International Journal of Security and Its Applications
Vol.9, No.10 (2015), pp.31-46
http://dx.doi.org/10.14257/ijsia.2015.9.10.03

Joint Encryption and Error Correction Technical Research Applied an Efficient Turbo Code

Jianbin Yao[1], Jianhua Liu[2] and Yang Yang[3]

[1]*School of Information Engineering, North China University of Water Resources and Electric Power, Zhengzhou 450045, China*
[2]*School of Software, North China University of Water Resources and Electric Power, Zhengzhou 450045, China*
[3]*China Mobile Group Henan Co., Ltd. Xuchang branch, Xuchang 461000, China*
yaojbin@163.com,liujianhua@ncwu.edu.cn,dayangyang278@126.com

Abstract

In order to improve safety and reliability of secure communication system, we propose a joint encryption error correction coding scheme. In this scheme, a conflict-free interleaver parallel decoding method of Turbo codes is used, which is known simply as" efficient Turbo codes", and it is combined with chaotic encryption together. This scheme makes the information encryption and efficient Turbo coding step be completed at the same time, and explain the encryption/decryption process through the efficient parallel decoding method, and verify the feasibility of the scheme through the application of Turbo code in image transmission as an example. The Matlab simulation results show that, the scheme performance is more excellent and effective in security and reliability than the existing joint encryption and error correction coding scheme. Our proposed scheme may provide an excellent encoding candidate scheme for secure communication system.

Keywords: *Turbo codes, chaotic encryption, interleaver, secure communication, joint encryption and error correction*

1. Introduction

In late eighties of last century, McEliece used Goppa code construct a public-key cryptosystem, which is called McEliece system [1].Since then, cryptography and channel coding were combined together, which were separated disciplines originally. In 1997, the U.S. NSF (National Science Foundation) established a special working group to study the combination of encryption information technology and error control, which emphasized the importance of joint encryption and error correction technology, but did not give a specific embodiment [2]. In recent years, there were also some studies on encryption and error correction coding techniques [3-10], but most of the studies used two or more steps to complete message encryption and error control, in which the ability of error correction was limited [4]. Because of the excellent performance and wide application of Turbo codes, it was a good candidate to use Turbo codes to design a joint encryption and error correction algorithms. XiaoY. *et al.* proposed a encryption method based on Turbo Code Interleaver[5]. In this method, they used a secret key to control the Turbo code encoder interleaver, at the same time, they added an external interleaver before the Turbo encoder , which uses two interleaver to ensure the safety and reliability of the encryption scheme. In Payandeh A et al study [6], security of coding system relied on the drilling after cascade of Turbo code, which depended on the drilling rate. El-Iskandarani M. A., who proposed a two-dimensional chaotic map based encryption algorithm used in image transmission [7]. Cam proposed a correction encryption scheme, which made the AEC (Advanced Encryption Standard) and Turbo coding together [8]. Chai Y. et al built a

ISSN: 1738-9976 IJSIA

JEEC (Joint Encryption and Error Correction) coding scheme which combined the encryption technology and channel coding technology and achieved by one step[9], making it a comprehensive technical program and applied to information transmission. Zhang proposed the scheme which combined chaotic encryption and Turbo coding and achieved by step [10-12], in this scheme, the encryption was achieved by encryption modules which was embedded into turbo encoder and controlled by the chaotic system. This program achieved the combination of the error correction coding and encryption of information. Via the simulation experiment proved that this scheme had good security and reliability, however, there were no introduction for decryption scheme, and in the secret key sensitivity test, it had the poor effect on rate change of the pixel; in reliability analysis of this system , the characteristic of BER (Bit Error Rate) which compared with the standard Turbo Systems was not obvious, and under the same conditions, as the SNR, the system magnitude is high, which means the process of information transmission were vulnerable to interference.

As the mainstream of research in the field of error-correcting codes, Turbo codes are high-performance channel codes based on interleaved coded and iterative decoding, because it is more close to the Shannon limit performance. But its encoding and decoding is carried out in a long code and the case of multiple iteration, so there is sharp rise in complexity of realization, and large delay in decoding. Decoding delay is mainly from interleaver and iterative decoding algorithm, and iterative decoding delay is mainly from the calculated delay and the number of iterations at each iteration, and this delay is mainly caused by the complex calculation process of soft information and slow speed of convergence. How to reduce the decoding delay? There have been many research results. In this paper, we propose a parallel conflict-free interleaver Turbo code decoding method, referred to efficient Turbo codes. The so-called efficient, which has two meanings: Firstly, the code has high efficiency and low latency; Secondly, the code has excellent performance and low bit error rate.

Through the combination of encryption technology and channel coding technology and performance by one step, we will build a joint encryption error correction (JEEC) encoding scheme and a comprehensive system used in information transmission, then Shannon secure communication system model will be to simplify, and the communication system becomes more efficient, while safety and reliability of the communication system will be ensured. The former means that when the attacker uses a wrong key to decipher the received sequence, it will receive completely different information; The latter emphasizes that the encryption system should have a high immunity to channel errors, that is, the correct error correction code which used in system must have excellent error detection and correction capability. In this way, we can practically realize the improvement of encryption effect using channel coding, or that encryption can be used to improve channel coding, the two things complement with each other, and improve the safety and reliability of secure communication systems.

