Crypto-Coding as DES-Convolution for Land Mobile Satellite Channel

Rajashri Khanai
Research Scholar,
Department of Electrical and Electronics Engineering,
Gogte Institute of Technology,
Belgaum, Karnataka, INDIA

G. H. Kulkarni, Ph.D
Professor,
Department of Electrical and Electronics Engineering
Jain College of Engineering,
Belgaum, Karnataka, INDIA

ABSTRACT
In this paper, secure channel coding schemes based on convolutional codes are suggested to enhance the performance of combined cryptography and coding theory, which is called "Crypto-Coding". In the proposed work, Data Encryption Standard (DES) for security and channel coding algorithm such as convolutional code for efficient transmission are combined in a mono-block. This modification is required to improve the overall system performance. The combined System's performances are evaluated on Land Mobile Satellite (LMS) Channel. The results are compared with the system using ideal encryption and decryption.

Keywords
Crypto-coding, Convolutional coding, Data Encryption Standard (DES), Land Mobile Satellite (LMS) Channel.

1. INTRODUCTION
Digital communications and storage have happened to be component of our daily lives. Robust data transmission and data storage are taken for approved. People hardly realize that errors occur from time to time in data transmission and storage systems, and if the use of error control techniques were not in existence, reliable data transmission and storage would not be possible. Errors in data transmission and storage systems can come from many different sources such as random noise, interference, channel fading, or physical defects, to name a few. These channel errors must be reduced to a tolerable level to make sure the quality of data transmission and storage [1].

To combat the errors, normally two strategies, either individual or combined are used.

The first strategy is the automatic repeat request (ARQ). An ARQ system attempts to detect the existence of errors in the received data. If any errors are found, the receiver sends information to the transmitter of the existence of errors. The transmitter then resends the data until they are acceptably received.

The second one is known as the forward error correction (FEC), which not only detects but also corrects the errors, so that data retransmission can be avoided saving precious time parameter. In many practical applications retransmission may be difficult or not even feasible at all. For example, it is impossible for any receiver in a real-time broadcasting system to request data to be resent. In this case, FEC is the only viable solution. Either way, error control codes (ECC) are used for detecting the presence of errors and correcting them.

Despite of the apparently conflicting goals for robust data transmission, they have common genesis and provide many interesting relationships [2]. Shannon was the first to give cryptography a formal, mathematical treatment, focusing primarily on the task of encryption. In his model of a cryptosystem (or as he called it, a "secrecy system"), Shannon defined secrecy in terms of the amount of information a cipher-text (i.e., an encrypted message) reveals about its underlying message. To obtain perfect secrecy, a cryptosystem would need to reveal zero information about an encrypted message [3].

2. CONVOLUTIONAL CODING
Convolutional codes were first introduced in 1955 by Elias [4]. Since then they have achieved immeasurable popularity in practical applications The codes are not only equal (or sometimes even superior) to block codes in performance but also relatively simpler to decode. They are the type of error-correcting codes that are often used to improve the performance of wireless digital communication links, like satellite links. One important difference between convolutional codes and block codes is that the encoder contains memory. Encoders of convolutional codes can also be divided into two categories, namely feed-forward and feedback. In both of these categories the encoder can be systematic or non-systematic.

2.1 Convolutional encoder
For a (n, k, m) binary convolution code, the message input to the encoder is a binary sequence. Upon receiving an input bit m_t at time *t*, the encoder shown in figure 1 produces an *n*-bit codeword $c_t = \left(c_t^{(1)}, c_t^{(2)}, c_t^{(3)}, \ldots\ldots\ldots, c_t^{(n)}\right)$ as follows:

$$c_t^{(i)} = \sum_{j=0}^{v-1} g_j^{(i)} \oplus m_{t-i} \qquad (1)$$

where $i = 1,2,\cdots,n.g_j^{(i)} \in \{0,1\}$ are the coefficients. These coefficients comprise the encoding logic of the encoder [5].

The (n, k, m) encoder has the parameters like number of outputs, input bits entering the encoder at a time and number of memory elements respectively as indicated in the figure 1 below.

