A Novel Turbo-Based Encryption Scheme Using Dynamic Puncture Mechanism

Qian Mao and Chuan Qin
School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, Shanghai 200093, China
Email: maoqiansh@gmail.com, qin@usst.edu.cn

***Abstract*—This paper proposes a novel encryption method based on Turbo code. In most communication systems, information encryption and error correction are always independent. While joint encryption and error correction codes combine these two processes into one. In order to provide information encryption and error correction simultaneously, we generate a normal random sequence that controls the puncturing mechanism by a secret key in the Turbo encoder. The puncturing mechanism is dynamic and controlled by the secret key. On the other hand, the key-controlled puncturing mechanism deletes the parity bits randomly, which ensures a high error correction capability for the Turbo code. When decoding, only the legal receiver can generate the same normal random sequence using the secret key, then classify and decrypt the received sequence correctly. While for the illegal receivers, because a wrong secret key results in a wrong puncturing mechanism, and the Turbo decoder is sensitive to the puncturing mechanism, they will get a totally wrong decoding result. Meanwhile, this coding scheme also provides good error correction capability for the encrypted information while it is transmitted in a noisy channel. Experimental results show that the proposed method performs well in terms of both security and error-immunity.**

***Index Terms*—encryption, Turbo code, puncture, security, bit error rate**

I. Introduction

Cryptography is used to protect information from interception by illegal receivers in communication channels. Over the past fifty years, many typical encryption methods, such as DES, AES, RSA, and chaotic cryptography, have been proposed to provide high security for information communication [1-4]. Current encryption techniques are usually sensitive to noise. Therefore, a few errors in transmission may cause the encryption system to collapse. In order to overcome this problem, it is necessary to adopt error correction codes before transmission [5, 6]. Until now, most encryption systems have been designed independently with the error correction coding. However, if we integrate the encryption process with the error correction coding, the communication system will be more efficient, and its security and reliability can be ensured simultaneously.

The gist of the joint encryption and error correction codes lies in the system's security and reliability. The system's security means the attacker will get different information when he or she decrypts the received sequence with the wrong secret key. And the system's reliability means the encryption system has a high level of immunity to channel errors; that is, the error correction code used in the system must have a high level of error-correcting capability.

Some researches have been done on the secret communication based on error correction codes, but most of them need two steps for information encryption and error correction [7-9]. Gligoroski *et al*. proposed a scheme of joint error correction and encryption [10], but the error correction code in the scheme is based on hard decision and the error-correcting capability is low.

Since Berrou firstly introduced the Turbo codes [11], a lot of researches have been done. This is because the Turbo codes have excellent error correction performance, which is near to tht Shannon limitation if the frame size is large enough [12-13]. Therefore it is advantageous to design encryption scheme using Turbo code. Cam *et al*. combined the AES encryption with Turbo code into a single step [14]. El-Iskandarani *et al*. proposed an encryption method based on a two-dimensional chaotic map, but this scheme is used only for image transmission [15]. Yang presented an encryption method using the interleaver of the Turbo code [16]. In this method, the interleaver is controlled by a secret key, so information bytes can be encrypted during Turbo encoding. But this scheme increases the time delay because of the information encryption.

The coding rate of the normal Turbo code is 1/3. In order to obtain a higher coding rate, a puncturing mechanism is often adopted [17-18]. By periodically eliminating some bits from the output of the recursive systematic convolutional encoders of the Turbo code, a higher coding rate can be achieved. The performance of the punctured Turbo codes has been widely researched [19-21]. Most puncturing mechanisms delete the parity bits periodically. If we puncture the parity bits irregularly and control the puncturing algorithm with a secret key, the information will be encrypted during Turbo encoding. The key point of this dynamic puncturing mechanism is that the error correction capability of the Turbo code is ensured during the information encryption.

This paper proposes a new encryption method based on a dynamic puncturing mechanism. In the following,

doi:10.4304/jnw.7.2.236-242

Section Ⅱ provides a brief review of the normal Turbo code, and Section III presents the proposed encryption scheme. Experimental results are shown in Section IV, and Section V concludes.

II. REVIEW OF THE NORMAL TURBO CODES

The main components of the Turbo encoder are an interleaver and two recursive systematic convolutional (RSC) encoders. To obtain a higher coding rate, the puncturing mechanism is adopted in the output of the two RSC encoders, as shown in Fig. 1.

