# Combined Encryption and Image Compression Using Adaptive Quadtree Decomposition and Coupled Chaotic Systems

RANJAN BOSE AND SAUMITR PATHAK
Department of Electrical Engineering
Indian Institute of Technology, Hauz Khas, New Delhi 110016 INDIA
http://paniit.iitd.ac.in/~rbose

*Abstract:-* The proposed technique combines quadtree-based compression and chaotic-encryption, and can be used for secure image transmission over the internet. The method of quadtree decomposition, an image representation technique, essentially decomposes a given image into its four major quadrants, which are further decomposed progressively. The technique provides for a powerful variable resolution or variable block size image coding with potential for flexible and more efficient bit allocation than other fixed block size schemes. In the proposed technique, the quadtree decomposition is not regular but is varied adaptively according to a parameter of irregularity resulting in unequal block quadrant sizes. We have used the coupled chaotic system process for this purpose. We have compared the compression performance of our new scheme with regular decomposition and the two compare well. Thus, if the parameter of irregularity is incorporated into the key along with the tree structure of the image, then our algorithm transforms into a fast image encryption tool, providing medium to high level security for multimedia and internet applications.

*Key-Words:-* Encryption, Compression, Quadtree Decomposition, Coupled Chaotic Systems

## 1 Introduction

While block-sizes in transform coding, which are fixed prior to processing, often are large enough not to be able to satisfactorily treat high detail regions, block sizes in VQ based methods are often too small to take advantage of the redundancies of large homogenous regions. Quadtree decomposition [1] of images provides a variable block size image coding technique and offers the potential of a better variation of the number of bits spent per unit area, according to local detail [2, 3]. Theoretical results concerning the variation of threshold as the block size changes [4] and on bit allocation based on rate-distortion theory [4] have helped address some of the difficulties in optimizing the quadtree scheme with sight on its usefulness as a compression scheme. Quadtrees have also been used in inter-frame sequence coding with good compression properties [5]. Mathematical analysis of quadtrees have been done in [6] and [7].

In [8], quadtrees have been explored as an image compression technique which can be used for image encryption by partial encryption of the data. Part of the image data, including tree structure and bit allocation information, is encrypted while the rest of the image information is transmitted without encryption. The encrypted part is critical to the regeneration of the entire image, and it has been shown that cryptanalysis is difficult if a particular type of leaf ordering is used.

In this paper, we propose a flexible quadtree decomposition scheme which carries out non-regular decomposition. Using this scheme, we have implemented an image encryption

algorithm which introduces irregularities into the decomposition using state-of-the-art random generation schemes. Results indicate that the scheme does not affect compression performance while offering medium-to-high level security. The joint compression and encryption is suitable for multimedia and internet applications where fast deployment of security is the ever-recurring need.

## 2 Regular Quadtree Decomposition

Regular quadtree decomposition consists of the successive subdivision of the image array into four equal-sized quadrants. If any of the resultant quadrants consists entirely of a homogenous region, or a region not absolutely homogenous but which still passes a test of similarity, then the quadrant is retained as a leaf, to be represented by the mean luminance signal of the four quadrants. Otherwise the region is subdivided into quadrants, subquadrants, etc. until blocks are obtained (possibly single pixels) that consist of an acceptable homogeneous configuration. Thus the region quadtree can be characterized as a variable resolution data structure. The first decomposition is termed as the highest level. Each further decomposition is termed as a progressively lower level. An image of size $2^n$ x $2^n$ can be decomposed into at most ($n$+1) levels. Since the parent node intensity is a mean value of the children node intensities, the test of similarity examines the error of this representation in the property of interest [5, 8] and each level, except the bottom, the node intensity is calculated according to the following:

for $i = 1,..., n$;
  for $k,l = 0,..., 2^{n-1} - 1$;
    $$x_i(k,l) = \frac{1}{4}\sum_{j=0}^{1}\sum_{m=0}^{1} x_{i-1}(2k+j, 2l+m)$$
  end
end

(1)

Several tests of similarity have been defined in literature [3], among them are the mean square error test and the simple absolute difference test.