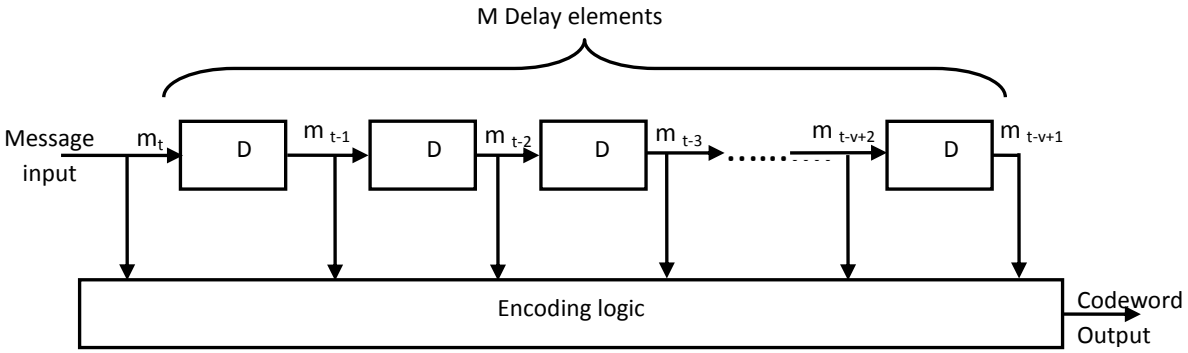

Fig 1: Structure of binary convolutional encoder

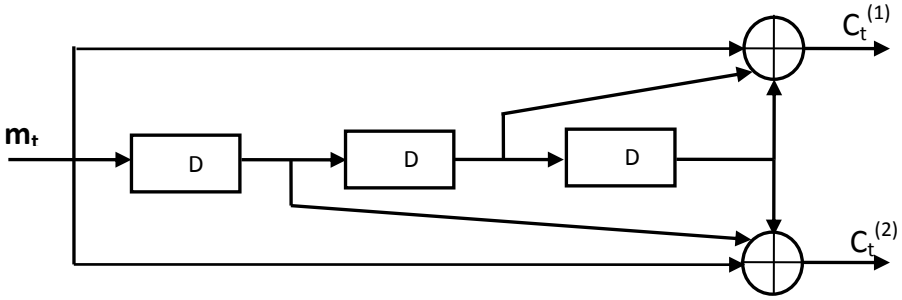

Fig 2: A (2, 1, 3) binary non-systematic feed-forward convolutional encoder.

An example of $(2, 1, 3)$ binary code is implemented and combined with cryptographic algorithm DES with a rate $R = 1/2$ is explained with a figure 2 shown above.

The output equation are given by

$$\left.\begin{aligned} c_t^{(1)} &= m_t \oplus m_{t-2} \oplus m_{t-3} \\ c_t^{(2)} &= m_t \oplus m_{t-1} \oplus m_{t-3} \end{aligned}\right\} \quad (2)$$

The codeword for the above diagram is hence generated as

$$c_t = \left(c_t^{(1)} c_t^{(2)}\right) \quad (3)$$

This equation indicates that, the codeword not only depends on the present input m_t but also on previous inputs like m_{t-1}, m_{t-2} and m_{t-3}. The constraint length is 4 and coding rate is $R = 1/2$.

The state diagram is constructed by the transition table of a given $(2, 1, 3)$ encoder which is depicted in figure 3. From this state diagram both encoding and decoding of information is possible.

Because of three memory elements, it consists of 4 states named as *00, 01, 10* and *11*. With the input *0* and *1* the state transition diagram is assembled.

In the decoding process, the trellis has to be drawn as shown in figure 4 and received sequence has to be traced out using decoding algorithm.

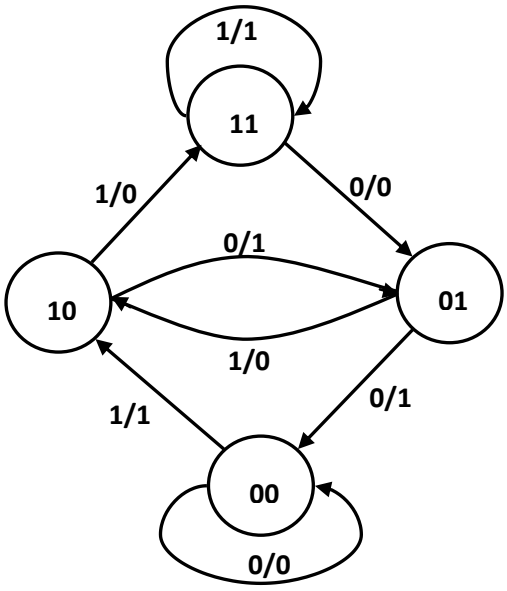

Fig 3: A state diagram of (2, 1, 3) convolutional encoder.

2.2 Convolutional decoder (Viterbi decoding)

The best known algorithm of decoding of the convolutional codes was introduced by A. Viterbi in 1967 [4]. The code sequence v which is transmitted over the channel and the received sequence r can be written as

$$\boldsymbol{r} = \boldsymbol{v} + \boldsymbol{e} \quad (4)$$

Where ***e*** is the error sequence.