In order to improve the safety and reliability of secure communication system, in view of the security of chaotic convolutional coder [13], this paper studies a chaotic encryption combined with Turbo coding error correction coding scheme. In the scheme, designing a Turbo codes on the basis of a conflict-free interleaver parallel decoding method, that is efficient Turbo Code, which is applied to JEEC, explaining the efficient Turbo code encryption/decryption principle and encryption/decryption process. In this solution, decoding latency has been greatly declined, and the throughput of system has been largely improved. With efficient Turbo code which is applied to image transmission as an example, this paper make theoretical analysis and simulation verification for feasibility of the improved scheme. Compared with the results of literature [11], it is sure that safety and reliability of communication system which using efficient Turbo code decoding scheme is better, and this scheme

providing an excellent encoding candidate scheme for secure communication system.

2. Encryption

2.1. Encryption Scheme

PCCC type Turbo code is mainly composed of an interleaver and two interleaver RSC component encoders. Assuming the rate of each component encoder is 1/2, and the length of the generated polynomial is K, and storing series of parasitic memory is $M = K - 1$,and the generator matrix of two component encoders are $G_1 = [g_{10}, g_{11}, \cdots, g_{1,M}], G_2 = [g_{20}, g_{21}, \cdots, g_{2,M}]$.

Thus, assuming the number of Turbo codes input bits is K, the respectively corresponding three-way output are:

$$X_k = u_k \tag{1}$$

$$Y_{1k} = \sum_{i=0}^{M} g_{1i} u_{k-i} \bmod 2 \tag{2}$$

$$Y_{2k} = \sum_{i=0}^{M} g_{2i} u_{k-i} \bmod 2 \tag{3}$$

From (1)(2)(3), we can conclude that the output of the first channel coding is the original information sequence, and the output of the second path and the third path is a sequence of parity information produced by the encoder of the two components. Therefore, in order to achieve the Turbo coding encryption, we should encrypt its three outputs, in particular the output of the first road of the original information sequence.

There are two key parameters in the program: First, interleaver parameters (such as QPP interleaver parameters and registers the initial state and the feedback coefficient generated sequences based on conflict-free interleaver m sequence), Only the correct interleaver parameters can decoding have smooth progress; Second, Logistic chaotic map of the initial value encrypts the first road information sequences of Turbo coding system by the chaotic sequences, which generated by itself. However, it controls the output of two component encoder, i.e. generator matrix which control component encoder. In this way, three outputs of coding systems are controlled by chaos key, which is shown in Figure 1.

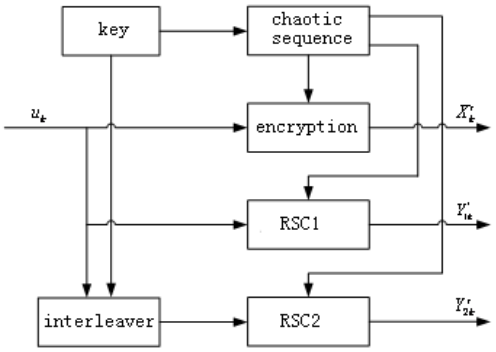

Figure 1. Encryption Scheme based on Turbo Codes

2.2. Encryption Algorithm

2.2.1. System-bit Encryption Information Sequence:n Logistic mapping chaotic dynamical system is expressed as:

$$s_{k+1} = f(s_k, \mu) = \mu s_k (1 - s_k), k = 0,1,2,\cdots \tag{4}$$

When $\mu \in [3.569946, 4]$,the chaotic map in a chaotic state, and mapping variables $s_k \in (0,1)$, it will produce a non-periodic sequence $\{s_k\}$ which does not converge. When the different initial value s_0 is input, the system will produce an entirely different output sequence. The output decimal sequence is distributed in the interval (0,1) , not the two-valued logic sequence. So, in order to make it become a sequence of 0 and 1, it needs binary processing, which conduct as follows:

$$t_k = \begin{cases} 0, & s_k < 0.5 \\ 1, & s_k \geq 0.5 \end{cases}, k = 0,1,2,\cdots \quad (5)$$

Among them, $\{s_k\}$ is chaotic sequence which generated by logistic map. $\{t_k\}$ is a logical sequence which after its binary. In order to realize the combination of encryption and Turbo coding, and does not leak original information, the output must be encrypted. Here, in order to encrypt, with the ideology of grouping password, we interleave the original information rearrange through logistic chaotic sequence which have good security.

Specific encryption System-bit information sequence process and steps are as follows:

1)Chaotic sequence $\{s_k\}$ is generated by the Logistic mapping, and generated a pseudo-random binary sequence $\{t_k\}$ through its binary processing. Suppose the number of data is i ,which the value is "1" in $\{t_k\}$,however, the number of data is *j*, which the value is "0"in $\{t_k\}$, among them, $i + \mathrm{j} = N$, N is the length of sequence.

