —Regions of Interest— in the case of still images, or the spatio-temporal areas including motion in the case of moving picture.

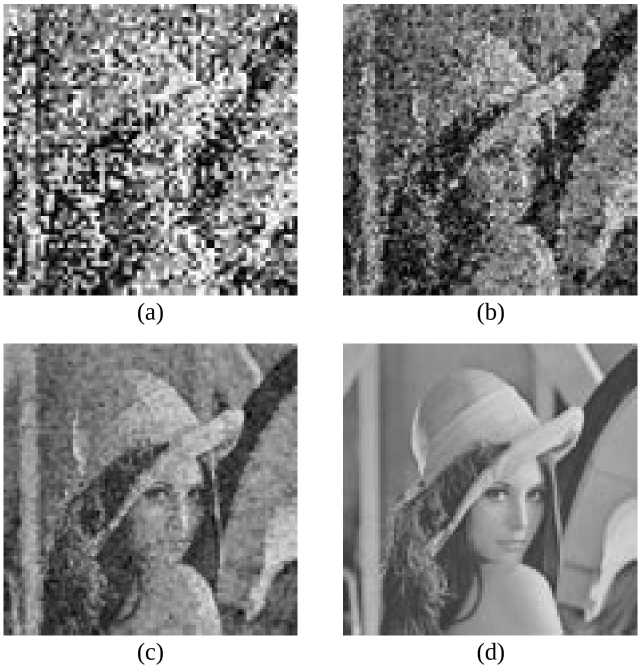

Figure 3: *Fractal compression of Lena face with access control using* (a) *8/8 protected bits,* (b) *6/8 protected bits,* (c) *5/8 protected bits, and with* (d) *no access control (0/8 protected bits).*

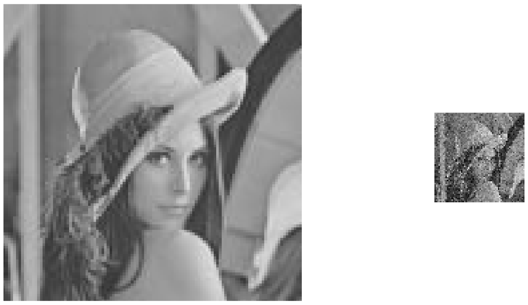

Figure 4: *Icon representation of Lena face with access control using*

6. ACKNOWLEDGMENTS

This work is in partly supported by DGA/DRET — groupe Télécommunications & Détection—.

7. REFERENCES

[1] B. Macq & J.-J. Quisquater, "Digital Images Multiresolution Encryption", *IMA Intellectual Property Project Proceedings*, Vol. 1, jan. 1994.

[2] M. Barnsley & L. Hurd, "Fractal Image Compression", AK Peters, Wellesley, 1993.

[3] A. E. Jacquin, "Image Coding Based on a Fractal Theory of Iterated Contractive Image Transformations", *IEEE trans. on Image Processing*, Vol. 2, No. 1, pp. 18-30, jan. 1992.

[4] Y. Fisher, "Fractal Image Compression – Theory and Application", Springer-Verlag, New York, 1994.

[5] S. Roche & J.-L. Dugelay, "Improvements in I.F.S. Formulation for its Use in Still Image Coding", *1995 IEEE Workshop on Nonlinear Signal and Image Processing*, Vol. 1, Neos Marmaras Halkidiki Greece, sept. 1995.

[6] J. Massey, "On Sabatical Visit Winter 1995", *Institut Eurecom Library*, jan. 1995.

[7] J.-L. Dugelay, J.-M. Sadoul & M. Barakat, "A comparative Study of Existing Approaches to Moving Picture Coding using I.F.S.", *Int. Symp. on Multimedia Communications & Video Coding´*, oct. 1995.