Design and Simulation of Secure Communication System

Lecturer. Ahmed S. Hadi *Asst. Lecturer. Zaid Ali Salman*

Asst . Lecturer. Saleem M. Mohammed

Department of Information and Communication Engineering
Al-Khwarizmi College of Engineering
University of Baghdad

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.

تصميم ومحاكاة منظومة اتصالات آمنة

م.أحمد ستار هادي م.م.زيد علي سلمان م.م.سليم موله محمد

قسم هندسة المعلومات والاتصالات

كلية الهندسة الخوارزمي / جامعة بغداد

الخلاصة

في هذا البحث تم تقديم نظام يقوم بتشفير وضغط البيانات في نفس الوقت. وتستند الخطة المقترحة على نظام الترميز العشوائي MQ، حيث سيتم استخدام تسلسل الفوضى التي تكون بمثابة مفتاح التشفير، بدلا من الرقم العشوائي الذي يستخدمه نظام الترميز القياسي MQ. وعلاوة على ذلك تم اقتراح الريد سلمون (RS)، كمرمز قناة للاتصالات الموثوق بها وكمرمز لنقل البيانات الآمنة عبر القنوات اللاسلكية.

1. 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 **[1]**.

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 **Figure.(1)**, shows that the arithmetic coding is work near optimality [2]**.** 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 [3, 4]. The randomized MQ - coder will be used in this paper due to its effective way to compress multimedia contents [5, 6].

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.

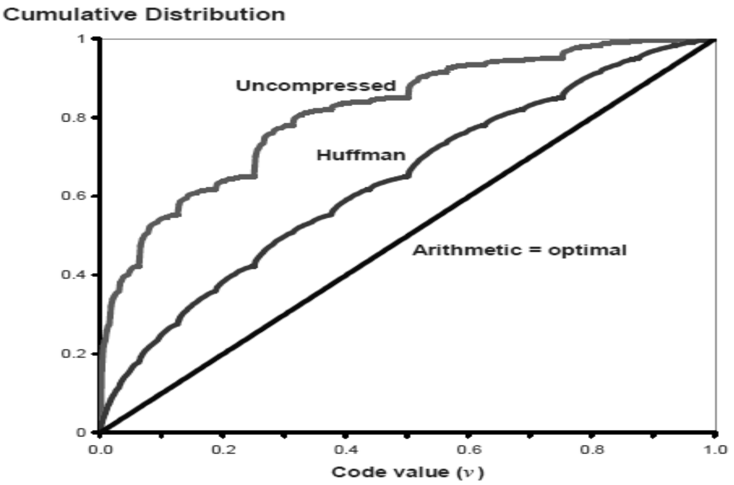


Fig .(1): Source Coding Compression [2].

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 **Figure.(2).** Where h(n) 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 [6].

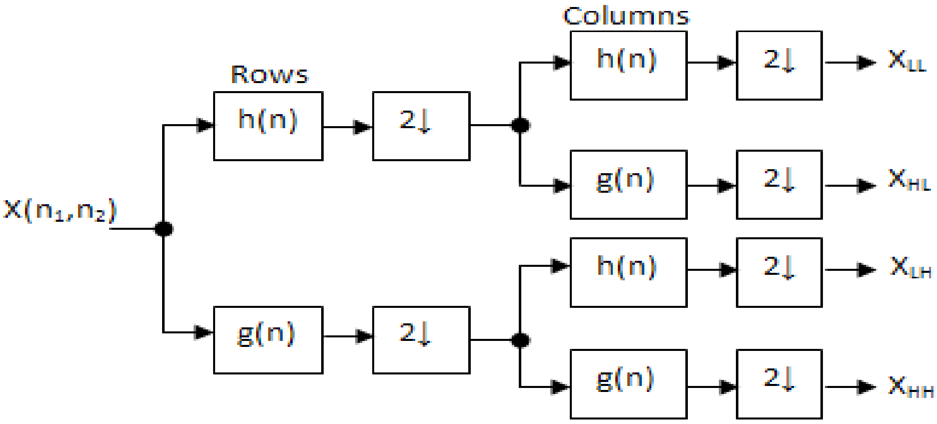
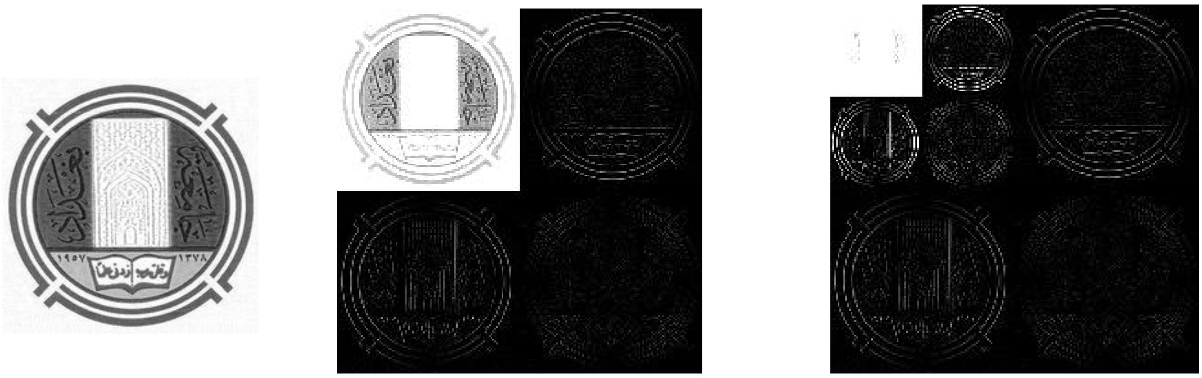