2)Find the position which data value is "1" in the $\{t_k\}$, that is, the value of *k* when $t_k = 1$, $k = \{p_1, p_2, \cdots, p_i\}$ .Remove the system bit output of Turbo coding system, that is, $\{p_1, p_2, \cdots, p_i\}$ position of the plaintext data sequence $\{X_k\}$, then, we can obtain sequence $\{M_i\} = \{X_{p_1}, X_{p_2}, \cdots, X_{p_i}\}$ which length is i , in the following, $\{m_i\}$ sequence obtained by interleaving. Similarly, Find the position which data value is "0" in the $\{t_k\}$, that is, the value of *k* when $t_k = 0$, $k = \{q_1, q_2, \cdots, q_j\}$, Remove the system bit output of Turbo coding system, that is, $\{q_1, q_2, \cdots, q_i\}$ position of the plaintext data sequence $\{X_k\}$, then, we can obtain sequence $\{N_j\} = \{X_{q_1}, X_{q_2}, \cdots, X_{q_j}\}$ which length is j , in the following, $\{n_j\}$ sequence obtained by interleaving.

3) $\{m_i\}$ and $\{n_j\}$ are connected to be a series sequence $\{X'_k\}$, that is, $\{X'_k\} = \{\{m_i\}, \{n_j\}\}$, $\{X'_k\}$ sequence is a sequence of cipher text which encrypted the plaintext sequence $\{X_k\}$ sequence, and make $\{X'_k\}$ sequence a system output bit sequence in Turbo coding system.

2.2.2. Encryption Parity Bit Information Sequence: In the standard Turbo coding system, the polynomials of forward and feedback are determined, therefore state grid map of component code is determined, and the generated check sequence is also determined. The check information sequence encryption is controlling the forward polynomial of component encoder, through the chaotic sequence generated by Logistic map as a switch, that is the generation of matrix, which is shown in figure 2.

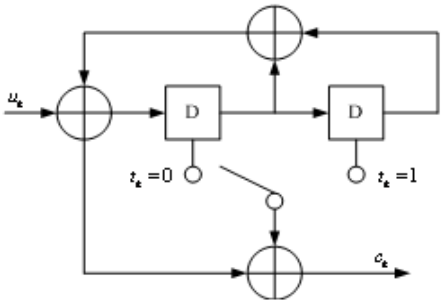

Figure 2. Parity Bit Information Sequence Encryption Scheme

Assuming the constraint length of component encoder is 2, and the generated binary chaotic sequence is $\{t_k\}$.In the clock K, If the chaotic sequence generator matrix value $t_k = 0$, then the code generation using the parity bits corresponding to $G_1(D) = [1+D+D^2, 1+D]$;If $t_k = 1$,then the code generation using the parity bits corresponding to $G_2(D) = [1+D+D^2, 1+D^2]$.By the transformation of generated matrix, the check sequence component encoder output is also stochastic, and reaching the effect of encryption.

3. Decryption

3.1. Decryption Principle

The main structure of Turbo code decryption program is Turbo code decoder, and it can be serial decoders or parallel decoders, which have difference between ordinary Turbo decoder : firstly, interleaver parameters controlled by the key, and the decoder needs to be fed into the interleaver and anti-interleaver before decryption; Secondly, before the start of the decoding, the information sequence received from the first route should be decrypted, that is, generate chaotic sequence by the Logistic mapping of the initial value, and de-interleaving the first circuit information sequence, then fed to the decoder for decoding; Finally, in the component decoder, it should store the trellis diagram according to the component encoder requires different generation matrix, in order to select different encoded output from different trellis, when decrypting based on the chaotic sequence. Turbo code decryption scheme is shown in Figure 3.

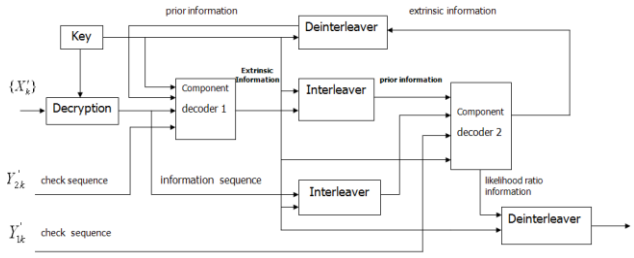

Figure 3. Turbo Code Decryption Scheme

In the conventional iterative decoder Turbo codes, Turbo-code decoding is each component decoder decodes the serial manner after receive a full frame of data, which is shown in Figure 3. Each iteration of two components is the decoding processing of the data blocks, which result in a larger coding delay, which is proportional to the size of the data block length.

3.2. Decryption Process

3.2.1. System-bit Information Sequence Decryption: In the symmetric cryptosystem, encryption key is the same with decryption key, and send and receive sides informed each other via a secure channel of communication, or through a third party authorization. After obtaining the key, decryption can be proceed smoothly. Decrypt specific steps are as follows:

a. Chaotic sequence $\{s_k\}$ is generated by a key (Logistic mapping initial value), through its binary processing, pseudo-random binary sequence $\{t_k\}$ is generated. Suppose the number of data is *i*, which the value is "1" in $\{t_k\}$;and the number of data is *j*, which the value is "0" in $\{t_k\}$.Among them, $i + \mathrm{j}=N$, N is the sequence length.

b. Find the position in which data value is "1" in the $\{t_k\}$, that is, the value of *k* when $t_k = 1$, $k = \{p_1, p_2, \cdots, p_i\}$,Similarly, find the position which data value is "0" in the $\{t_k\}$, that is, the value of *k* when $t_k = 0$, $k = \{q_1, q_2, \cdots, q_j\}$.

c. De-interleaving the data in $\{X'_k\}$ which is pre-*i*, then put results of de-interleaving in the position $\{p_1, p_2, \cdots, p_i\}$ sequentially; Similarly, de-interleaving the data in $\{X'_k\}$ which is post *j*, then put results of de-interleaving in the position $\{q_1, q_2, \cdots, q_j\}$,at last, the system-bit information sequence whose length is *N* is obtained.

