Simultaneous Color Image Compression and Encryption using Number Theory

Vikram Jagannathan[1], R. Hariharan[1], Aparna Mahadevan[1] and **E. Srinivasan[2]**

[1]Final Year, B. Tech, [2]Assistant Professor
Electronics and Communication Engineering, Pondicherry Engineering College
Email:vikkyjagan@gmail.com

Abstract

The dependence on computing machines and utility of information has been growing tremendously in the last few decades. As a result, evolving effective techniques for storing and transmitting the ever increasing volumes of data has become a high priority issue. Image compression addresses the problem by reducing the amount of data required to represent a digital image. The underlying basis of the compression process is the removal of redundant data. Selection of a suitable compression scheme for a given application depends on the available memory for processing, the number of mathematical computations and the available bandwidth for transmission.

The security of digital images is another important issue that has been receiving considerable attention in the recent past. Different image encryption methods have been proposed in the literature towards ensuring the security of data .The encryption process transforms a 2-D pixel array into a statistically uncorrelated data set. In this paper, an enhanced number theory based color image compression and encryption scheme is proposed. This technique encompasses the twin-based application of image compression and image encryption simultaneously adopting a model based paradigm for the general compression-encryption standards.

1. INTRODUCTION

Images form the significant part of data, particularly in remote sensing, biomedical and video conferencing applications [1]. The use of and dependence on information and computers continue to grow, so too does our need for efficient ways of storing and transmitting large amounts of data. For example, someone with a web page or online catalog that uses dozens or perhaps hundreds of images will certainly need to use some form of image compression to store those images. This is because the amount of space required to hold unadulterated images can be prohibitively large in terms of cost. Fortunately, there are several methods of image compression available today [2]. However, the digital pictures require far more computer memory and transmission time than that needed for plain text. For real time applications, in order to handle huge amount of data, the image compression schemes are needed.

Image compression is a process intended to yield a compact representation of an image, thereby reducing the image storage / transmission requirements. Generally, data compression is of two types: reversible compression (lossless) and non-reversible (lossy) compression. Reversible compression

results in a reduction of redundant data, but the reduction is in such a way that redundancy can be subsequently restored into the data. Non-reversible compression results in the reduction of information itself in which the lost information can never be recovered. The non-reversible scheme provides more compression than its reversible counterpart [3].

2. COMPRESSION TECHNIQUES

In real time, such as on-board processing, the resources are severely restricted both in available bandwidth and memory. For such applications, commonly used compression techniques for images have their own limitations.

In most widely known reversible coding, such as the Huffman Code, if the color level values are large, the design of the Huffman Code is quite complex, since it involves large processing to obtain all statistics and the compression achieved is very less. While scalar predictive schemes such as Differential Pulse Code Modulation (DPCM) are simple to implement, the redundancy reduction capability is not good compared to other coding techniques. For the same image quality, DPCM usually requires a higher bit rate and is more vulnerable to channel error [4-6].

In block coding schemes such as Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT), Vector Quantization (VQ), Block Truncation Coding (BTC), either the compression ratio is high and the coding is complex (DWT, DCT, VQ) or the compression ratio is modest and the coding is also moderate (BTC) [7-8]. The number of operations (multiplication) for two–dimensional block coding schemes such as the Discrete Cosine Transform requires $N^2 \log_2 N$ computations to code an image block size of $N \times N$. Moreover the choice of block size is a trade-off between the compression efficiency and image quality. If the block size becomes too large, degradation effects such as ringing and blocking effects are introduced, especially in blocks containing high-contrast edges [9].

For Vector Quantization, the number of operations required is $K^2 \times N$ for coding the same $N \times N$ block, where K is the number of code words. Moreover Vector Quantization yields a better image quality only when the bit rate is lower [10]. Thus, popular block coding schemes are suitable only for specific applications where the processing power is adequate or where dedicated hardware may be used. However, most of the real time applications such as on-board processing constraints make it almost infeasible to use orthogonal transform coders or Vector Quantization coders.

