Design of Secure Image Transmission In MANET using Number Theory Based Image Compression and Quasigroup Encryption (NTICQE) Algorithm

Munivel E[1] and Rajeswari Mukesh[2]

[1]Easwari Engg. College, Chennai-89, TN, India
[2]Assistant Professor, Easwari Engg. College, Chennai-89, TN, India

Abstract: Image compression and image encryption are pivotal to proper storage and transmission of images over MANET. Simultaneous image compression and encryption aims at achieving enhanced bandwidth utilization and security at the same time. The Number Theory based Image Compression and Quasigroup Encryption (NTICQE) algorithm employs number theoretic paradigm - Chinese Remainder Theorem and Quasigroup Encryption, to solve congruencies and hence realize the twin ideals of compression and encryption simultaneously. Quasigroup encryptor that has very good data-scrambling properties and, therefore, it has potential uses in symmetric cryptography.

Keywords: Quasigroup, Encryption, Decryption, Threshold, Chinese Remainder Theorem (CRT).

1. Introduction

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.

Images play a pivotal role in several applications like remote sensing, biomedical, video conferencing. Interest in digital image processing methods stems from the following principal application areas: improvement of pictorial information for human interpretation; and processing of image data for storage and transmission for machine perception. Whenever an image has to be transmitted, two significant issues need to be addressed. One is to accommodate the image within the allotted bandwidth and the other is to ensure secure transmission of images.

The NTICQE algorithm has been implemented on color images. The image coding results, calculated from actual image size and encoded image file, are comparable to the results obtained through much more sophisticated and computationally complex methods.

Image compression [2] and image encryption [1] are two fundamental image processing techniques extensively used towards meeting the requirement of efficient utilization of bandwidth and security. Currently, the need to develop a new coding technique which will have the features of coding benefits depending on the statistics of the image, inbuilt encryption module to enable secure transmission and less system complexity has been technique is an attempt to provide a remedy for both the bandwidth utilization and the encryption problems at the same time.

2. Architectural Design

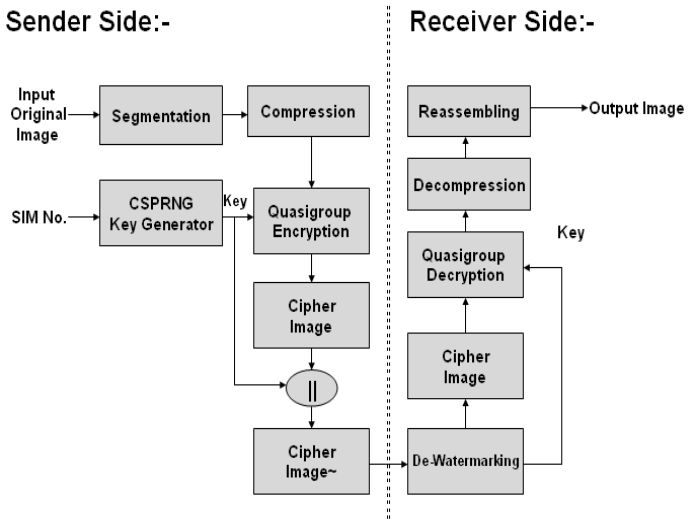

Fig. 1 Block Diagram

The schematic block diagram of the NTICQE scheme is shown in Fig. 1. When conventional algorithms are used, the image compression, and image encryption [1] modules are generally distinct. This at times increases the process time considerably or reduces the level of security.

This problem is addressed by the use of simultaneous image compression and image encryption [2] employing the proposed NTICQE algorithm, where both the transmitter block and the receiver block attain the twin ideals in the same module.In this paper, the concept of NTICQE has been described for color images, in lossless mode of compression [2], with enhancement of the compression ratio and encryption level.