3.2.2. Parallel Efficient Turbo Decoding of Conflict-free Interleaver: After getting parameters of interleaver and decrypting the system-bit information sequence, decoding Turbo codes are happening, in order to complete the final decoding of joint encryption error correction codes. Decoding can be serial decoding and parallel decoding. In this paper, we use the parallel decoding and the parallel conflict-free interleaver, so that decoding delay are greater saved. To solve the problem of memory conflicts which generated by Turbo codes when they are parallel decoding, the conception of non-conflict interleaver is introduced [14], in which interleaver and anti-interleaver functions are required to meet the conditions :

$$\begin{cases} \left\lfloor \frac{\pi(j+tW)}{W} \right\rfloor \neq \left\lfloor \frac{\pi(j+vW)}{W} \right\rfloor \\ \left\lfloor \frac{\pi^{-1}(j+tW)}{W} \right\rfloor \neq \left\lfloor \frac{\pi^{-1}(j+vW)}{W} \right\rfloor \end{cases} \tag{6}$$

Among them $0 \le j < M$, $0 \le t \ne v < M$

Serial decoding of Turbo codes have several algorithm, such as MAP algorithm, Log-MAP algorithm, Max-Log-MAP algorithm and so on, which can also be applied to the parallel decoding of Turbo codes, because each decoding of sub-block is equivalent to a serial decoding, and there is a parallel relationship between different sub-blocks.

Parallel decoding structure of Turbo Code is the process of decoding of the original data block whose length is *N*[15], and converting to the equal length sub-blocks decoding, whose number is *M*, as shown in Figure 4.

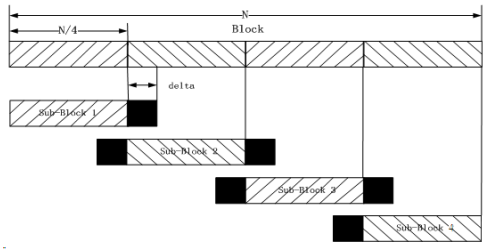

Figure 4. The Division of Data Blocks

Each component decoder have independent sub-decoder which number is *M*, the decoder structure is shown in Figure 5. Compared with the structure of the conventional serial decoding, parallel decoding structure make the decoding delay about 1/*M* of the original, and the data speed rate is about *M* times of the original, by increasing the cost of hardware.

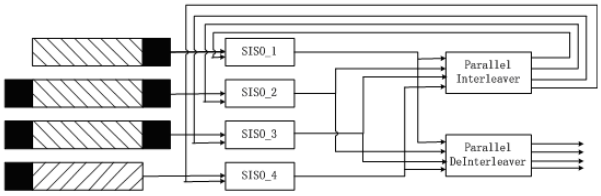

Figure 5. Turbo Code Parallel Decoding Structure

However, because the forward and backward state metrics of serial decoding are computed based on the entire block of data, initial value of the metric calculation of the forward recursion and the backward state is determined value. In the parallel decoding process, each sub-block simultaneously works, and the value of state metrics in the beginning and the end of each sub-block are undefined, so solution is as follows.

The initial value of the forward and backward state metrics referred to $\alpha^m_{(m-1)W}(S)$ and $\beta^m_{mW}(S)$ respectively, which sub-blocks number is m. Because the trellis diagram of Turbo code is a process of Markov, so the initial information of sub-block's forward and backward state metrics $\alpha^m_{(m-1)W}(S)$ and $\beta^m_{mW}(S)$ may be accumulated by redundant information (Figures 4 and 5 of the dark portion). If there is enough redundant information, relatively accurate initial value of the sub-blocks' state metrics can be obtained. The first sub-blocks initial value of forward state metric and the last sub-blocks initial value of backward state metric are computed without the accumulation of redundant information, because they are same in initialization and serial decoding, whose value is determined, respectively namely:

$$\alpha^1_0(S)=\begin{cases}1, & S=0\\ 0, & S\neq 0\end{cases}, \beta^M_N(S)=\begin{cases}1, & S=0\\ 0, & S\neq 0\end{cases} \tag{7}$$

For the other uncertain sub-blocks forward initial value $\alpha^m_{(m-1)W}(S)$, $2\le m\le M$,it should be obtained by forward recursion calculation on redundant information of the division in $m-1$ sub-blocks; Similarly, for the other uncertain sub-blocks forward initial value of state metric $\beta^m_{mW}(S)$, $1\le m\le M-1$,it should be obtained by backward recursion calculation on redundant information of the division in $m-1$ sub-blocks. To get more reasonable value of $\alpha^m_{(m-1)W}(S)$ and $\beta^m_{mW}(S)$, it need generalized treatment on the initial state of the redundant information, however, initial value of state metric is:

$$\begin{aligned}\hat{\alpha}^m_{(m-1)W-delta}(S)&=1/N_S, 2\le m\le M\\ \hat{\beta}^m_{mW+delta}(S)&=1/N_S, 1\le m\le M-1\end{aligned} \tag{8}$$