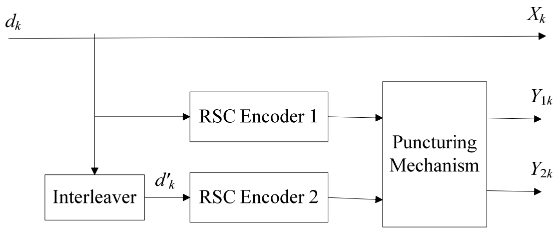


Figure 1. Flowchart of a Normal Turbo Encoder

In the puncturing mechanism of a normal Turbo code, the deleted bits are usually located periodically. Fig. 2 shows an example of a puncturing algorithm of the normal Turbo code. In Fig. 2, Y_{1i} (i = 1, 2, …) is the ith output bit of RSC encoder1 in Fig. 1, and Y_{2i} (i = 1, 2, …) is the ith output bit of RSC encoder2. The puncturing algorithm deletes the bits at even locations in Y_{1i} and the bits at odd locations in Y_{2i}. By this means, the parity bits are reduced by half, and the coding rate of the Turbo code is increased from 1/3 to 1/2.

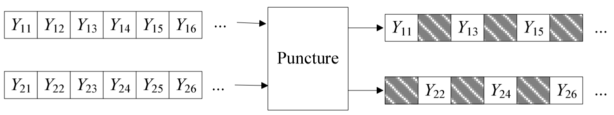


Figure 2. An Example of the Puncturing Scheme of the Normal Turbo Code

After the puncturing, the transmitting sequence is

$$X_1, Y_{11}, X_2, Y_{22}, X_3, Y_{13}, X_4, Y_{24}, X_5, Y_{15}, X_6, Y_{26}, \cdots,$$

where X_i (i = 1, 2, …) is the ith bit of the first output of the encoder, shown as Fig. 1.

On the receiver side, the decoder uses the same puncturing algorithm to classify X_i, Y_{1i}, and Y_{2i} in the received sequence, and then sends them to a Turbo decoder to start an iterative decoding process.

It is clear that only parity bits can be punctured, since deletion of systematic bits leads to inferior performance for decoding. If one parity bit is reserved for every k information bits, the coding rate r is

$$r = \frac{k}{k+1}. \tag{1}$$

Fig. 3 shows the Bit Error Rate (BER) performances of the normal Turbo codes whose coding rates are 1/2 and 1/3 respectively, when the SNR of the Additive White Gaussian Noise (AWGN) channel varies from 1.0 dB to 3.0 dB. In this experiment, the Turbo frame size is 400 bits, and the log-maximum *a posteriori* (Log-MAP) algorithm is implemented when decoding.

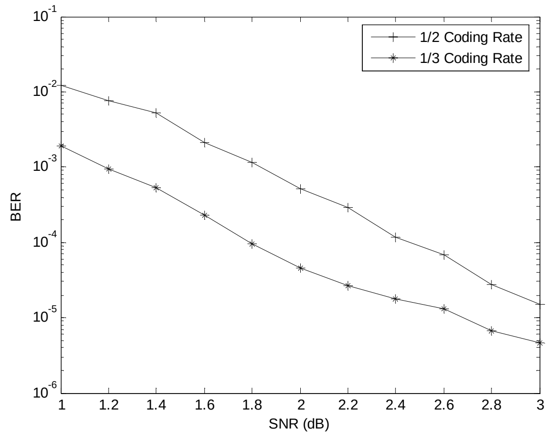


Figure 3. BER Curves of the Normal Turbo Codes with Different Coding Rates

From this figure we see that when the coding rate increases from 1/3 to 1/2, the SNR increases about 0.8dB.

It is proven that the asyptotic bit-error probability for a maximum-lilelihood decoder on the AWGN channel is

$$P_b \approx \max_w \frac{wn_w}{N} Q\left(\sqrt{\frac{2rd_{w,\min}^{TC} E_b}{N_0}}\right), \tag{2}$$

where $d_{w,\min}^{TC}$ is the minimum weight Turbo-Codeword for wight-w input, n_w is the number of wight-w inputs resulting in a weight-$d_{w,\min}^{TC}$ Turbo-Codeword, and E_b/N_0 is the user bit energy to one-sided noise power spectral density ratio. The maximizing w in (2) is primarily function of the interleaver and is never equal to one, since a weight-one input will lead to nonremergent paths in both RSC encoders [22].

