Journal of Applied Sciences Research, 8(1): 326-330, 2012
ISSN 1819-544X
This is a refereed journal and all articles are professionally screened and reviewed

ORIGINAL ARTICLES

Design and Simulation of Secure Communication System

Ahmed S. Hadi, Zaid A. Salman and Saleem M. Mohammed

University of Baghdad/ Al-Khwarizmi College of Eng.

ABSTRACT

In this paper a modified scheme that offers both encryption and compression will be presents. The proposed scheme is based on a randomized MQ –coder, where a chaotic sequence that act as the encryption key, will be used instead of the random number that used by standard MQ - coder. Furthermore, for reliable communications, Reed-Solomon code is proposed as channel coding for secure data transmission over the wireless channel.

Key words: Encryption, Compression, Randomized MQ –Coder, Chaotic Sequence, Reed-Solomon Code, and Wireless Channels.

Introduction

Data compression or source coding is the method of compression the data to smaller amount than an un-encoded representation, by using specific encoding schemes. The most important data compression techniques that are used currently are Huffman and Arithmetic Coding (Krishna BharathKolluru, 2009).

Arithmetic Coding is more efficient and more flexible from all the source codes, due to its efficiency when dealing with a huge data such as images. The third line in fig.1, shows that the arithmetic coding is work near optimality (Amir Said, 2004). Recently, arithmetic code is used in many image and video coding techniques, such as H.264, and JPEG2000. While the older versions of these techniques are encoded by using Huffman code. This replacement is due to the high compression ratio, flexibility, and optimality that the arithmetic code offers (G. Langdon and J. Rissanen, 1981; Hyungjin, Kim, 2007). The randomized MQ - coder will be used in this paper due to its effective way to compress multimedia contents (Marco Grangetto, 2006; S. Burrus, 1998).

This paper is organized as follows; in section two the theory of discrete wavelet transform (DWT), chaotic sequence, randomized MQ - coder, and Reed-Solomon code (RS) will be present. The proposed system with its results will be present in section three and four respectively. Finally section five will contains the conclusion.

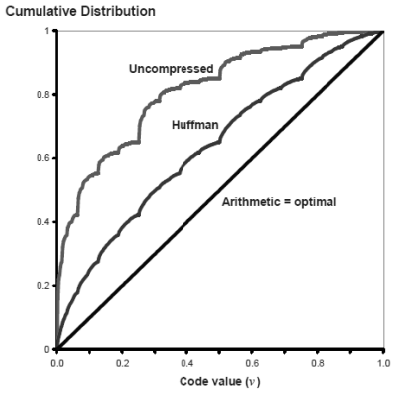


Fig. 1: Source Coding Compression (Amir Said, 2004).

2. The Theory of Discrete Wavelet Transform, Chaotic Sequence, Randomized MQ-Coder, and Reed Solomon Code:

2.1. Discrete Wavelet Transform (DWT) For 2-D Signal:

A 2-D DWT is equivalent to two one dimensional DWT in series. It's implemented as 1-D row transform followed by 1-D column transform on the data obtained from the row transform as shown in fig.2. Where h(n)

Corresponding Author: Ahmed S. Hadi, University of Baghdad/ Al-Khwarizmi College of Eng.
E-mail: ahmed sattar [ahmedsattar2002@gmail.com]

and g(n) are the low pass filter and high pass filter which splits the signal into two subspaces, the low pass filter generates the details of the signal (X_L) and the high pass filter generates the noise signal (X_H). X_{LL}, X_{HL}, X_{LH}, and X_{HH} are the details-sub signal, noise detail sub signal, detail noise sub signal and noise sub signal respectively (S. Burrus, 1998).

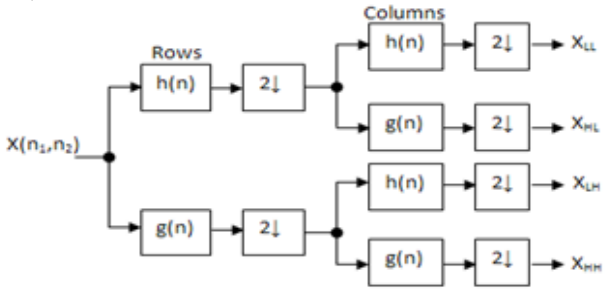
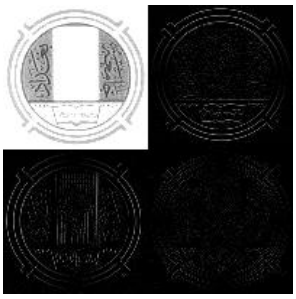


Fig. 2: One Level Filter Bank for Computation of 2-D DWT.