The Viterbi algorithm finds a code sequence y such that it maximises the probability $\boldsymbol{p}(\boldsymbol{r}/\boldsymbol{y})$ and is as follows: $S_{i,j}$ is the state in the Trellis diagram that corresponds to the state

S_i at a time j. Every state in the trellis is assigned a value denoted $V(S_{i,j})$. L is the decoding path.

1.
   a. Initialize time j = 0.
   b. Initialize $V(S_{0,0}) = 0$ and all other $V(S_{i,j}) = 1$.
2.
   a. Set time j = j+1.
   b. For all i set $V(S_{i,j})$ to the best partial path metric going to state S_i at time j. To do this: first, calculate branch metric, and then add the branch metric to $V(S_{i,j-1})$.
3.
   a. For all i set $V(S_{i,j})$ to the best partial path metric going to state S_i at time j.
   b. If there is a tie for the best partial path metrics, then any one of the partial path metric may be chosen.
4. If $j < L$ go to step 2.
   a. Start trace back through the trellis by following the branches of the best survivor path.
   b. Store the survivor k symbol. These are currently decoded k information symbols.

Set time j = 0: go to step 2. Here is the start of new truncation window.

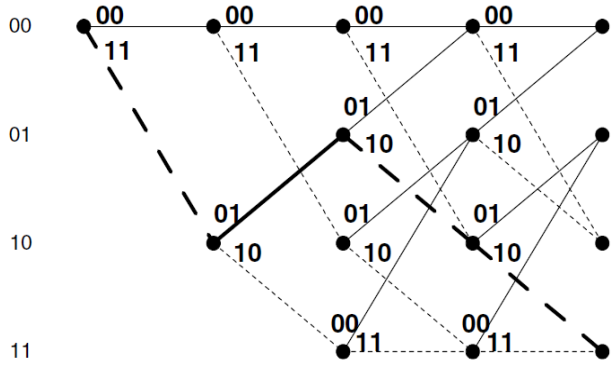

Fig 4: A (2, 1, 3) Trellis decoding structure.

3. DATA ENCRYPTION STANDARD (DES)

The generally used encryption scheme is based on the Data Encryption Standard (DES) adopted in 1977 by the National Bureau of Standards, now the National Institute of Standards and Technology (NIST), as Federal Information Processing Standard 46 (FIPS PUB 46)[ ]. The algorithm itself is referred to as the Data Encryption Algorithm (DEA). For DES encrypts blocks of 64-bit data using a 56-bit key. The algorithm transforms 64-bit plaintext in a sequence of steps into a 64-bit ciphertext. The similar steps, with the same key, are used for reversible process called as decryption to get back the plaintext [17].

3.1 DES encryption

The overall DES encryption scheme is shown in Figure 4. For the encryption scheme, there are two inputs functions: the plaintext to be encrypted and the key. In this case, the length of the plaintext must be 64-bits and the key is 56-bits.