Fig .(2): One Level Filter Bank for Computation of 2-D DWT.

An example for implementing the 2-D DWT Haar type is shown in **Figure.(3.b)**.. **Figure.(3)**.and **Figure.(3.c)** shows the one and the two level 2-D DWT respectively for the original image shown in **Figure(.3.A).**



(a) Original Image. **(b) One Level 2-D DWT.** **(c) Two Level 2-D DWT**

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

2.2. 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. In this paper a chaotic sequence using logistics map will be used. The logistic map is defined as:

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

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

The map is chaotic for all r and has lyapunov exponent $\lambda = log\, r > 0$ [7].

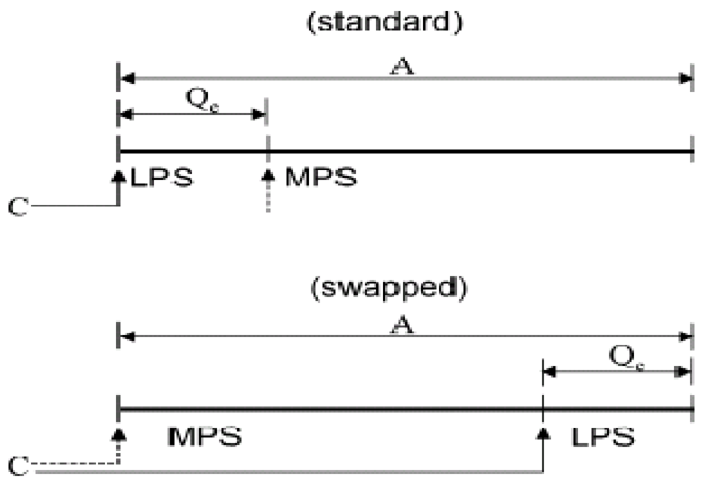


Fig .(4): MQ encoding intervals [5].

2.3. Randomized MQ-Coder [5]

The randomized MQ-coder is based on the definition of the two alternative interval conventions shown in **Figure.(4).** The standard MQ-coder assumes that the LPS interval precedes the MPS interval; while the randomized MQ coder allows swapping these two intervals randomly [8, 9] as follows:

For i = 0: N - 1
Draw a random number ri using the random generator;
If ri = 1 then select the order [LPS, MPS] for encoding bit bi,
Otherwise select the order [MPS, LPS].

2.4. Reed Solomon Code (RS) [10]

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 error locator 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.

3. Proposed System Model

Our proposed method is to merge the compression and encryption blocks into one block, rather than two blocks (as shown **Figure.(5)** below), that proposed in [11].