Among them, N_S is the number of states of the RSC in the Turbo code, *delta* is the length of the sub-block's redundant information. Through forward recursion calculation on $\hat{\alpha}^m_{(m-1)W-delta}(S)$, sub-block's forward initial value of state metric can be obtained whose number is $m(2\le m\le M)$,that is $\alpha^m_{(m-1)W}(S)=\hat{\alpha}^m_{(m-1)W}(S)$;Similarly, Through backward recursion calculation on $\hat{\beta}^m_{mW+delta}(S)$,sub-block's backward initial value of state metric can be obtained whose number is $m(1\le m\le M-1)$,that

is $\beta_{mW}^{m}(S) = \hat{\beta}_{mW}^{m}(S)$.The calculation on the state metrics of redundant information only for determination of each sub-block initial value of forward and backward state metrics, and it does not participate in the calculation on external information and likelihood information. Therefore, after obtaining sub-block's initial value of forward and backward state metrics, the value of state metric of redundant information can be discarded, without allocating a storage unit for storing these values. Figure 6 shows the calculation of forward and backward state metrics.

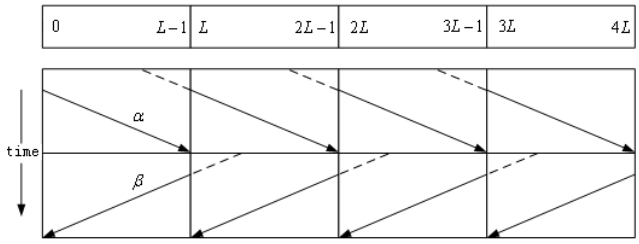

Figure 6. The Calculation of Forward and Backward State Metrics

4. Joint Encryption and Efficient Error Correction Coding and Analysis based on Turbo Codes

4.1. Security Analysis of Encryption and Efficient Error Correction System based on Turbo Code

4.1.1. Analysis of Statistical Tests: Security of joint encryption and error correction coding means that the attacker cannot use the wrong key to decrypt the source of information, as well as resistance to various attack algorithms. In this paper, we take image transmission as an example to analyze the security and reliability of the scheme. As a classical grayscale image in image processing, Lena with the size of 256×256 pixels and 256 gray levels is used in our numerical simulations. When image processing happened in system, firstly, ray value of each pixel is converted to a binary value of 8, so that obtain the image information which represented by the binary sequence table, and then make joint encryption and efficient error correction coding with the proposed scheme.

4.1.1.1. Histogram Statistics of Image Pixel Gray Value

Security of a password system is directly affected by the distribution characteristics of cipher text information. Uneven distribution information of Cipher text, as a starting point, which could be used by attackers for cipher text attack. Here, we use the histogram of the image to describe this feature.

In the histogram statistics the number of each gray value's appearance in a digital image, and then displays them through the two-dimensional Cartesian coordinate system, the abscissa represents the gray value of the pixels in the digital image, the vertical axis represents the frequency of emergence.

Assuming logistic chaotic mapping parameter $\mu = 4$, initial value $s_0 = 0.123456789$, and encrypt the original image. By contrast, the original and encrypted images are shown in Figure 7, and their histograms of pixel gray value are shown in Figure 8.

Figure 7. (a) Original Image; (b) Encrypted Image

As shown in the Figure 7(b), the encrypted image is similar to a white noise and any information of the original image is present.

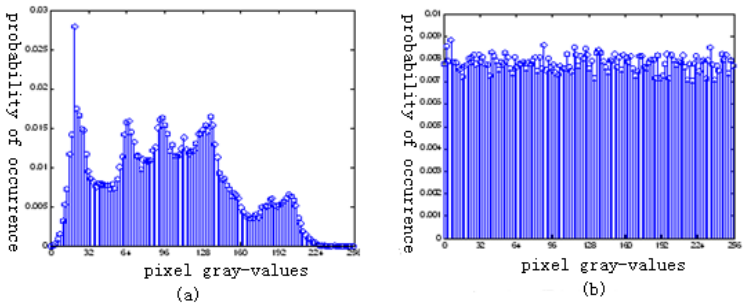

Figure 8. (a) Histogram of Original Image "Lena" (b) Histogram of Encryption Image "Lena"

Statistical results from the histogram, as shown in Figure 8, the distribution of pixel gray-values of encrypted image, which value between $0 \sim 255$, is more uniform than original image. Completely different from statistical characteristic of original image's pixel gray-values, the encrypted image completely changes the statistical characteristic of original image. It indicate that the scheme have obvious affect in hiding information of image, which may provide better resistance for known cipher text attack and statistical attack, and reach the effect of image encryption.

4.1.1.2. Correlation Statistics of Image Pixel Gray-values

The statistical definition of correlation is calculated by the following equation:

$$\operatorname{cov}(x, y) = E((x - E(x))(y - E(y))) \tag{9}$$

$$r_{xy} = \frac{\operatorname{cov}(x, y)}{\sqrt{D(x)} \cdot \sqrt{D(y)}} \tag{10}$$

Among them, x and y are gradation values of adjacent pixels, $E(\cdot)$ is the mean value, $D(\cdot)$ is the variance.