3. Segmentation and Compression

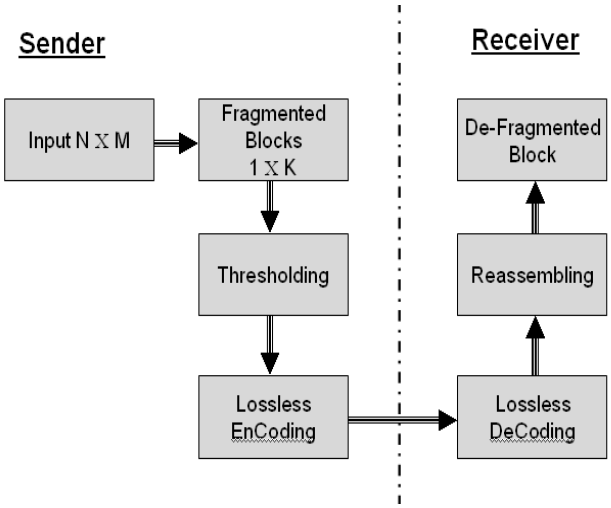

Fig.2 Segmentation and Compression

The CRT [2] solves the system of linear congruencies

a=b (mod n), reducing it to a set of

a=b (mod ni), where ni, n2 ... ni are prime factors of n. This principle of the CRT is used in the NTICQE algorithm.

3.1 Flow Diagram

The flow diagram of the NTICQE based image coding system is shown in Fig. 2.

3.2.Algorithm Description

The images are generally represented in the form of N x M matrix. In color image coding applications the color spaces, namely red, green and blue in 24 bits per pixel (bpp) RGB scale of 8 bpp each are compressed separately as in the gray scale image.

An image of size N x M is taken and is fragmented into blocks of size 1 x K. Each pixel r[i] in the block is divided by 16 to produce two half pixels of 4 bits each. This process is called thresholding [2].

a[i] = r[i] /16, i = i to K

a'[i] = r[i] mod 16, i = i to K.

Thus the input image is considered as a sequence of half pixels a[l,2,...K], a'[1,2,...KX] and the key sequence is a set of relatively prime numbers given by

n[l,2.,K] > a[i] and a'[i].

Image: a[1, ..., K], a'[1, ..., K] -> block of half pixels

Key: n[1,..., K] -> set of relatively prime integers

Now the Coefficients of the CRT are calculated by generating N for each key value using P, where P is the product of all the keys

$N[i] = P / n[i]$ where $P = \prod n[i]$.

Now the linear congruencies are generated by using the equation

$N[i] * x[i] = 1 \pmod{n[i]}$ where x[i] satisfies the above congruency and $C[i] = N[i] * x[i]$.

These stages are carried on prior to transmission, the values of C[i] can be generated once the key is decided; hence they are calculated and stored in the system to be used during transmission. For the transmission of the image, the value of TR is determined for each block of K half pixel values as follows.

$TR = \sum C[i] * a[i] * (\text{Mod } P)$-Cipher Text (quotient)

$TR' = \sum C[i] * a'[i] * (\text{Mod } P)$-Cipher Text (remainder)

For K half pixel values, one TR and TR' value is transmitted providing compression; moreover, this value is dependent on the key used which incorporates encryption.

This is the most vital step of the algorithm as it ensures simultaneous encryption and compression [2].At the receiving end, the K half pixel values are generated from the single value TR and TR'.

ar[i] = TR (mod n[i])-Plain Text (quotient)

ar'fi] =TR' (mod n[i])-Plain Text (remainder)

The pixels are then reconstructed from the half pixels as

s[i] = ar[i] * 16 + ar'[i]