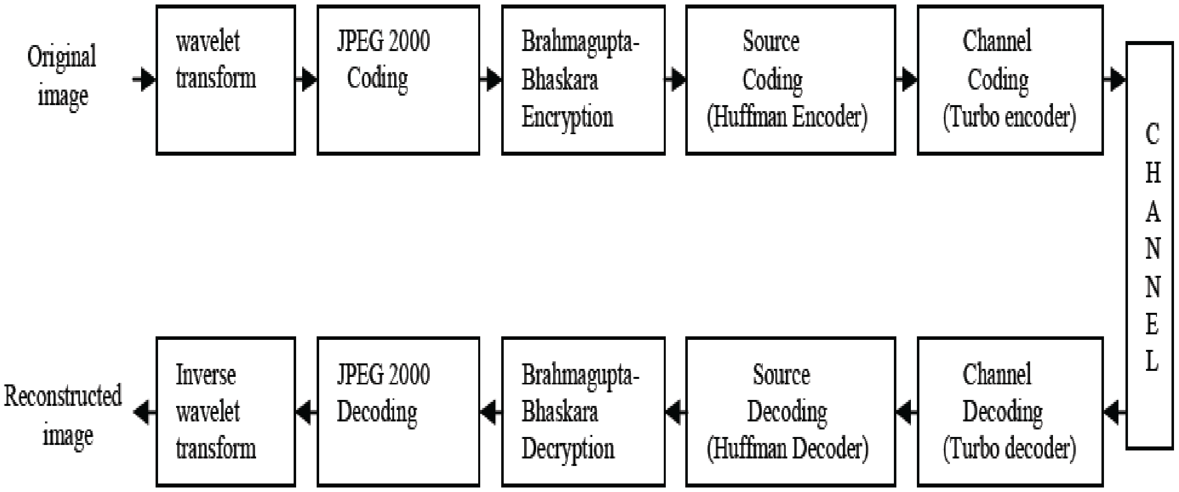

Original image
wavelet transform
JPEG 2000 Coding
Brahmagupta-Bhaskara Encryption
Source Coding (Huffman Encoder)
Channel Coding (Turbo encoder)
CHANNEL
Reconstructed image
Inverse wavelet transform
JPEG 2000 Decoding
Brahmagupta-Bhaskara Decryption
Source Decoding (Huffman Decoder)
Channel Decoding (Turbo decoder)

Fig. (5): Block diagram of the transmission and reception scheme proposed by [11]

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

```
for i = 0: N - 1
```

Generate a chaotic sequence ri; if ri = 1 then select the order [LPS, MPS] for encoding bit bi, Otherwise select the order [MPS, LPS].

The chaotic sequence here 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 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.

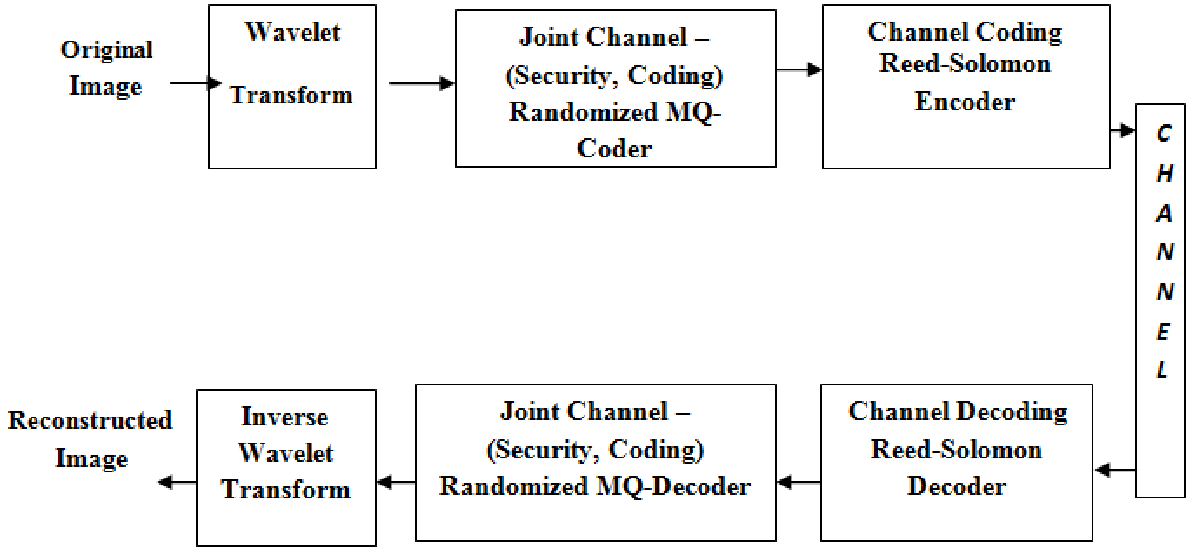

Original Image
Wavelet Transform
Joint Channel – (Security, Coding) Randomized MQ-Coder
Channel Coding Reed-Solomon Encoder
CHANNEL
Channel Decoding Reed-Solomon Decoder
Joint Channel – (Security, Coding) Randomized MQ-Decoder
Inverse Wavelet Transform
Reconstructed Image