For test, 1000 pairs of horizontal and vertical adjacent pixels are selected randomly from the original image and the encrypted image, and obtained results are shown in Table 1.The correlation of adjacent pixels of the original image is close to 1, which have strong correlation characteristic, however, the correlation of adjacent pixels of encrypted image is close to 0, which basically irrelevant, which indicate that statistical characteristic of the pixels of the original image has been diffused into the encrypted image randomly.

Table 1. The Correlation of Adjacent Pixels

Image	before encryption	After encryption
The correlation of horizontal adjacent pixels	0.9756	0.0021
The correlation vertical adjacent pixels	0.9768	-0.0018

In order to visualize the improvement of correlation, we draw the distribution of pixel gray-values of 1,000 pairs of horizontal adjacent position, which before and after encryption, as shown in Fig9. As can be seen, in the original image, 1,000 pairs of horizontally adjacent pixel gray-values, whose distribution present approximate linear relationship, which drawn by the ascending order. However, in the encrypted image, 1,000 pairs of horizontal adjacent pixel gray-values, whose distribution is in a mess. It shows that the scheme can effective reduce the correlation between adjacent pixels of the image, and resistant attack of related algorithms.

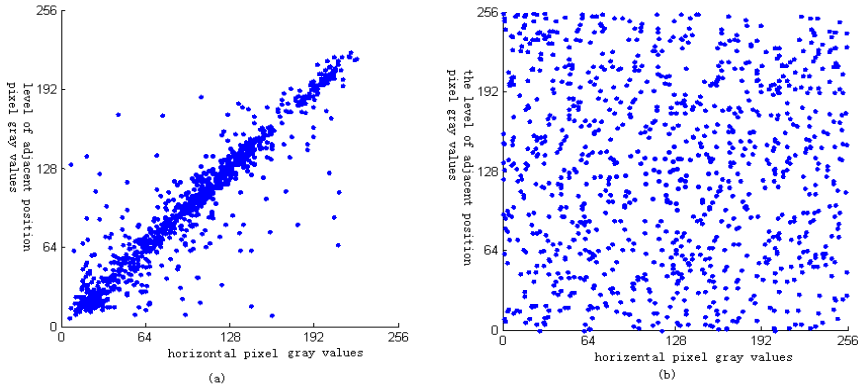

Figure 9. The comparison of horizontal adjacent position pixel gray-values correlation, which before and after image encryption. (a)The level of adjacent position pixel gray-values with original image.(b) The level of adjacent position pixel gray-values with encryption image.

4.2. Key Analysis

4.2.1. Key Sensitivity Analysis: To evaluate the performance of an encryption scheme, sensitivity of the key is an important standard. The sensitivity of key includes two meanings: a. there are two totally different encryption results because of minor changes in the encryption key. b. If the decryption key has minor changes, it could not properly decrypt for the encrypted result.

In order to test the sensitivity of the key in the scheme, the change rate of image pixel is used as an evaluation indicator. The change rate of image pixel is defined as following:

$$R = \frac{\sum_{i=1}^{W}\sum_{j=1}^{H} Diff(P(i,j), P'(i,j))}{W \times H} \tag{11}$$

$$Diff(P(i,j), P'(i,j)) = \begin{cases} 1, & P(i,j) \neq P'(i,j) \\ 0, & P(i,j) = P'(i,j) \end{cases} \tag{12}$$

Among them, W and H represent the image's width and height, $P(i,j)$ and $P'(i,j)$ respectively represent the gray value of original image and encrypted image at the pixel location(i,j). The test is divided into two steps:

a) With the initial value of Logistic chaotic map $s_0 = 0.123456789$ as the key, the original Lena image is encrypted, the encrypted image denoted as $\mathrm{Lena}(s_0)$. Then change the value of the key $s_0' = 0.123456788$, and encrypt the original Lena image, the encrypted image denoted as $\mathrm{Lena}(s_0')$.Comparing change rate of pixels, which with two slightly different keys encrypt the same image respectively, which is shown in Table 2.

Table 2. The Rate of Pixel Change between the Images of Different Keys Encryption

The images of different keys encryption	Rate of pixel change(%)
$\mathrm{Lena}(s_0)$ and $\mathrm{Lena}(s_0')$	99.60

b) With s_0 and s_0' as keys, respectively decrypt the encrypted image which encrypted by key s_0, and the images are denoted as Figure $\mathrm{Lena}(s_0 \mid s_0)$ and $\mathrm{Lena}(s_0 \mid s_0')$.Comparing change rate of pixels, which are decrypted with correct key and wrong key, as shown in Table 3.

Table 3. The Rate of Pixel Change between the Images of Different Keys Decryption

The images of different keys decryption	Rate of pixel change(%)
$\mathrm{Lena}(s_0 \mid s_0)$ and $\mathrm{Lena}(s_0 \mid s_0')$	99.64

We can conclude from the results of Table 2 and Table 3, encrypt the same image with encryption keys which have minor differences will lead to a high change rate of pixel, so that there is great difference between encrypted image and original image. In addition, decrypt the same image with decryption keys which have minor differences will also lead to a high change rate of pixel, so that there is great difference between decrypted image and original image. So, the encryption algorithm has good sensitivity of key, which can resist brute-force attacks and attacks based on sensitivity.