III. PROPOSED TURBO-BASED ENCRYPTION SCHEME

In the Turbo coding scheme, the puncturing mechanism of the encoder and the decoder must be consistent. Now we adopt a dynamic puncturing mechanism and use a secret key to control it, only the legal receiver who has the key can classify X_i, Y_{1i}, and Y_{2i} correctly with the same puncturing mechanism, and then decode successfully. By this means, the information will be encrypted.

On the other hand, an inappropriate puncturing mechanism will reduce the error correction capability of the Turbo code. In order to ensure a good BER performance, the reserved parity bits should be irrelevant as much as possible.

We present an encryption scheme based on the dynamic puncturing mechanism of the Turbo code. This scheme provides good security and high error correction capability in one coding step. The encryption and decryption process are described as follows.

A. Encryption Process

The main procedure of encryption is shown as Fig. 4. The structure is similar to that of the normal Turbo encoder, except that the puncturing mechanism is controlled by a secret key.

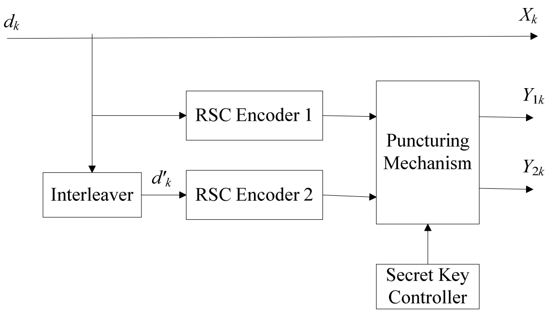


Figure 4. Flowchart of the Encryption Process

Suppose the length of the RSC encoder is K, the memory is $M = K$-1, and the generators of the two RSC encoders are $G_1 = [g_{10}, g_{11}, \ldots, g_{1,K\text{-}1}]$ and $G2=[g_{20}, g_{21}, \ldots, g_{2,K\text{-}1}]$, respectively. Then the outputs of the kth input bit d_k are:

$$X_k = d_k, \quad (3)$$

$$Y_{1k} = \sum_{i=0}^{K-1} g_{1i} d_{k-i} \mod 2, \quad (4)$$

$$Y_{2k} = \sum_{i=0}^{K-1} g_{2i} d_{k-i} \mod 2. \quad (5)$$

In the present encryption scheme, the puncturing mechanism is controlled by a secret key; that is, different keys result in different puncturing schemes. On the other hand, in order to ensure a high error correction capability of the coding scheme, the coding rate varies from 1/2 to 1/3 in our dynamic puncturing mechanism. To meet these goals, the following steps are implemented:

a) Suppose the secret key is k.
b) Using k as an initial value, generate a normal random sequence P. The elements in the sequence are integers, the mean of the sequence is 0 and the standard deviation is d. The length of the sequence is equal to the frame size of the Turbo code.
c) If $P(i)$ is 0 and i is even (i = 1, 2, …), delete the output bit of RSC encoder1 Y_{1i}; if $P(i)$ is 0 and i is odd, delete the output bit of RSC encoder2 Y_{2i}; if $P(i)$ is not 0, both Y_{1i} and Y_{2i} are reserved.

By this process, a key-controlled dynamic puncture is achieved. Fig. 5 shows the flowchart of this process.

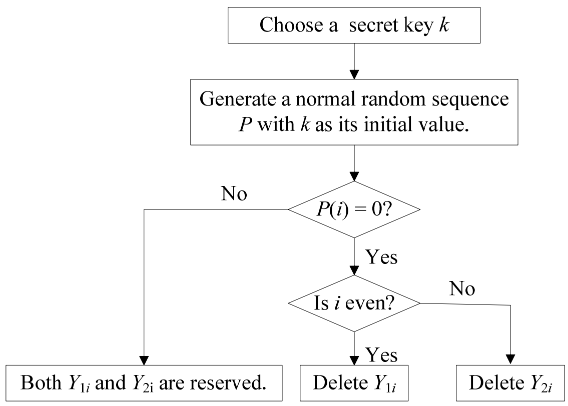


Figure 5. Flowchart of the Dynamic Puncturing Mechanism

Fig. 6 shows the puncturing scheme under the condition of P = 0, 0, 0, 1, 0, 0, …. Since the 4*th* number in sequence P is 1, both Y_{14} and Y_{24} are reserved after puncturing. While for the other parity bits, either Y_{1i} or Y_{2i} is reserved, since the corresponding element in P is 0.