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

Fig. (7): Original Image.

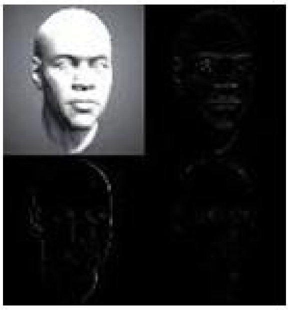


Fig. (8): Wavelet Coefficients.

Fig. (9):Transmitted Detailed Image.

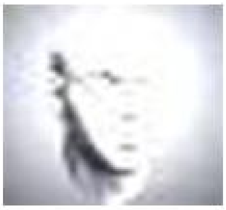


Fig. (10): Received Image with Randomized MQ-Coder

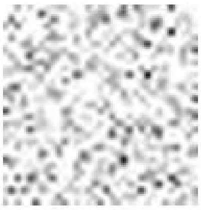


Fig. (11): Received Image with normal MQ-Coder

According to [12]; It founds that the standard version of RS codes such as RS (255, 223, 8) and RS (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.

4. Results

Image in **Figure.(7)**, is selected as image to get the wavelet coefficient from it, as shown in fig. 8, then we took the detailed coefficient (as shown in **Figure.(9**), to transmit it through the system stated in **Figure.(6)**, and received by randomize MQ-Coder with the correct initial of chaotic sequence, as shown in **Figure.(10),** while the rubbish one received by normal MQ-Coder is shown in **Figure.(11**).

5. 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. A modified MQ-Coder, based on chaotic sequence is proposed. Reed-Solomon code is preferred to be used as channel coding instead of Turbo Coding which double or triple the size of data.

References

1. **Krishna BharathKolluru, "Optimization of Arithmetic and MQ coding", ECE 734 VLSI Array Structures for Digital Signal Processing, 2009.**
2. **Amir Said, "Introduction to Arithmetic Coding - Theory and Practice ", Academic Press, 2004.**
3. **G. Langdon, and J. Rissanen, “Compression of black-white images with arithmetic coding,” IEEE Transactions on Communication, COM-29 (6): 858–867, 1981.**
4. **Hyungjin, Kim, Jiangtao Wen, and John D. Villasenor, "Secure Arithmetic Coding", IEEE Transactions on Signal Processing, 55 (5), 2007.**
5. **Marco Grangetto, Enrico Magli, and Gabriella Olmo, "Multimedia Selective Encryption by Means of Randomized Arithmetic Coding", IEEE Transactions on Multimedia, 8 (5), 2006.**
6. **S. Burrus, R. A. Gopinath, and H. Guo, “Introduction to Wavelets and Wavelet Transforms”, Prentice hall, 1998.**
7. **Hongxia Wang Ke Ding Changxing Liao, “Chaotic watermarking scheme for authentication of JPEG Images”, International Symposium on Biometrics and Security Technologies (ISBAST), pp: 1-4, 2008.**
8. **David Salomon, "Data Compression, the complete reference", 4rt edition, Springer-Verlag, London Limited, 2007.**
9. **I. H. Witten, R. M. Neal and J. G. Cleary, “Arithmetic Coding for Data Compression" Comm. ACM, 30 (6): 520, 1987.**
10. **Bernard Sklar, "Digital Communications, Fundamentals and Applications", second edition Prentice Hall, 2001.**
11. **M. Padmaja, Syed Shameem , "Secure Image Transmission over Wireless Channels", International Conference on Computational Intelligence and Multimedia Applications, 2007.**
12. **R. Logeshwaran, and I. Joe Louis Paul, "Performance Study on the Suitability of Reed Solomon Codes in WiMAX", ICWCSC, 2010.**