## 3 Flexible Decomposition

Flexible decomposition of an image can be interpreted as a region-growing algorithm which works best in a rectangularly structured image. The compressed file is a collection of such rectangular regions represented by the color information as well as the positional and dimensional information of the region being encoded. In the case of an image which is has less rectangular symmetry in its content, a rectangular interpretation of the image yields a greater number of regions, thus decreasing compression. In a complex real-world image, which is more likely to be encountered than the previous kind of images, with no implicit rectangular intentions, a large number of regions result and the size can be estimated as follows. The quantity

$$M = (\log c + 2(\log m + \log n)) \text{ bits} \qquad (2)$$

is the memory requirement of a rectangular artifact, where $c$ is the number of colors to be encoded and $m$ and $n$ are horizontal and vertical dimensions of the image. This can be reduced to:

$$M = \frac{\log c(mn)^2}{8} \text{ bytes.} \qquad (3)$$

Since an uncompressed image takes up

$$mn \log c \text{ bits,} \qquad (4)$$

compression can be estimated as

$$\frac{\left[mn\log c - i\log c\left(mn\right)^2\right]\times 100}{mn\log c} \qquad (5)$$

where $i$ is the number of rectangular artifacts recognized during decomposition.
Since an unrecognized artifact takes $m_j n_j \log c$ bits for representation, where $m_j n_j$ is the size of the artifact, there is profit in compression only when

$$\log c(mn)^2 > m_j n_j \log c. \qquad (6)$$

For an average 128 X 128 image, this means that there if profit only when artifact size is greater than 4 x 4.

Rule-based flexible decomposition of an image may be carried out either using entropy criteria to decide the best possible horizontal and vertical coordinate along which to carry out quad decomposition, or using a recursive algorithm for arriving upon the best solution. Flexible decomposition requires $(m_j + n_j)$ comparisons for each quadrant which result in $(4(\log m) - i)\ (m_j + n_j)$ comparisons.

## 4 Arbitrary Flexible Decomposition

Abandoning rule-based quadtree decomposition since it is computationally expensive, there is the possibility of an arbitrary decomposition algorithm which decomposes the image at each step into four unequal quadrants. Motivation for this possibility is derived from the fact that images have no intrinsic quality which favors regular quadtree decomposition. This is especially true when considering image compression, an important application of quadtree decomposition, since spatial redundancy in real-world images is not inherently aligned along the regular quadrants. Quadtree decomposition is suitable since in addition to an uncomplicated algorithm, the uncompressed tree structure for the image takes

$$B_P = \frac{4^n - 1}{3 \times 4^n} \text{ bits/pixel}, \tag{7}$$

where $n = \log m$ is the depth of the entire tree for the image. This amounts to not more than 33% of the total rate of the image. Compression reduces tree size further, taking up anything from 10% to 20% of total image rate [8]. They can be compressed further using a suitable encoding. On using an arbitrary series like the chaos series generated by the logistic map which is completely defined using its initial condition and which shows properties of sensitivity and error propagation, an arbitrary decomposition of the quadtree can be carried out without expending additionally on specifying the tree structure. We have used the following family of recursive chaotic equations:

$$x_{n+1} = \alpha x_n(1 - x_n), \tag{8}$$

where $\alpha > 3.87$. A direct application of this algorithm is for image encryption since image decoding can be completely key-dependent, where key is a 128 bit number from which seed values and iteration level can be derived using a pre-defined method.

Image encryption is carried out by decomposing the image along semi-arbitrary bisections of the plane, using two separate chaos series for the x and y dimensions. Chaotic series are employed to generate two arbitrary numbers which upon subtracting from and adding to the regular column and row division yields quadrants within a prior-set percentage threshold of their regular equal-sized versions. Recursive decomposition is then progressively carried out on each quadrant, and the process stops when either the quadrant in question is converted into a leaf or when one of the dimensions of a quadrant becomes 1 pixel wide. Alternatively, the decomposition tree may be formed from the lowest level upwards by generating an image-wide decomposition pattern, and gradually climbing the tree up as quadrants are combined into leafs or are retained to reflect detail. This second method is the faster among the two since it avoids carrying out wasteful computation among the higher levels of the decomposition tree, which stand the least chance to be retained as leafs.

