Compression Mechanism for Multimedia System in consideration of Information Security

By

Nileshsingh V. Thakur\textsuperscript{1} and Dr. O.G. Kakde\textsuperscript{2}
Dept. of Computer Science
\textsuperscript{1}SRKNEC, \textsuperscript{2}VNI T, India.

\texttt{thakurnisvis@rediffmail.com, ogkakde@cse.vnit.ac.in}

MI R DAY International Workshop

24 / 01 / 2009
Encryption and Compression

Raw image encryption - Image encrypted before compression

- Image permutation that changes the pixels' position randomly [4-5]
- Kwok et al. (2007) used the cascaded chaos maps to construct the stream cipher [6]
- Zhou et al. (2007) used the discrete Kolmogorov flow map [7]
- Gao et al. (2007) used two chaotic maps to shuffle the image pixels [8]
- Zhang et al. (2005) Discrete exponential chaotic maps’ confusion and diffusion properties are improved and used [10]
- Yen et al. (1999) The Chaotic Neural Network is used to design the stream cipher [11]
- The 2-dimensional Baker map is used to construct the block cipher [12-13]
- The 3-dimensional chaotic maps are used to make the block ciphers [14-15]
Compressed image encryption - Image encrypted after compression

- The two steps are combined to reduce processing time by adding a pseudo-random shuffle into the data compression process [16]
- Intelligent Dictionary-based Encoding for preprocessing and encryption [17]

Partial encryption-
- The DCT coefficients’ signs are encrypted in DCT transformed blocks [19]
- The data blocks are permuted in frequency domain [20,21]
- Both the coefficients’ signs and block positions are encrypted [22,23]
Possible Multimedia System Security Mechanism
Fractal Coding

- Gray level images through rectangular domain and range blocks
- Range Blocks (RB), Domain Blocks (DB), Codebook Blocks (CB)
- Minimized the quantity $RB = \sum_{i=1}^{n} (s_{c_i} + o - r_i)^2$
- Y. Fisher’s least squares regression method
- Quantization of $s$ & $o$
- Among all codebook blocks, find the block with minimal error
  $$E(RB_i, CB_i) = \min E(RB_l, CB_k)$$
- Output-Code for current range block-indices for $s$ & $o$ and index identifying the optimal codebook block
Spiral Architecture

Basics-
Spiral Addressing, Spiral Counting, Spiral Addition, Spiral Multiplication
Spiral Architecture

**Constraint and Solution-**

- No supporting hardware
- Construct or mimic

**Why?**

- The difference of light intensities between pixels is highly related to the distance between them: the closer they are, the less difference observed
- Due to the difference between the centre hexagon and other neighboring hexagons would be quite small, each set of seven hexagons may enjoy very similar light intensities
- Rotation invariant
One-Plane image formation:

- Hierarchical partitioning exploits the strong correlation based on quadtree partitioning.
- Each block can be represented by a mean value of all pixels’ trichromatic coefficient ratios.
- These mean values, position and size of a block can be stored as the first part of the compressed image.
- One-Plane image can be formed with weighted sum of the three-color components.
Proposed Compression Mechanism

• Intuitively,

  The variance of trichromatic coefficients is small when the three-color planes are strongly correlated, in such a case, larger blocks can be obtained, implying as consequence, that higher compression ratio can be achieved.

<table>
<thead>
<tr>
<th>Color Space</th>
<th>Covariance</th>
<th>Variance</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>R</td>
<td>G</td>
</tr>
<tr>
<td>R</td>
<td>1.0</td>
<td>0.9930</td>
</tr>
<tr>
<td>G</td>
<td>0.9930</td>
<td>1.0</td>
</tr>
<tr>
<td>B</td>
<td>0.9784</td>
<td>0.9916</td>
</tr>
</tbody>
</table>
Proposed Compression Mechanism  

Spiral architecture

Construction of Spiral architecture-
1. Read a color image $\mathbf{CI}$ with size $N \times N$

2. Calculate the trichromatic coefficients for each pixel (equation (1))

3. Subdivide the image recursively by quad tree partitioning
   (a) Partition the image in 4 non-overlapped blocks with size $\frac{N}{2} \times \frac{N}{2}$
   (b) For each such a block, calculate the average trichromatic coefficient and variances (equation (2) and (3))
   (c) The process of division continues, if equation (4) (with a pre-defined tolerance) is not satisfied. When this occurs, the block will be divided into another four quadrant sub-blocks, and for each of them, the same steps 2), 3), is repeated again. The process of quarter halts if any one of the two conditions are satisfied:
      (i) The pre-defined maximum dividing level is reached;
      (ii) Or, equation (4) is satisfied.
   (d) If all of the blocks have been processed (recursively returned), the whole process terminates.

   $$v_{rr}^I \leq \text{tolerance and } v_{gg}^I \leq \text{tolerance and } v_{bo}^I \leq \text{tolerance} \quad (4)$$
4. One-plane image $S$ is produced with a value of $S_{ij}$ associated to each pixel.