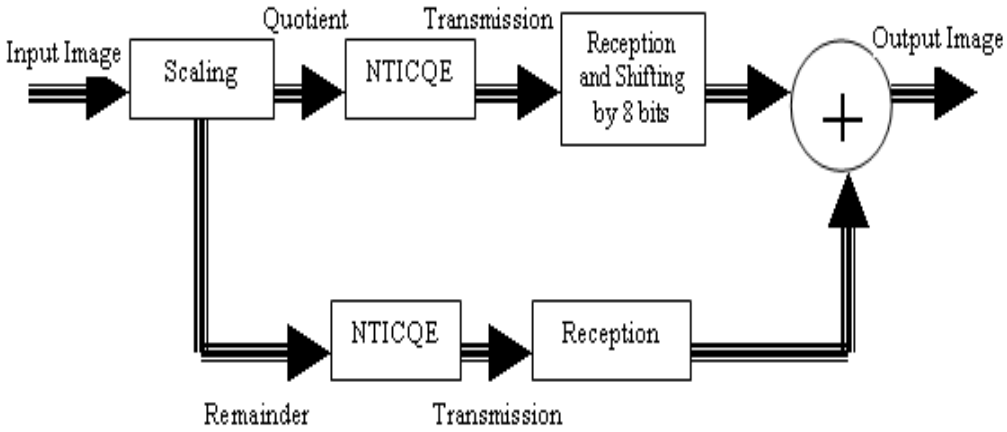

Fig. 3 Lossless transmission and reception

3.3 Image Encoding and Decoding

As explained in the previous section, the encoded image, to be transmitted, is given by

TR = E C[i] * a[i] (Mod P)

Where C[i] are pre-calculated coefficient and a[i] are the pixel values after applying the threshold. Since C[i] are pre-calculated, they need not be calculated for every TR.

The reason for using Chinese Remainder Theorem [2] for solving the linear congruencies is to reduce a bigger number to a smaller representation.

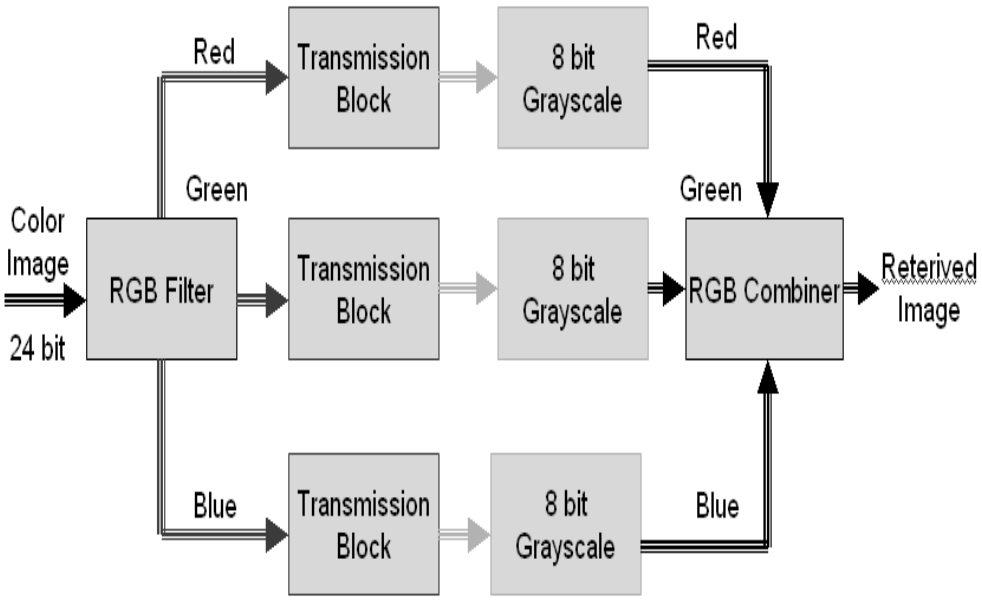

Fig. 4. Color Image Transmission

For image of size N x M and block size K, all (N x M)/K TR are computed. After computing all TR, the frequency of each distinct TR and their counts are determined. They are sorted in descending order of their count and assigned new set of numbers.

A table of unique TR and an equivalent code is generated. Using this table each TR obtained is encoded into this new code. The same is followed for TR'. At the receiver, the same encoding table is used to recalculate the actual TR and TR' values from which the half pixel values ar[i] and ar'[i] and thus the reconstructed image pixels s[i] are determined.