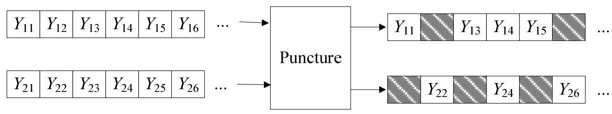


Figure 6. An Example of the Proposed Puncturing Scheme

Therefore in this example, after puncturing the transmitting sequence is

$$X_1, Y_{11}, X_2, Y_{22}, X_3, Y_{13}, X_4, Y_{14}, Y_{24}, X_5, Y_{15}, X_6, Y_{26}, \cdots.$$

Since the standard deviation d determines the quantity of 0s in the sequence P, the larger d is, the smaller the coding rate is, as shown in Tab. I. On the other hand, a large standard deviation means better security of the encryption scheme. When d = 0, the dynamic puncturing mechanism becomes periodic puncturing scheme of the normal Turbo code, the coding rate is 1/2, and the information can not be encrypted. Therefore, in order to provide high security and a high coding rate simultaneously, we should have a tradeoff and select a suitable d.

TABLE I.
DIFFERENT STANDARD DEVIATIONS AND THEIR CODING RATES

Standard Deviation d	0	0.25	0.3	0.4
Coding Rate r	0.5	0.493	0.482	0.461

B. Decryption Process

During the decryption, the receiver firstly generates the sequence P using the secret key k, and classifies X_i, Y_{1i}, and Y_{2i} in the received sequence according to P. Then the receiver sends them to a Turbo decoder, shown as Fig. 7.

Among the three kinds of received bits, X_i and Y_{1i} are input to the first decoder (DEC1), and X_i and Y_{2i} are input to the second decoder (DEC2). After that, the Turbo decoder will start the iterative decoding process.

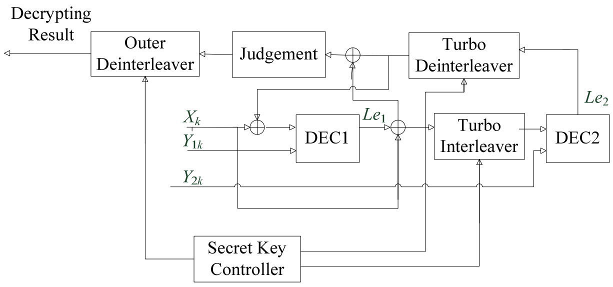


Figure 7. Flowchart of the Decryption Process

In the Turbo decoding process, the Log-MAP algorithm is implemented. Let us give some definitions firstly, as shown in Tab. II.

TABLE II.
SOME DEFINITIONS OF THE TURBO DECODER

Symbol	Definition
d_k	the *k*th original information bit
S_k	the state of the *k*th node of the decoder
R	vector of all the received bits in a frame
$\hat{d}_k$	the *k*th output of the decoder after judgement

In a Log-MAP decoding algorithm, the decoder decides $\hat{d}_k$ = 1 if $P(d_k = 1 \mid r) > P(d_k = 0 \mid r)$, and decides $\hat{d}_k$ = 0 otherwise. Therefore we compute the Logarithm of Likelihood Ratio (LLR) $L(d_k)$ of the *k*th input bit d_k and judge $\hat{d}_k$ by it. $L(d_k)$ is

$$L(d_k) = \log\left[\frac{P(d_k = 1 | observation)}{P(d_k = 0 | observation)}\right], \quad (6)$$

where $P(d_k = i | observation)$, i = 0 or 1, is the *a posteriori probability* (APP) of the input bit d_k [11].