4.2.2. Analysis of Key Space: Logistic chaotic map is very sensitive to initial values, while different parameters μ will produce completely different chaotic sequence, so both can be used as a single key, and also be combined as a key to use.

For this scheme, the key space $K = (f, \mu, s_0, N)$, the key parameters which are double-precision and floating-point numbers are stored in the computer, in which the interleaver parameter f is determined by the choice of interleaver, and μ can take any value of the parameter between $[0, 4]$, and the initial value s_0 can be take any value between $(0,1)$, and N is iterations of chaotic map, that is the length of chaotic sequence or the length of information sequence. Only when these parameters of keys are correct, can the original information be restored, so the system have a very large key space to resist brute-force attacks and strengthen the defensive system.

Indeed, Turbo codes' unique coding structure also makes it easy contact with secure communication system, which have many encodes parameters, such as the generator polynomial, puncturing rate, etc. However, erroneous decoding parameter will result in failing of decoding, and cannot recover the original information, so the encoding parameters Turbo codes can also be used as a key.

4.3. Reliability of Joint Encryption and Error Correction Coding Analysis based on Effective Turbo Codes

Reliability refers to the error correction performance of the system, and the system can withstand varieties of noise which interfere the transmission of information, in order to reduce the error rate of communications. The structure of Turbo Codes are changed at a certain extent in this scheme, so in order to analyze its effect on the performance of error correction ability of Turbo Codes, we can compare the BER characteristics in this scheme with the BER characteristics in standard Turbo codes, and with the result we can judge the correction ability of this scheme. Simulation parameter settings: AWGN channel, BPSK modulation, frame size 1024, generating matrix A, the rate 1/3, QPP interleaver B, the degree of parallelism C, decoding algorithm Log-MAP, the number of iterations 5, 10000 frames. The simulation results are shown in Figure 10.

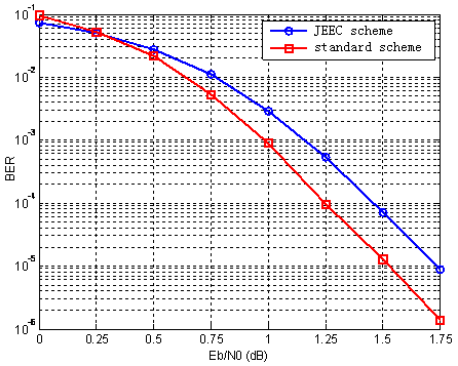

Figure 10. The BER comparison CJEEC with Standard Scheme

Simulation of Figure 10 compares reliability of the joint error correction coding with standard encryption Turbo coding. From the comparison of BER characteristics, we conclude that the gap is not more than 0.25dB between joint encryption and error correction coding and standard encryption Turbo coding, what's more, with the beginning from 0.5dB ,there is rapid decline in the curve of bit error rate, and the bit error rate has reached 10-4magnitude when the gap is 1.5dB,furthermore,the bit error rate has reached 10-5magnitude when the gap is 1.75dB.Therefore, the joint encryption error correction coding still has a good performance in error correction . And with the scheme in literature [11], the bit error rate has reached 10-3magnitude when the gap is 1.7dB, so information transmission system is vulnerable to interference, and its reliability is not high.

The result of recovery through the receiver 8 iterative decoding after image transmission with different signal noise ratio, the simulation results are shown in Figure 11. Along with the increasing number of iterations, the result of image recovery by the receiver when the SNR is 1dB is shown in Figure 12. Recovery results of image can be seen from Figures 11 and 12, with the increasing signal noise ratio, the distortion of recovery image is getting smaller, and the effect is getting better; as the same, with the increasing iterations, the distortion of recovery image is getting smaller, and the effect is getting better. This result is consistent with the performance of Turbo code, and verify the reliability and feasibility of joint encryption and error correction coding.

Figure 11. The result of image recovery with different signal noise ratio when iter=8. (a) The result of image recovery when the SNR=-0.5 dB.(b) The result of image recovery when the SNR=0 dB.(c) The result of image recovery when the SNR=0.5 dB.(d) The result of image recovery when the SNR=1dB.(e) The result of image recovery when the SNR=1.5 dB.(f) The result of image recovery when the SNR=2 dB.

Figure 12. The result of image recovery with different iterations when the SNR=1 dB.

(a) The result of image recovery when iter=1.(b) The result of image recovery when iter=2.
(c) The result of image recovery when iter=3.(d) The result of image recovery when iter=4.
(e) The result of image recovery when iter=5.(f) The result of image recovery when iter=6.
(g) The result of image recovery when iter=7.(h) The result of image recovery when iter=8.