Color images require significantly more storage, bandwidth and transmission time than grayscale images. Hence, it is essential to develop a new coding technique which will have features of block size depending on the statistics of the image, minimum rate of distortion, more coding benefits and less system complexity [11]. In the following section, we implement such a scheme, namely number theory based image compression and encryption, which is suitable for on-board applications as well as ground applications.

3. NUMBER THEORY BASED IMAGE COMPRESSION

The following scheme is based on the number theoretic and the JPEG (Joint Picture Experts Group) standards [6]. In this method, the image is represented in the form of a square matrix of size 256×256, 512×512, 1024×1024 and so on. Color images are comprised of three spaces: red, green and blue. In color image coding applications each space is compressed separately as in the grey scale image. Each pixel is of 8 bits and the amplitude value varies from 0 to 255. The image coding system

based on the Number Theory is carried out by the following procedure. An image of size N × N is taken and is fragmented into blocks of size 1 x K. Each pixel in the block is represented with a smaller bit representation by dividing by 16.

$$ai = bi / 16, i = 1 \text{ to } K \quad (1)$$

Now, they are represented as linear congruencies

$$yi = ai \pmod{ni} \quad (2)$$

for some fixed integer ni. The congruencies are solved using the number theoretic paradigm. The common solution for a system of linear congruencies is obtained using the method of Chinese Remainder Theorem.

4. CHINESE REMAINDER THEOREM

The Chinese Remainder Theorem is mainly based on the algorithm of linear congruencies. Congruence is nothing more than a statement about divisibility [12]. The Chinese Remainder Theorem is mainly based on the system of linear congruencies a = b (mod n) which can be reduced to a set of a = b (mod ni), where n1, n2, … ni are prime factors of n.

4.1 Theorem

Let n1, n2, . . . , nk denote k positive integers which are relatively prime, and let a1,a2, . . . , ak denote any k integers. Then the congruencies x = ai (mod ni), i = 1, 2. . . k have common solutions. Any two solutions are congruent modulo n1, n2. . . nk.

$$Y = X \pmod{P} \text{ where } P = n1 * n2 * \ldots * nk. \quad (3)$$

$$X = (a1*N1*x1) + \ldots + (ak*Nk*xk) \pmod{P} \quad (4)$$

$$\text{i.e. } X = \sum ai*Ni*xi \text{ (Mod P)} \quad (5)$$

where Nk = P / nk in which xk satisfies

$$Ni*xi = 1 \pmod{ni}$$

The remainder of the solved congruencies X is transmitted. At the receiving end, using X, ai are found using ai = X (mod ni) and then multiplying by16, the original pixel values are reconstructed.

4.2 Numerical Example

Let n (1) = 17, n (2) = 18, n (3) = 19 & n (4) = 23 which are relatively prime.

Let a (1) = 11, a (2) = 12, a (3) = 13 & a (4) = 15

Encryption:

P = 133722
N1 = 7866, N2 = 7429,
N3 = 7038 and N4 = 5814;
x1 = 10, x2 = 7, x3 = 12 and x4 = 9
X = 29064

Decryption:
al (1) = 11, al (2) = 12, al (3) = 13, al (4) = 15.

5. IMAGE ENCODING

Consider an image of size N × N. Various blocks of K pixels are taken, divided by 16 and then linear congruencies are applied to it. These congruencies are solved using the Chinese Remainder Theorem. The remainder of the solved congruencies X is obtained using the equation

$$X = \sum ai \times Ni \times xi \pmod{P} \quad (6)$$

Where Ni and xi are pre-calculated coefficients and ai are the pixel values after applying the threshold. The Ni and xi are pre-calculated and they need not be calculated for every X.

The reason for using Chinese Remainder Theorem for solving the linear congruencies is to reduce a bigger number to a smaller representation. For image of size 256 × 256 and block size 4, all 16384 X are computed. After computing all X, the frequency of each distinct X and their counts are determined. They are sorted in descending order of their count. A table of unique X and an equivalent smaller code is generated. Using this table each X obtained is encoded into this smaller code.