5. The image $S$ and the mean value of trichromatic coefficient ratio of each block are stored as the first part of compressed image.

6. The one-color plane image $S$ is represented in Spiral Architecture to get image $S'$.

7. Compress $S'$ by invoking the fractal coding algorithm, codebook blocks formed by taking median of the pixel intensities of each cluster of seven hexagons.

8. Store the indices for the quantized coefficient $s$ and $o$ and the index $l$ identifying the optimal codebook block $CB_l$ as the second part of compressed image.
Proposed Compression Mechanism Equations used

\[ R_{ij} = \frac{R_{ij}}{R_{ij} + G_{ij} + B_{ij}} \]  
\[ G_{ij} = \frac{G_{ij}}{R_{ij} + G_{ij} + B_{ij}} \]  
\[ B_{ij} = \frac{B_{ij}}{R_{ij} + G_{ij} + B_{ij}} \]  

\[ M_{rr} = \frac{1}{m^2} \sum_{i=L_x}^{m+L_x} \sum_{i=L_y}^{m+L_y} R_{ij} \]  
\[ M_{gg} = \frac{1}{m^2} \sum_{i=L_x}^{m+L_x} \sum_{i=L_y}^{m+L_y} G_{ij} \]  
\[ M_{bb} = \frac{1}{m^2} \sum_{i=L_x}^{m+L_x} \sum_{i=L_y}^{m+L_y} B_{ij} \]  

\[ V_{rr} = \frac{1}{m^2} \sum_{i=L_x}^{m+L_x} \sum_{i=L_y}^{m+L_y} \left| R_{ij} - M_{rr} \right| \]  
\[ V_{gg} = \frac{1}{m^2} \sum_{i=L_x}^{m+L_x} \sum_{i=L_y}^{m+L_y} \left| G_{ij} - M_{gg} \right| \]  
\[ V_{bb} = \frac{1}{m^2} \sum_{i=L_x}^{m+L_x} \sum_{i=L_y}^{m+L_y} \left| B_{ij} - M_{bb} \right| \]  

\[ V_{rr} \leq \text{tolerance and } V_{gg} \leq \text{tolerance and } V_{bb} \leq \text{tolerance} \]  

\[ S_{ij} = R_{ij} R_{ij} + G_{ij} G_{ij} + B_{ij} B_{ij} \]
● Firstly we have separated the image into non-overlapping range blocks of seven pixels

● Defined the overlapping domain blocks of seven times more in general, i.e. 49 pixels or 343 pixels

● Each pixel in the image can be the centre of domain block

● To reduce the computational complexity, we only searched for up to 343 domain blocks, which are around each range block
1. Use the fractal decoding algorithm and the second part of compressed image to decode image $S''$.

2. By using first part of compressed image and equation (5) to get $R_{ij}''$, $G_{ij}''$, and $B_{ij}''$ where

$$R_{ij}'' \approx R_{ij}, G_{ij}'' \approx G_{ij}, B_{ij}'' \approx B_{ij}$$

3. $R_{ij}''$, $G_{ij}''$, and $B_{ij}''$ are used to reconstruct image $CI'(spiral)$

$$CI \approx CI'$$

Where

$$S_{ij} = R_{ij} RR_{ij} + G_{ij} GG_{ij} + B_{ij} BB_{ij} \quad (5)$$
Experiments are carried out on different images with the tolerance values 0.01 to 0.05.
Experimental Results

Tolerance=0.01
Experimental Results

Tolerance = 0.02
Experimental Results Decompressed Images
Conclusion and Future Scope

- As the tolerance value increases, the compression ratio increases with little trade off in image quality.

- Depending on the color image database domain and the requirement of compression ratio and image quality, one can select the relevant tolerance value.

- For the natural images, one can select the higher tolerance value and for the indoor images, lower tolerance value.

- In proposed approach one-plane image is represented in Spiral Architecture which gives the one dimensional representation due to the spiral multiplication.

- Presently we have considered that individual pixel as the hexagonal pixel. Proposed mechanism can become robust, once it is possible to represent the whole composite one plane image in spiral architecture. For this purpose, we may have to use the sub sampling so that we can able to mimic the spiral architecture on square architecture for whole image.

- Stream ciphers can be used for encryption or partial encryption can be possible by encrypting some typical parameters.


• Access control system for the MAC/packet family: EUROCRYPT. European Standard EN 50094, CENELEC (European Committee for Electrotechnical Standardization), December 1992.


References

- R. Hamzaoui, M. Muller and D. Saupe, "Enhancing fractal image compression with Vector Quantization", DSPWS, 1996.
References

Thank You.....