Furthermore, the APP can be indicated as a conditional probability, therefore (6) becomes

$$L(d_k) = \log\left[\frac{\sum_m P(d_k = 1, S_k = m | R)}{\sum_m P(d_k = 0, S_k = m | R)}\right]. \quad (7)$$

In (7), $P(d_k = i, S_k = m | R)$ is the joint probability of d_k and state S_k under the condition of the received sequence R. This soft output from each constituent decoder is divided into three parts: the extrinsic output L_{e_k} which is new information derived by the current stage of decoding, a weighted version of the systematic input L_{s_k}, and a copy of the input *a priori* information L_{a_k} [23], that is

$$L(u_k) = L_{e_k} + L_{s_k} + L_{a_k}. \quad (8)$$

The Turbo decoder judges the result $\hat{d}_k$ according to $L(d_k)$ after several iterations.

In the decoding process, if the receiver uses the wrong key to build sequence P, he or she will confuse X_i, Y_{1i}, and Y_{2i}, and the decoding will fail. Only a legal receiver can generate the right P, which is equal to that of the transmitter. Then he or she will extract X_i, Y_{1i}, and Y_{2i} accurately and decode successfully. By this means, a successful information encryption and decryption can be achieved.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

In this section, we demonstrate the security and reliability of the proposed encryption scheme. In the experiments, the input data are the numbers ranging from 0 to 255, the channel is the AWGN, and the parameters of coding are listed in Tab. III.

TABLE III.
PARAMETERS OF THE TURBO CODE

Item	Parameter
Generate Matrix	g = [1 1 1;1 0 1]
Frame Size	400 bits
Iteration Number	5
Decoding Algorithm	Log-MAP

A. Security of the Proposed Encryption Method

The encryption method is secure if the attacker will obtain the wrong results when he or she uses incorrect keys to decode. We use the correlation value C to measure the similarity between the original data and the decrypted data.

$$C = \frac{\sum_{i=0}^{M}\left(A_i - \overline{A}\right)\left(B_i - \overline{B}\right)}{\sqrt{\sum_{i=0}^{M}\left(A_i - \overline{A}\right)^2 \sum_{i=0}^{M}\left(B_i - \overline{B}\right)^2}}. \quad (9)$$

In (9), A_i and B_i are the values of the *i*th data of the original and decrypted sequence, respectively, $\overline{A}$ and $\overline{B}$ are the averages of the original and decrypted sequence, and M is the length of the information sequence.

In the following experiments, we study the security of the proposed encryption scheme with different standard deviations of the normal random sequence P. To simulate the attack scenarios, we use 1000 randomly generated secret keys, where only the 500th one is correct. Fig. 8–11 show the correlation results between the original input data and the decoded data using different keys with the four coding rates shown in Tab. I. When the coding rate is 1/2, which means the standard deviation of the sequence *P* is 0, the correlation result showes that the decrypted data is exactly same with the original data, no matter which secret key is used when decrypting, as shown in Fig. 8. This means the coding scheme can not encrypt information. With the increase of the standard deviation of the sequence *P*, the defference of the decrypted data with correct and the wrong keys becomes big. And there is only one correlation peak in the location of the 500th key; the rest have low correlation values, as shown in Fig. 9-11. This result indicates that the proposed encryption method has reliable security, if a proper coding rate is selected.