5. Conclusion

Based on the secret communication theory, this paper research the scheme of joint encryption error correction coding with the efficient Turbo codes, and explain encryption / decryption principles and encryption / decryption processes of improved scheme with the use of effective Turbo decoding. Taking efficient Turbo codes for image transmission as an example, theoretical analysis and numerical simulations are carried out to verify the

feasibility of our proposed scheme, and the performances are compared with the results in literature [10].From comparison, we can conclude that communication system using efficient Turbo code decoding scheme have better performance in security and reliability, and conflict-free parallel decoding way reduce the decoding delay and improve the throughput of system, which make a strength for the rapid development of wireless communications, and provide a good candidate coding scheme for wireless security communication system. Subsequent work can be analyzed in password attack on the proposed scheme of joint encryption error correction, and verify the safety of scheme in certain attack case.

Acknowledgements

This work was supported by National Natural Science Foundation of China(Grant No. 61205003). The authors would like to thank the editor and reviewer for the helpful comments on the manuscripts.

References

[1] R. J. McEliece. A Public-Key Cryptosystem Based on Algebraic Coding Theory. DSN Progress Report, **(1978)**, pp. 114-116, Pasadena, CA: Jet Propulsion Lab.
[2] Report of the Working Group on Cryptology and Coding Theory, National Science **(1997)**. http://www.nsf.gov/pubs/1998/nsf9814/nsf9814.htm.
[3] M. Padmaja, S. Shameem. Secure Image Transmission over Wireless Channels. IEEE International Conference on Computational Intelligence and Multimedia Applications, **(2007)** December 13-15, vol. 4, pp. 44-48, Sivakasi, Tamil Nadu.
[4] Y. L. Grushevsky, G. F. Elmasry. Adaptive RS Codes for Message Delivery over an Encrypted Mobile Network, IET Communications, vol. 3, no. 6, **(2009),** pp. 1041-1049.
[5] Y. Xiao, Y. Zhao, Y. M. Xie, H. L. Moon. The Soft Encrypting Channel Based on Turbo-code En-decoders for Wireless Data Transmission. In proceeding of TENCON, **(2005)** November 21-24,pp. 1-6. Melbourne, Qld.
[6] A. Payandeh, M. Ahmadian, A. M. Reza. Adaptive Secure Channel Coding Based on Punctured Turbo Codes. IEEE Proceedings on Communications, **(2006)** April, vol.153, no.2, pp. 313-318.
[7] M. A. El-Iskandarani, S. Darwish, S. M. Abuguba. Reliable Wireless Error Correction Technique for Secure Image Transmission. Proceedings of Security Technology, 43rd Annual International Carnahan Conference on, **(2009)** October 5-8, pp. 184-188, Zurich, Switzerland.
[8] H. Cam, V. Ozduran, O. Ucan. A Combined Encryption and Error Correction Scheme: AES-Turbo, IU-Journal of Electrical & Electronics Engineering, vol. 9, no. 1, **(2012),** pp. 861-866.
[9] Q. Chai, G. Gong. On the (in)security of two Joint Encryption and Error Correction schemes, International Journal of Security and Networks, vol. 6, no. 4, **(2011),** pp.191-200.
[10] Q. Mao, C. Qin, L. J. Sun. Turbo-based encryption with error correction capability, Journal of Computational Information Systems, vol. 8, no. 7, **(2011),** pp.2876-2885.
[11] W. J. Zhang, Q. Mao. Error-correcting and Encryption Joint Coding Scheme Based on Turbo Code, Radio Communications Technology, vol. 38, no. 5, **(2012),** pp. 29-32.
[12] Q. Mao , C. Qin. A novel turbo-based encryption scheme using dynamic puncture mechanism, Journal of Networks, vol. 7, no. 2, **(2012),** pp.236-242.
[13] J. T. Zhou, A. C. Oscar. On the security of chaotic convolutional coder. IEEE Transactions on Circuits and Systems. vol. 58, no. 3, **(2011),** pp.595-606.
[14] A. Nimbalker, T. K. Blankenship, B. Classon and T. E. Fuja.Contention-Free Interleavers for High-Throughput Turbo Decoding. IEEE Transactions on Communications, vol. 56, no. 8, **(2008),** pp. 1258-1267.
[15] X. J. Zhang, M. Zhao, S. D. Zhou, J. Wang. Parallel decoding of turbo product codes for high data rate communication. The 57th IEEE Semiannual Vehicular Technology Conference**, (2003)** April 22-25, vol. 4,pp.2372-2375.

Authors

Yao Jianbin is currently working as a lecturer in the Dept. of Communication, College of Information Engineering, North China University of Water Resources and Electric Power, China. He has received the B. Tech degree and the M. Tech degree from the Shanxi Normal University, China, both in Electronics and Information Engineering. He has several publications in various conferences and journals at international repute. His research interests include Signal Processing and Image Encryption.

Liu Jianhua is currently working as a Professor and Head of the College, College of Software, North China University of Water Resources and Electric Power, China. He has received his Ph D degree in Management Science and Engineering from the Beijing University of Posts and Telecoms, China. He has 26 years of teaching experience and is actively associated with national professional bodies. He has several publications to his credit at national and international level. His research interests include Image Processing, database application and Computer Security.

Yang Yang is currently working as an communication Engineer in the Xuchang branch, China Mobile Group Henan Co., Ltd. He has received the B. Tech degree from the North China University of Water Resources and Electric Power, and the M. Tech degree from the University of Electronic and Science Technology of China, both in Electronics Information Engineering and Cryptography. His research interests include Signal Processing, Error Control Codes.