6. IMAGE DECODING

Image decoding is performed at the receiving end. At the receiver, ai are found for each X using the equation

$$ai = X \pmod{ni}. \quad (7)$$

The original pixel values are then reconstructed using the formula

$$Rpi = (ai \times 16) + Q, \; i = 1 \text{ to } K. \quad (8)$$

Where,
Rpi = reconstructed pixel
T = Threshold
Q = quality factor

This decoding technique has zero latency. It starts emitting decompressed text immediately after receiving the first code word, emitting K output characters for every compressed code word.

6.1 Compression Modes

This number theory based compression technique works as a lossy as well as lossless scheme. In the lossy mode, a negligible error is obtained with more compression.

For the lossless mode of compression, two sets of congruencies are considered. In the first step**,** the individual color values are divided by 16 and the quotients are represented as linear congruencies and solved using Chinese Remainder Theorem. In the second set, the original color values are divided by 16 and their remainders are taken. The solutions thus arrived at by applying the Chinese Remainder Theorem to these remainders are also transmitted. The compression ratio achieved for a block size of 1 x 10 is 3.88 : 1.

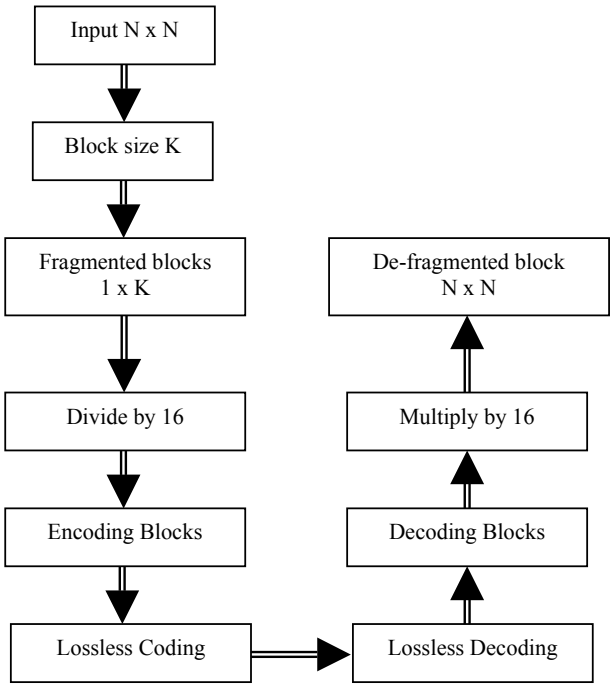

Fig. 1: Flow Diagram of the Image Compression and Encryption Scheme

7. IMAGE ENCRYPTION

This number theory based technique is applicable for encryption application by suitable selection of ni. This process provides image compression while encryption provides security. The encryption of the image is carried out using Chinese Remainder theorem.

For a good encryption/decryption scheme the receiver must faithfully decrypt the encrypted message using the key [13]. In the proposed scheme, the encryption level mainly depends on the combinations of ni. During decoding**,** the same combination of ni, which was selected for encoding should be applied correctly. The proposed scheme is very easy to adopt as the computational and number crunching steps are very small compared to other methods.

8. SIMULATION RESULTS

The picture used for simulation is shown in Fig. 2. It is the original Lena picture of size 260 × 260. Fig. 3 is the lossless decompressed Lena picture with block size 10 and the compression ratio is 3.88:1. Fig. 4 is the lossy decompressed Lena picture with block size 10. The compression ratio obtained is 16:1. Fig. 5 is the decompressed Lena using improper key. The software portion of this scheme was developed and tested using MATLAB for low and high dimensional images. The results are tabulated in Table 1.