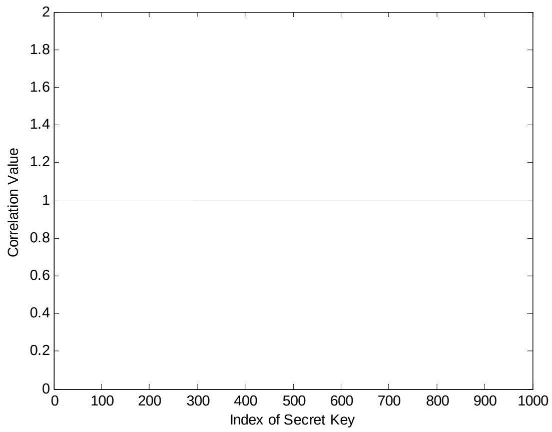


Figure 8. Correlation Result When Coding Rate equals 0.5

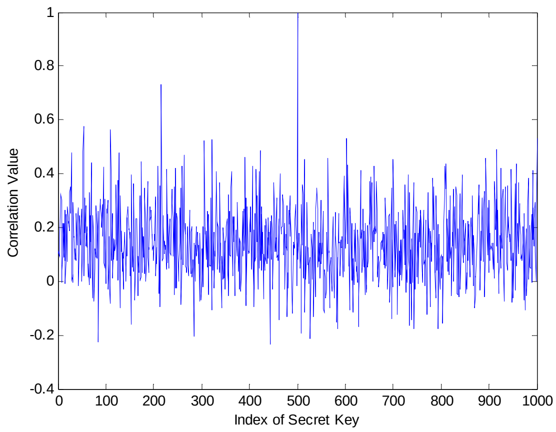


Figure 9. Correlation Result When Coding Rate equals 0.493

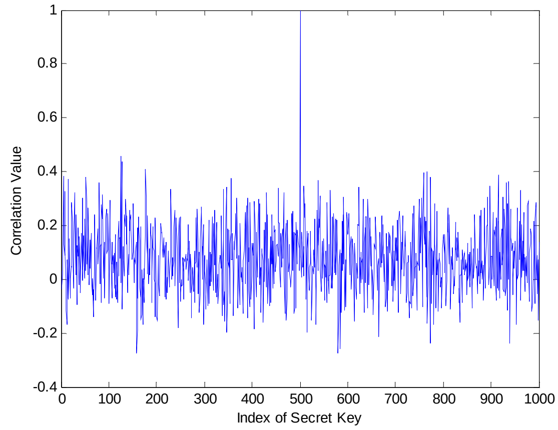


Figure 10. Correlation Result When Coding Rate equals 0.482

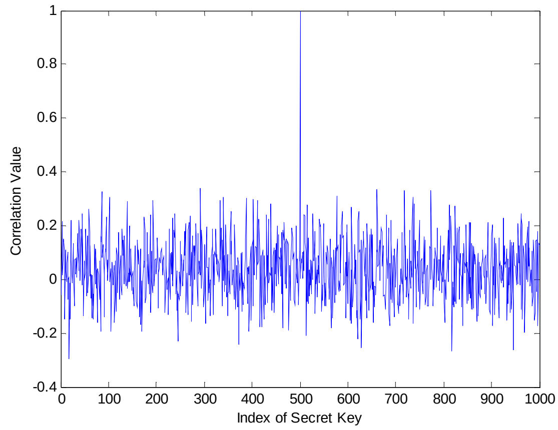
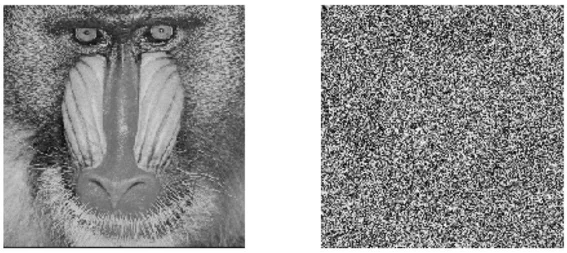


Figure 11. Correlation Result When Coding Rate equals 0.461

Fig. 12-14 show some experiment results about the applications of our Turbo-based encryption scheme in image encryption. In these figures, (a) is the original image, and (b) is the decrypted image using a wrong key when the standard deviation of the sequence *P* is 0.3. From these experiment results we see that our Turbo-based encryption scheme has good effect for the image encryption.

(a) The Original Image (b) The Encrypted Image

Figure 12. Experimental Results of Cameraman



(a) The Original Image (b) The Encrypted Image

Figure 13. Experimental Results of Baboon

(a) The Original Image (b) The Encrypted Image

Figure 14. Experimental Results of Tiffany

B. *BER of the Proposed Encryption Method*

The BER performance of the encryption method based on the error-correcting code is important. Fig. 15 shows the BER performances of the normal Turbo code and the proposed encryption code at the same coding rate when the SNR of the AWGN channel varies from 1.0 dB to 3.0 dB. The coding rate in this experiment is 0.482. Fig. 15 shows that the BER performance of the proposed encryption scheme is as good as that of the normal Turbo code, so the dynamic puncturing mechanism does not decrease the error correction capability of the Turbo code.