An example for implementing the 2-D DWT Haar type is shown in fig. 3. Fig.3.band fig. 3.c shows the one and the two level 2-D DWT respectively for the original image shown in fig. 3.a.

(a) Original Image.



(b) One Level 2-D DWT.

(c) 2-DTwo Level DWT.

Fig. 3: 2-D DWT for One and Two Levels.

Chaotic Sequence:

The chaotic sequence depends on the initial condition where a two sequence with closely initial condition will give different sequence. So that the initial condition of the chaotic sequence represents the key of encryption in crypto system. The logistic map is defined as:

$$X(n+1) = r.X(n).mod(q)$$

$$n = 0, 1, \ldots, x_0 \epsilon [0, q], \qquad r = \frac{p}{q} > 1, \qquad and\ p\ is\ a\ co-prime\ to\ q.$$

The map is chaotic for all r and has lyapunov exponent $\lambda = log\ r\ > 0$ (Hongxia Wang, 2008).

2.2. Randomized MQ-Coder (Marco Grangetto, 2006):

The randomized MQ-coder is based on the definition of the two alternative interval conventions shown in Fig. 4. The standard MQ-coder assumes that the LPS interval precedes the MPS interval; the randomized MQ coder allows swapping these two intervals randomly (David Salomon, 2007; I.H. Witten, 1987).
For i = 0: N - 1
Draw a random number ri using the random generator;
Ifri = 1 then select the order [LPS, MPS]for encoding bitbi,
Otherwise select the order [MPS, LPS].

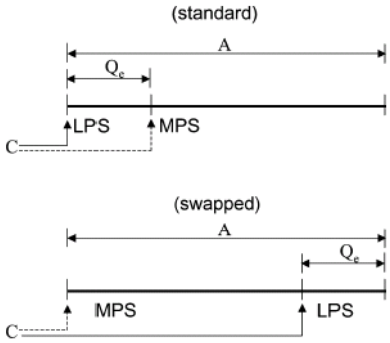


Fig. 4: MQ encoding intervals (Marco Grangetto, 2006).

2.4. Reed Solomon Code (RS) (Bernard Sklar, 2001):

Reed Solomon (RS) codes are systematic linear block codes specified as RS (*n, k*), with *m* bit symbols. This means that the encoder takes *k* data symbols of *m* bits each, appends *n - k* parity symbols, and produces a code word of n symbols (each of m bits) from the field GF (2^n).

The Reed Solomon decoder tries to correct errors and/or erasures by calculating the syndromes for each codeword. Based upon the syndromes the decoder is able to determine the number of errors in the received block. If there are errors present, the decoder tries to find the locations of the errors using the *Berlekamp-Massey algorithm* by creating an *errorlocator polynomial*. The roots of this polynomial are found using the *Chien search algorithm*. Using *Forney's algorithm*, the symbol error values are found and corrected. For an RS (*n,k*) code where *n-k = 2t*, the decoder can correct up to *t* symbol errors in the code word. Steps involved in decoding of RS codes are.

3.Proposed System Model:

Our proposed methodis to merge the compression and encryption blocks into one block, rather than two blocks (as shown fig.5 below),that proposed in (M Padmaja, 2007).

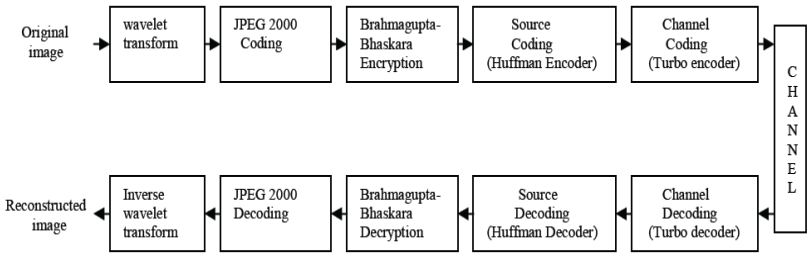


Fig. 5: Block diagram of the transmission and reception scheme proposed by (M Padmaja, 2007).

As shown in fig. 5, there is a block for encryption and another block for compression (source coding), in our system shown in fig. 6 below, the encryption and compression is merged into one block, which is the randomized MQ-Coder, that work as follows:

for i = 0: N - 1
generatea chaotic sequence*ri;*
ifri = 1 then select the order [LPS, MPS]for encoding bit bi,
otherwise select the order [MPS, LPS].

The chaotic sequencehere represents the encryption key. If encoder and decoder use the same initial S, then they will generate the same chaotic sequence, and be synchronized; on the contrary, if the correct initial is not available, the decoder will not be able to correctly decode the compressed data.Thus the randomized MQ-Coder with chaotic sequence will encrypt and compress the detailed coefficient result from 2D-DWT.