Using this scheme, encoded image transmission through a public channel consists of a tree structure specification, based on arbitrary decomposition, followed by the color information. The key, on which the decomposition was based, is transmitted separately through a secure network, and is necessary for image decoding. The image size is encapsulated with the key.

Decryption is carried out in the following way. The tree structure is already known and is parsed for 1s and 0s. The image size is extracted from the key and an empty matrix is created for recreating the new image. Each arbitrary decomposition is represented by a diad which represents the intersection of the horizontal and vertical bisections. The different quadrants are generated with the help of the two chaos series and color information is extracted from the bitstream following the tree structure information in the encoded image.

Fast and cryptographically secure chaotic processes have been proposed and studied in literature [9-10]. We have used the coupled chaotic system process used in [11]. Consider two different chaotic maps $M_1(x_1, p_1)$ and $M_2(x_2, p_2)$. For these maps, iterations may be represented as:

$$x_1(i+1) = M_1(x_1(i), p_1) \quad \text{and}$$
$$x_2(i+1) = M_2(x_2(i), p_2) \tag{9}$$

Here $x_1(0)$ and $x_2(0)$ are the initial conditions and $p_1$ and $p_2$ are the control parameters. The $i^{th}$ pseudorandom bit, $b_i$, is defined as:

$$b_i = \begin{cases} 1, & x_1(i) > x_2(i) \\ \text{no output}, & x_1(i) = x_2(i) \\ 0, & x_1(i) < x_2(i) \end{cases} \tag{10}$$

# 5 Simulation results

In the following simulations performed on a series of images, we have calculated the mean square error (MSE) and the peak signal to noise ratios (PSNR) for varying quality threshold and parameter of irregularity. For testing the proposed technique, we have used files downloaded from the Calgary Corpus available on the web (ftp.cpcs.ucalgary.ca/pub/projects/text.compression.corpus). Fig. 1 gives the variation of (i) MSE and (ii) PSNR with compression strength for (a) regular quadtree decomposition and (b) arbitrary flexible quadtree decomposition. The different curves in (b) have been obtained for coefficient of irregularity 0.1, 0.15, and 0.2.

As can be seen from the figure, the flexible quadtree segmentation compares well with regular segmentation in the compression achieved versus distortion. The performance decreases marginally for low bitrates. Please note that we have used the coupled chaotic system process for the encryption process as discussed in section 4. Thus the algorithm combines both encryption and compression to give a fast encryption technique for multimedia applications. The security of the application can be adjusted as per the need by increasing the key-size of the key.

# 6 Conclusions

We have proposed a flexible arbitrary quadtree-based decomposition for images that has applications in cryptography. The decomposition is not regular but is varied according to a parameter of irregularity resulting in unequal block quadrant sizes. We have used the coupled chaotic system process for this purpose. If the parameter of irregularity is incorporated into the key along with the tree structure of the image, then our algorithm transforms into a fast image encryption tool, providing medium to high level security for multimedia and internet applications. The compression performance of the new scheme is compared with the regular quad-tree decomposition technique and the two methods compare well. This shows that we have been able to add security to the image without compromising on the compression. If the parameter of irregularity is incorporated into the key along with the tree structure of the image, then our algorithm transforms into a fast image encryption tool, providing medium to high level security for multimedia and internet applications.

*References:*


[1] Samet, H., 1984, The Quadtree and Related Heirarchical Data Structures, *ACM Computing Surveys*, Vol. 16, No. 2, 187-260.

[2] Strobach, P., 1991, Quadtree-structured recursive plane decomposition coding of images, *IEEE Transactions on Signal Processing*, Volume 39, Issue 6, 1380-1397.

[3] Strobach, P., 1989, Image coding based on quadtree-structured recursive least-squares approximation, *International Conference on Acoustics, Speech, and Signal Processing*, 23-26 May, Volume 3, 1961 – 1964.