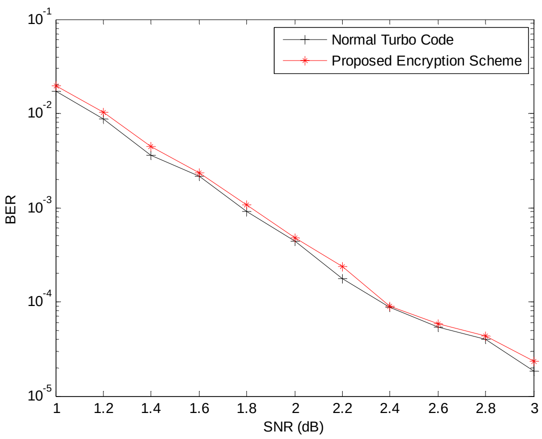


Figure 15. BER Comparison of the Proposed Encryption Scheme and Normal Turbo Code at the Same Coding Rate

Fig. 16 shows the BER performances of the proposed encryption scheme using different coding rates. From these curves, we find that a little variety of the coding rate does not change the BER performance obviously in our proposed encryption scheme. When the coding rate equals 1/2, the coding scheme is just the normal Turbo code with periodic puncturing, and the error correction capability is close to that of the proposed coding scheme.

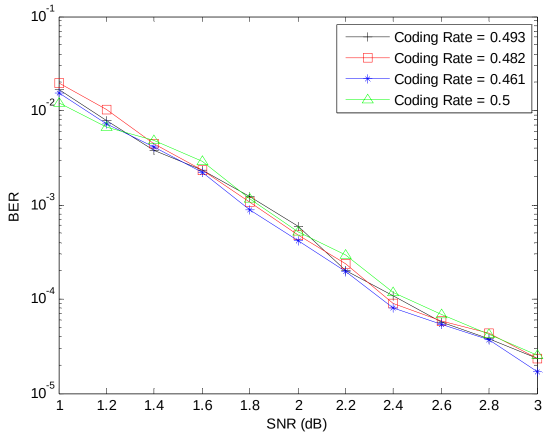


Figure 16. BER Curves of the Proposed Encryption Scheme at Different Coding Rates

V. CONCLUSIONS

This paper proposes an encryption scheme based on Turbo code. The information encryption is achieved by means of a key-controlled dynamic puncturing mechanism. Experiments are carried out to show the security and error-immunity of the method. We can conclude from the results that attackers without correct keys will never obtain the right decrypted data, and the error correction capability of the proposed coding scheme is as good as the normal Turbo code at the same coding rate.

ACKNOWLEDGMENTS

This work was supported by the Shanghai Specialized Research Foundation for Excellent Young Teacher in University (slg09005), and the OECE Innovation Foundation of USST (GDCX-Y-103).

REFERENCES

[1] A. A. Hasib, A. A. Md, and M. Haque, “A comparative study of the performance and security issues of AES and RSA cryptography”, *Proceedings of International Conference on Convergence and Hybrid Information Technology*, pp. 505-510, 2008.

[2] X. Li, J. L. Chen, W. X. Liu, and W. G. Wan, “An improved AES encryption algorithm”, *Proceedings of International Conference on Wireless Mobile and Computing*, pp. 694-698, 2009.

[3] H. M. Sun, M. E. Wu, W. C. Ting, and M. J. Hinek, “Dual RSA and its security analysis”, *IEEE Transactions on Information Theory*, vol. 53, no. 8, pp. 2922-2933, 2007.

[4] G. Millérioux, J. M. Amigó, and J. Daafouz, “A connection between chaotic and conventional cryptography”, *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 55, no. 6, pp. 1695-1703, 2008.

[5] L. Wang, B. Srinivasan, and N. Bhattacharjee, "Security Analysis and Improvements on WLANs", *Journal of Networks*, vol. 6, no. 3, pp. 470-481. 2011.

[6] P. H. Lee, U. Parampalli, and S. Narayan, "Secure Communication in Mobile Ad Hoc Network using Efficient Certificateless Encryption", *Journal of Networks*, vol. 4, no. 8, pp. 687-697. 2009.

[7] Padmaja, and M. Shameem, "Secure image transmission over wireless channels", *IEEE ICCIMA Conference Record*, pp. 44-48, 2007.

[8] Y. L. Grushevsky, and G. F. Elmasry, "Adaptive RS codes for message delivery over an encrypted mobile network", *IET Communications*, 2009, vol. 3, no. 6, pp. 1041-1049, 2009.