In Fig. 3., the block diagram of lossless transmission and reception of a single color space is depicted and in Fig. 4., it extended to the complete color image.

3.4 Image Encryption

This Quasigroup Encryption [1] technique is pertinent for encryption application by suitable selection of n[i]. They are selected such that they are greater than the largest half pixel value in the image. For a good encryption/decryption scheme [1, 4], the receiver must faithfully decrypt the encrypted message using the key. In the proposed scheme, the encryption level mainly depends on the combinations of n[i].

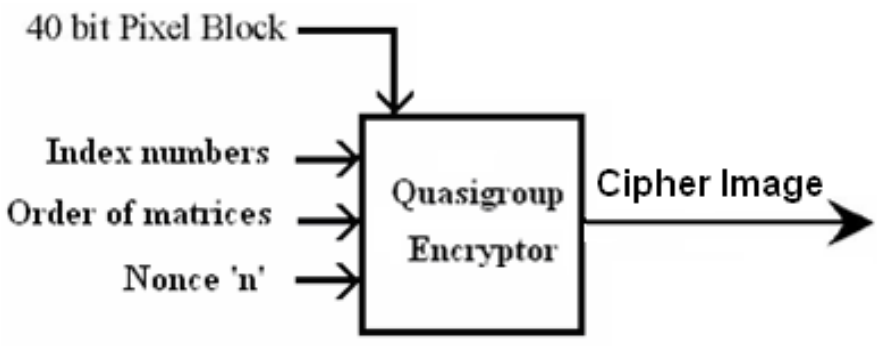

Fig. 5. Encryption Model

Consider a block size of 10 pixels each of 4 bits in length. Here, a sequence of 10 keys each 6 bits in length is employed. Then the maximum number of distinct key sequence '1' is factorial (10).

Decryption [1] is simply reverse method of Encryption. The 40 bit pixel block is operated with 60 bit key sequence to obtain an upto-60 bit cipher text block [1], which is transmitted as depicted in Fig. 5.

During decoding, the same combination of n[i], which was selected for encoding, should be applied correctly. The 60 maximum tryouts by an eavesdropper to crack the key is 2 The security can be further enhanced by scrambling [1, 2, 3, 4] the pixel blocks.

3.5 Implementation

The NTICQE algorithm has been implemented on MATLAB 7 for color images of size 260 x 260 and a key sequence of length 10. For the transmission of color images, the image is first filtered and red, green and blue components are separated. The algorithm is then applied to each of the color components separately and transmitted. At the receiving end, the three color components retrieved are combined in order to obtain the color image.

4. Chinese Remainder Theorem

The Chinese Remainder Theorem (CRT) [2] has been a useful tool in applications of number theory to other fields. The CRT is based on the solution of linear and modular congruencies [1, 2, 5]. Congruence is nothing more than a statement about divisibility.

4.1 Statement

Given a system of congruencies to different moduli:

x=a1 (mod ml), x=a2 (mod m2), . . ., x=ar (mod mr) and if each pair of moduli are relatively prime,

gcd (mi, mj) =1 for i .j, the system has exactly one common solution modulo M= ml * m2 * ... * mr and any two solutions are congruent to one another modulo M. The Chinese Remainder Theorem can be used to increase efficiency by making use of relatively small numbers in most of the calculation.

4.2 Merits of CRT

1. Increased efficiency in machine computation.
2. Reduced memory, and sophisticated hardware requirements.
3. Reduction in space requirement for storage of data because large numbers are converted into relatively smaller ones by solution of linear congruencies.
4. Use of simple arithmetic operations like addition, subtraction, multiplication, division and hence execution of Million Instructions Per Second (MIPS) is possible.
5. Faster computation process and hence reduction in processing time.
6. Widespread application in cryptography [1], secure transmission [1, 3, 5] of codes and signals in military and defense applications.