[4] Shusterman, E. and Feder, M, 1994, Image compression via improved quadtree decomposition algorithms, *IEEE Transactions on Image Processing*, Volume 3, Issue 2, 207-215.

[5] Strobach, P., 1990, Tree-structured scene adaptive coder, *IEEE Transactions on Communications*, Volume 38, Issue 4, 477–486.

[6] Faloutsos, C., 1992, Analytical Results on the Quadtree Decomposition of Arbitrary

Rectangles, *Pattern Recognition Letters*, Vol. 13, No. 1, 31-40.
[7] Floutsos, C., Jagadish, H.V., and Manolopoulos, Y., 1997, Analysis of the n-Dimensional Quadtree Decomposition for Arbitrary Hyperrectangles, *IEEE Transactions On Knowledge and Data Engineering*, Vol. 9, No. 3, 373-383.
[8] Cheng, H. And Li, H., 2000, Partial Encryption Of Compressed Images And Videos, IEEE *Transactions On Signal Processing*, Vol. 48, No. 8, 2439-2451.
[9] Tao, S., Ruili, W. and Yixun, Y., 1998, Perturbance-based algorithm to expand cycle length of chaotic key stream. *Electronics Letters*, 34 (9), 873–874.
[10] Tao, S., Ruili, W. and Yixun, Y., 1998, Clock-controlled chaotic keystream generators. *Electronics Letters*, 34 (20), 1932–1934.
[11] Li, S., Mou, X. and Cai, Y., 2001, Pseudo-random bit generator based on couple chaotic systems and its application in stream-ciphers cryptography. Progress in Cryptology - *INDOCRYPT 2001*, 16-20 December, 2001, Chennai, India, Lecture Notes in Computer Science (2247), 316–329, Springer-Verlag, Berlin.

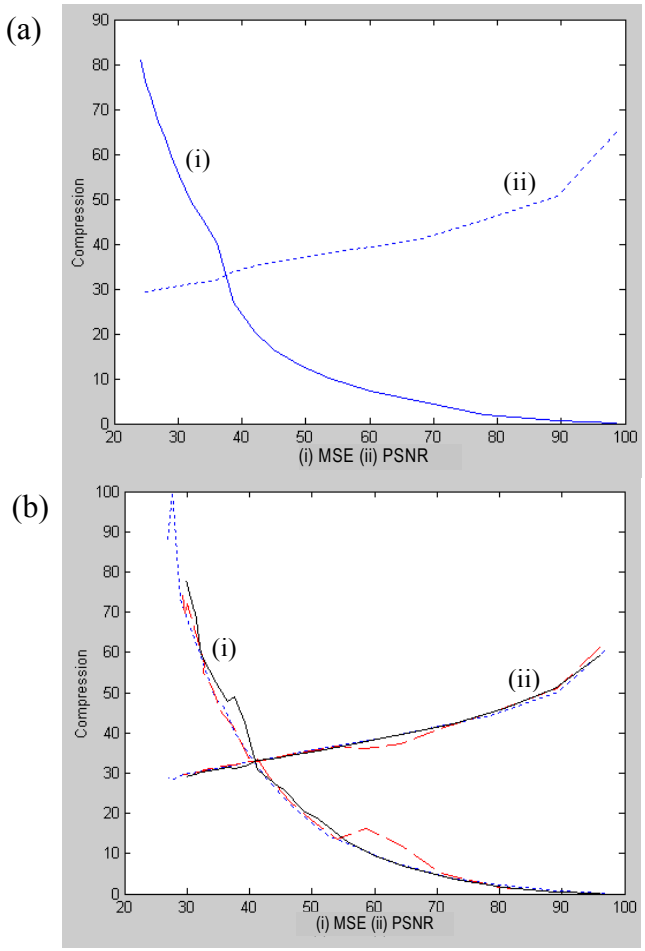


Fig. 1. Variation of (i) MSE and (ii) PSNR with compression strength for (a) regular quadtree decomposition and (b) arbitrary flexible quadtree decomposition. The different curves in (b) have been obtained for coefficient of irregularity 0.1, 0.15, and 0.2.