[9] C. Mathur, K. Narayan, and K. Subbalakshmi, "On the design of error-correcting ciphers," *EURASIP Journal on Wireless Communications and Networking*, vol. 2006, no. 2, pp. 1-12, November 2006.

[10] D. Gligoroski, S. Knapskog, and S. Andova, "Cryptcoding-Encryption and error correction coding in a single step," *Proceedings of International Conference on Security and Management*, pp. 1-7, June 2006.

[11] C. Berrou, A. Glavieux, and P. Thitimajshima, "Near Shannon limit error-correcting coding and decoding: Turbo codes", *Proceedings of IEEE International Conference on Communication*, pp. 1064-1070, 1993.

[12] S. Benedetto, and G. Montorsi, "Unveiling Turbo codes: some results on parallel concatenated coding schemes", *IEEE Trans. Inf. Theory*, vol. 42, no. 2, pp. 409-428, 1996.

[13] S. Park, and J. Jeon, "Interleaver Optimization of Convolutional Turbo Code for 802.16 Systems", *IEEE Communications Letters*, vol. 13, no. 5, pp.339-341, 2009.

[14] H. Cam, V. Ozduran, and O. Ucan, "A combined encryption and error correction scheme: AES-Turbo", *Journal of electrical & electronics engineering*, vol.1, pp. 861-866, 2009.

[15] M. A. El-Iskandarani, Saad Darwish, and Saad M. Abuguba, "Reliable wireless error correction technique for secure image transmission", *Proceedings of International Carnahan Conference on Security Technology*, pp. 184-188, 2009.

[16] Y. Xiao, "The soft encrypting channel based on Turbo-code en-decoders for wireless data transmission", TENCON 2005, pp. 1-6, 2005.

[17] J. Hagenauer, "Rate compatible punctured convolutional codes and their applications", *IEEE Trans. Commun.*, vol. 36, no. 4, pp. 389–400, 1988.

[18] D. Haccoun, and G. Bégin, "High-rate punctured convolutional codes for Viterbi and sequential decoding", *IEEE Trans. Commun.*, vol. 37, no. 11, pp. 1113-1125, 1989.

[19] M. A. Kousa, and A. H. Mugaibel, "Puncturing effects on turbo codes", *Proc. IEE Comm.*, vol. 149, no. 3, pp. 132-138, 2002.

[20] I. Chatzigeorgiou, M. R. D. Rodrigues, I. J. Wassell, and R. Carrasco, "A novel technique for the evaluation of the transfer function of punctured turbo codes," *Proc. of Intl. Conf. Comm.*, Istanbul, Turkey, pp. 1-6, 2006.

[21] I. Chatzigeorgiou, M. R. D. Rodrigues, I. J. Wassell, and R. A. Carrasco, "Analysis and design of punctured rate-1/2 Turbo codes exhibiting low error floors", *IEEE Journal on Selected Areas in Communications*, vol. 27, no. 6, pp. 944-953, 2009.

[22] Ö. F. Açıkel, and W. E. Ryan, "Punctured Turbo-Codes for BPSK/QPSK Channels", *IEEE Trans. Commun.*, vol. 47, no. 9, pp. 1315–1323, 1999.

[23] J. Hokfelt, O. Edfors, and T. Maseng, "A Turbo Code Interleaver Design Criterion Based on the Performance of Iterative Decoding", *IEEE Communications Letters*, vol. 5, no. 2, pp.52-54, 2001.

Qian Mao received the B.S. degree in Mechanical Engineering and Automation Science from Nanjing University of Aeronautics and Astronautics, Jiangsu, China, in 2000, and M.E. degrees in Traffic Information Engineering and Control from Shanghai Ship and Shipping Research Institute, Shanghai, China, in 2003, and the Ph.D. degree in Traffic Information Engineering and Control from Tongji University, Shanghai, China, in 2006. Since 2006, she has been with the faculty of the School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, where she is currently a Lecturer. Her research interests include information theory and coding.

Chuan Qin received the B.S. and M.E. degrees in electronic engineering from the Hefei University of Technology, Anhui, China, in 2002 and 2005 respectively, and the Ph.D. degree in signal and information processing from Shanghai University, Shanghai, China, in 2008. Since 2008, he has been with the faculty of the School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, where he is currently a Lecturer. His research interests include image processing and multimedia security.