Fig. 2: Original Lena image

Fig. 3: Decompressed Lena image Lossless (3.88:1)

Fig. 4: Decompressed Lena image Lossy (16:1)

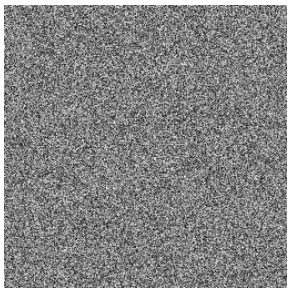

Fig. 5: Decompressed Lena using improper key

The Peak Signal to Noise Ratio (PSNR) obtained is moderate. The expression used for PSNR calculation is

$$RMSE = \sqrt{(\sum (P_i - R_i)^2 / N}\ ),\ i = 1 \text{ to } N$$

$$PSNR = 20 * \log_{10} [255/RMSE]$$

Where,

Pi = the pixel values for the original image
Ri = the pixel values for the decompressed image
N = number of pixels in the image.

- ICENT: Image Compression and Encryption using Number Theory (Proposed Scheme)
- VQ: Vector Quantization
- CR: Compression Ratio
- PSNR: Peak Signal-to-Noise Ratio

The image quality and compression obtained using ICENT is comparable to JPEG standards [14]. Further, the security of the image is enhanced by means of encryption which is obtained along with the compression. For an image size of N x N, in the proposed scheme (ICENT) the number of computational steps are N^2 / K where K is the block size.

Table 1: Comparison of various image compression techniques

CR	JPEG PSNR (dB)	JPEG2000 PSNR (dB)	VQ PSNR (dB)	ICENT PSNR (dB)
80	17.96	29.98	18.12	23.75
53.33	24.77	31.74	25.31	28.16
32	30.41	34.13	26.57	32.69
16	34.75	37.33	27.46	36.42
8	37.80	40.93	-	38.58
4	41.05	44.93	-	42.39

9. CONCLUSION

The scheme presented in this paper has simple implementation module. It also does the two-dimensional encoding operation with limited time by having less multiplication and very few arithmetic calculations. In this paper**,** for compression purpose**,** the block size (1×K) taken is 1× 10. Depending on the amount of compression and quality requirement, a large block size can be considered.

10. REFERENCES

[1] S.Wong, L. Zaremba, D. Gooden, and H. K. Huang, Feb. 1995, "Radiologic Image Compression—A review," Proc. IEEE, vol. 83, pp. 194–219

[2] A. K. Jain, "Image Data Compression: A review", 1981, Proc. IEEE, vol. 69, pp. 349–389

[3] Vinoly Seromony, "Image Encryption and Compression using Number Theoretic Paradigm", 2003, GSPx Conference, April

[4] Kenneth, R. C., "Digital Image Processing", 1996, Prentice-Hall International, Inc.

[5] Kou, Weidong, "Digital Image Compression: Algorithms", 1995, Kluwer Academics

[6] Veldhuis & Breeuwer, "An introduction to Source Coding", 1993, Prentice-Hall International, Inc.

[7] N. Ahmed, T. Natarajan, and K.R. Rao, "Discrete cosine transform", 1974, IEEE Trans. on Computers, vol. 23, pp. 90-93

[8] W.B. Pennebaker, J. Mitchell, "JPEG Still Image Compression Standard", 1993, New York: Van Nostrand Reinhold

[9] G.K. Wallace, "The JPEG still picture compression standard", 1991, Communication ACM, vol. 34, pp.31- 44

[10] N.M. Nasrabadi and R.A. King, "Image coding using vector quantization: a review", 1988, IEEE Trans. on Communications, vol. 36, pp. 957-571

[11] Murat, A. Tekalp, "Digital Video Processing", 1995, Prentice-Hall International, Inc.

[12] Ivan Nivan, Herbert S Zuckerman, "An Introduction to the Theory of Numbers", 1989, Wiley Eastern Limited

[13] Evangelos Kranakis, "Primality and Cryptography", 1986, Wiley - Teubner Series

[14] J. Modayil, H. Cheng, and X. Li, "Experiments in simple one-dimensional lossy image compression schemes," 1997, Proc. IEEE Multimedia Computer Sysems, pp. 614–615