Number Theory Based Color Image Compression and Encryption

Jackson Formiga

Plant High School (FL, USA)

ABSTRACT

This paper highlights the security of digital images based on number theory which tends to get immense attention in recent past. Encryption process produce statistically manipulated data from a two dimensional pixel array. In this paper, an enhanced number theory based color image compression and encryption scheme is proposed. This technique embraces a twin-based application of image encryption and compression concurrently accepting a model based example for the general compression-encryption standards.

INTRODUCTION

Modern era demands the efficient ways of storing and transmitting large amounts of data, most of social networking giants need to maintain a large number of images to store users data, an efficient image compression and encryption algorithm is a must need for them.

Image compression anticipated to gather the concrete data from image and exclude the unnecessary pixels while storing the data [1] Data compression can be used in two possible flavors loss less compression and lossy compression. Lossless compression removes the un-necessary data in such a way that while decompression the lost pixels can be easily predictable [2]. While lossy compression results in the reduced data can never be recovered and lossy scheme provide more compression as compare to lossless scheme [3].

Purpose and Research Problem

Recently published techniques certainly have their own limitations in-terms of bandwidth and memory, the most commonly lossless technique is Huffman Coding, which turn out be quite complex when we have color level values quite large, and secondly the compression level is quite low. Whereas predictive schemes are widely used to achieve data compression task, one of them is Differential Pulse Code Modulation (DPCM), the redundancy reduction scheme does not seems to be robust if compared to other coding techniques also for same quality images, it normally demands extensive bit rate and is more vulnerable to channel error but despite all these facts it is fairly easy to implement [4-6].

In block coding structures such as Block Truncation Coding (BTC), Discrete Cosine Transform(DCT), Vector Quantization (VQ), Discrete Wavelet Transform (DWT), either the compression ratio is high and the coding is complexor the compression ratio is diffident and the coding is also moderate [7-8]. The number of operations (multiplication) for two–dimensional block coding schemes such as the Discrete Cosine Transform requires N2log2N computations to code animage block size of N × N. Whereas RGB Color images are based on normally 3-4 layers and they obviously demands more storage and processing time than grayscale images. Indeed, to assure the fast transfer rate of multilayer images it is important 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].

Number Theory Based Image Compression

Images are normally represented in the form of a 2-D array whereas color images are consisting of three layers: blue, green and red. Each layer of color image is compressed separately as in gray scale image. Further each pixel is of 8 bits its intensity values are ranges 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.

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

Now, they are represented as linear congruencies

$$yi = ai \pmod{ni}$$

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 [12].

Number theory based compression techniques has the ability to works as a lossy and lossless structure. In lossy mode, minor error is attained with more compression.

In lossless scheme of compression, two sets of congruencies are considered. Each color values are (1) separately divided by an even number (we used 16) and further quotients are represented as linear congruencies and resolved by applying Chinese Remainder Theorem. Secondly, for original color values remainders were recorded after dividing the 16. The solutions reached at by applying the Chinese Remainder(2) Theorem to these remainders are also transmitted. The compression ratio achieved for a block size of 1 x 10 is 3.88 : 1.

In efficient encryption/decryption scheme the receiver should decrypt back the encrypted message using [9]. In proposed scheme, encryption level mainly depends on the combinations of ni. While decoding, the same combination of ni, which was selected for encoding should be asserted properly. The proposed scheme is very easy to adopt as the computational and numbe rrunching steps are very small compared to other methods.

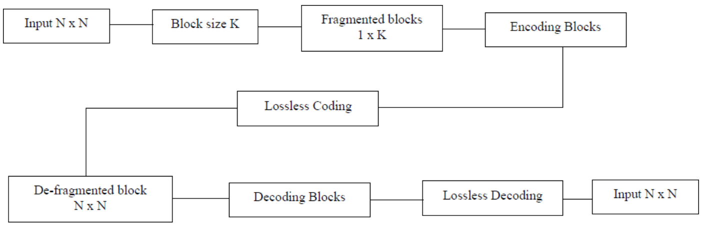

Figure 1. Image compression and encryption

Simulation

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

$$RMSE = \sqrt{(\Sigma (Pi-Ri)2/N)}, i = 1 \text{ to } N$$

$$PSNR = 20 * \log10 [255/RMSE]$$

Where,

Pi = pixel values from original image

Ri = pixel values from decompressed image

N = number of pixels in the image.

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.

REFERENCES

1. Ahmet, N., Nataraian, T., & Rao, K. (1974). Discrete cosine transform. IEEE. Trans on Computers, 23, 90-93.
2. Jain, A. (1981). Image data compression: A review. Proc. IEEE, 69, 349-389.
3. Kenneth, R. (1996). Digital image processing. Prenticce-Hall International Inc.
4. Murat, A. (1995). Digital Video Processing. Prentice-Hall International, Inc.
5. Nasrabadi, N., & King, R. (1988). Image coding using vector quantization: A review. IEEETrans on Communications, 36, 957-571.
6. Nivan, I., & Zuckerman, H. (1989). An Introduction to the Theory of Numbers. Wiley Eastern Limited.
7. Pennebaker, W., & Mitchell, J. (1993). JPEG still image compression standard. New York: VanNostrand Reinhold.
8. Seromony, V. (2003). Image encryption and compression using number theoretic paradigm. Conference.
9. Veldhuis, & Breeuwer. (1993). An introduction to source coding. Prentice-Hall International Inc.
10. Wallace, G. (1991). The JPEG still picture compression standard. Communication ACM, 34, 31-44.
11. Weidong, K. (1995). Digital image compression: Algorithms. Kluwer Academics.
12. Wong, S., Zaremba, L., Gooden, D., & Huang, H. (1995). Radiologic image compression: A review. Proc. IEEE, 83, 194-219.