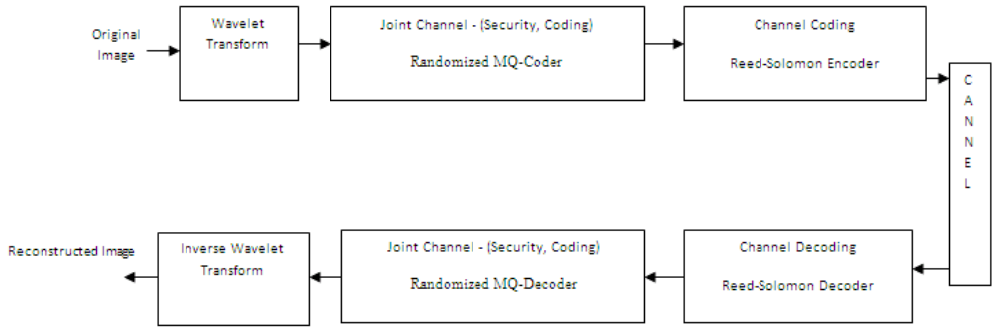


Fig. 6: Block diagram of the transmission and reception scheme.

According to (R. Logeshwaran, 2010); It founds that the standard version of RS codes such as RS(255,223,8) andRS(255,239,8) having less latency, gives good error correcting performance than the lower level codes, and also with optimal delay for WiMAX environment. Hence, we used the RS code versions RS(255,239,8) as a channel coding instead of turbo code.

Results:

Image in Fig. 7, is selected as image to get the wavelet coefficient as shown in fig. 8, then we took the detailedcoefficient(as shown in fig. 9), to transmit through the system stated in fig. 7, and received by randomize MQ-Coder with the correct initial of chaotic sequence, as shown in fig. 10, while the rubbish one received by normal MQ-Coder as shown in fig. 11.

Fig. 7: Original Image.

Fig. 8: Wavelet Coefficients.

Fig. 9: Transmitted Detailed Image.

Fig. 10: Received Image with Randomized MQ-Coder.

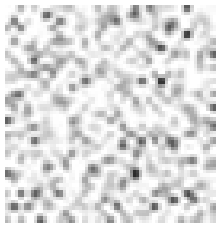


Fig. 11: Received Image with normal MQ-Coder.

Conclusion:

The system proposed in this paper aims to merge the Encryption and Source Coding in one Block called secure source coding to minimize the system complexity, We propose a modified MQ-Coder, based on chaotic sequence. We prefer a Reed-Solomon for use a channel coding instead of Turbo Coding which double or triple the size of data.

References

Amir Said, 2004. " Introduction to Arithmetic Coding - Theory and Practice ", Academic Press.

Bernard Sklar, 2001. "Digital Communications, Fundamentals and Applications", second edition, Prentice Hall.

Burrus, S., R.A. Gopinath and H. Guo, 1998. “Introduction to Wavelets and Wavelet Transforms”, Prentice hall.

David Salomon, 2007. "Data Compression, the complete reference", 4rt edition, Springer-Verlag, London Limited, 2007.

Hongxia Wang, Ke Ding, Changxing Liao, 2008. “Chaotic watermarking scheme for authentication of JPEG Images”, International Symposium onBiometrics and Security Technologies (ISBAST), pp: 1-4.

Hyungjin, Kim., Jiangtao Wen and John D. Villasenor, 2007. "Secure Arithmetic Coding", IEEE Transactions on Signal Processing, 55(5).

Krishna BharathKolluru, 2009. "Optimization of Arithmetic and MQ coding",ECE 734 VLSI Array Structures for Digital Signal Processing.

Langdon, G. and J. Rissanen, 1981. “Compression of black-white images witharithmetic coding,” IEEE Transactions on Communication, COM-29(6): 858-867.

Logeshwaran, R. and I. Joe Louis Paul, 2010. "Performance Study on the Suitability of Reed Solomon Codes in WiMAX", ICWCSC.

Marco Grangetto, Enrico Magli and Gabriella Olmo, 2006. "Multimedia Selective Encryption by Meansof Randomized Arithmetic Coding", IEEE Transactions on Multimedia, 8(5).

Padmaja, M., Syed Shameem, 2007. "Secure Image Transmission over Wireless Channels", International Conference on Computational Intelligence and Multimedia Applications.

Witten, I.H., R.M. Neal and J.G. Cleary, 1987. “Arithmetic Coding for Data Compression," Comm. ACM, 30 (6): 520.