5. Results and Discussion

NTICQE in lossless compression [1,5,6] mode the simulation results have been obtained with MATLAB 7 on color images with different textures and patterns.

The test images used for this module are a 260 x 260 color Lena image [2], a 260 x 260 color Pepper image [2,3,4,5] and a 260 x 260 color GoldHill [2,3,5,5] image. These test images are in RGB - 24 bpp format. The length of the pixel sequence and the key sequence are taken as 10.

Fig. 6. Decompressed Lena Image
Lossless (1.85:1)

The lossless – decompressed [2] images with their corresponding compression ratios are tabulated in Table 1. and are compared with existing techniques of its class. The Lena image is compressed to 1.85 times its original size as in Fig.6. The Pepper and GoldHill are compressed to 1.91 and 2.02 times the original size as shown in Fig.7. and Fig.8.

Fig. 7. Decompressed Pepper Image
Lossless (1.91:1)

Fig. 8 Decompressed GoodHill Image
Lossless (2.02:1)

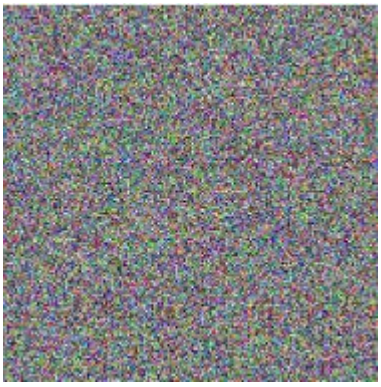

Fig. 9. Decompressed Pepper

Using Improper Key

Table 1: Comparative Study of the Compression Ratios for Various Lossless Compression Algorithms

Image / Algorithm	Lena (CR)	Pepper (CR)	GoldHill (CR)
JPEG-LS	2.26	2.06	2.04
JPEG2000	1.86	1.41	1.65
CALIC	2.33	1.73	1.74
SPIHT	1.91	-	1.70
FELICS	1.65	1.55	1.95
HUFFMAN	1.56	1.71	-
LWZ	1.18	1.36	-
NTICE	1.85	1.91	2.02

When the image is retrieved using an improper key, an unintelligible image is obtained as shown in Fig.9. This demonstrates the level of security provided by the encryption module present in the NTICQE algorithm.

6. Conclusion and Future Work

A technique for simultaneous image compression and image encryption [1,2] using number theoretic paradigm is developed. Two dimensional encoding operation performed by the proposed method is shown to be simple in terms of computational

complexity. The NTICQE algorithm is employed on color images and the encryption [1] and lossless compression [2,3,4] modes are studied. The amount of compression achieved for different images using the proposed method is comparable with that of the conventional methods and also high level of security is provided to the transmitted images.

7. Reference

[1] Maruti Venkat, Kartik Satti, July 2006 “A Quasigroup Based Cryptographic System”, International Journal of Network Security, Vol.7, No.1, pp. 15–24.

[2] Vikram Jagannathan, Aparna Mahadevan, Hariharan and Srinivasan, Feb.2007, “Number Theory Based Image Compression Encryption and Application to Image Multiplexing”, © 2007 IEEE - ICSCN, pp.59-64.

[3] Tiegang Gao, Zengqiang Chen, July 2007, “A New Image Encryption Algorithm Based on Hyper-Chaos”, © Elsevier, Physleta.2007.07.040.

[4] Xiao-Li Niu, Ju Liu, Jian-De Sun, and Jian-Ping Qiao, 2006, “A Novel Watermarking Method with Image Signature”, © Springer, pp. 293 – 298.

[5] Michael R. Peterson, Gary B. Lamont, Frank Moore, and Patrick Marshall, July 2006 “A Satellite Image Set for the Evolution of Image Transforms for Defense Applications”, © ACM GECCO’07, pp. 2901-2906.

[6] Chung-Ping Wu, C.-C. Jay Kuo, 2005 "Design of integrated multimedia compression and encryption systems", IEEE Transactions on Multimedia, vol.7, no. 5, pp. 828.