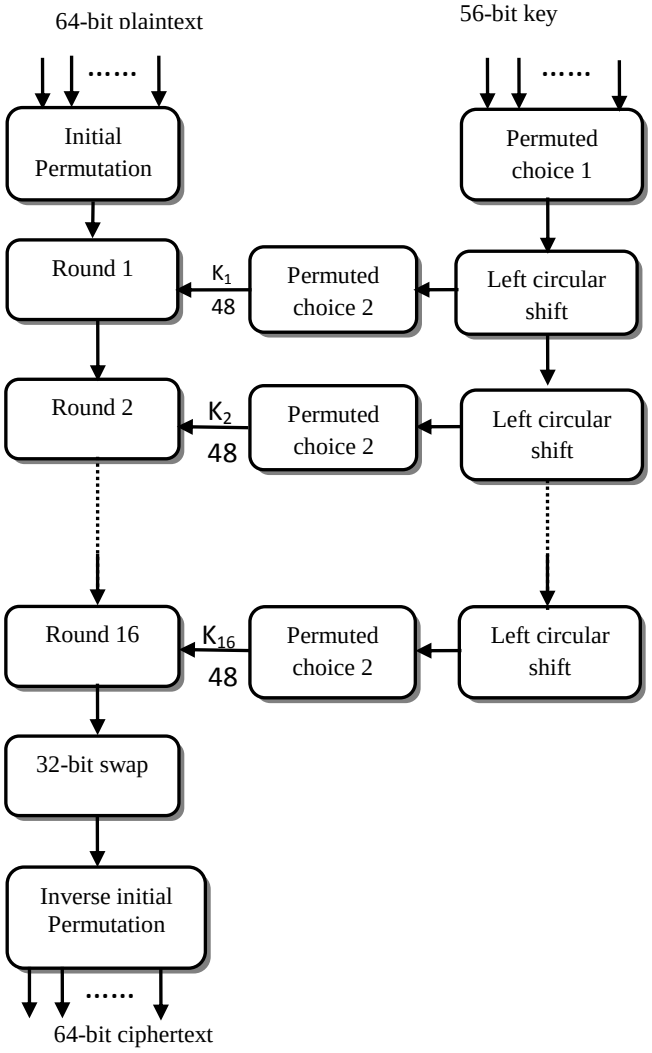

Fig 4: DES encryption structure [17].

Three steps are involved in the encryption process are -

- 64-bit plaintext passes through an initial permutation $[IP]$ that rearranges the bits to produce the *permuted input*.
- A phase consisting of 16 rounds of the similar function, which has both permutation and substitution functions. The output of the last (sixteenth) round will be consisting of 64 bits that are a function of the 64-bit input and 56-bit key. The right and left parts of the output are swapped to produce the **pre-output**.
- Finally, the pre-output is passed through a reverse permutation $[IP^{-1}]$ that is the inverse of the initial permutation function, to produce the 64-bit ciphertext.

With the exception of the initial and final permutations, DES has the exact structure of a Feistel cipher, a single round is as shown in figure 5.

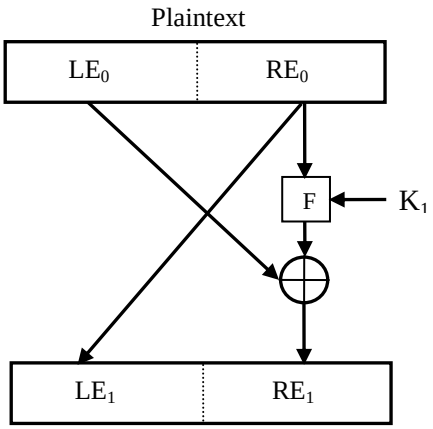

Fig 5: Single round of Feistel structure

shows the way in which the 56-bit key is used. Initially, the key is passed through a permutation function. Then, for each of the sixteen rounds, a *sub-key* (K_i) is produced by the combination of a left circular shift and a permutation. The permutation function is the same for each round, but a different subkey is produced because of the repeated shifts of the key bits.

3.1.1 Initial permutation and expansion

The initial permutation and its inverse are defined by tables, as shown in tables 1 and 2 respectively. The input to a table consists of 64-bits numbered from 1 to 64. The 64 entries in the permutation table contain a permutation of the numbers from 1 to 64. Each entry in the permutation table indicates the position of a numbered plaintext input bit in the output, which also consists of 64-bits.

Table 1. Initial Permutation $[\mathbf{IP}]$

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Table 2. Inverse Initial Permutation $[\mathbf{IP^{-1}}]$

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

The initial permutation $[IP]$ and its inverse $[IP^{-1}]$ are defined by tables, as shown in Tables 1 and 2, respectively. The input to a table consists of 64 bits numbered from 1 to 64.The 64 entries in the permutation table contain a permutation of the numbers from 1 to 64.
The permutation and inverse permutation is summarize by the following formulas:

$$X = (IP(M))$$
$$Y = IP^{-1}(X) = IP^{-1}(IP(M)) \quad (5)$$

If you examine the expansion table, you see that the 32 bits of input are split into groups of 4 bits and then become groups of 6 bits by taking the outer bits from the two adjacent groups. For example, if part of the input word is

Details of single round shows the internal structure of a single round structured as classic Feistel cipher. 64-bit plaintext is halved into intermediate value are treated as separate 32-bit quantities, labeled L (left) and R (right). The overall processing at each round can be summarized in the following formulas:

$$L_i = R_{i-1}$$
$$R_{i-1} = L_{i-1} \oplus F(R_{i-1}, K_i) \quad (6)$$

3.2 DES decryption

With any Feistel cipher, decryption uses the same algorithm as encryption; apart from that the application of the subkeys is reversed.

4. LAND MOBILE SATELLITE CHANNEL

The performance of a mobile satellite communications link can be determined by the propagation path between a satellite and mobile users. Coverage of extended service areas, especially in remote places, can only be achieved by using satellites either in geostationary orbit (GEO) or in non-GEO orbits [13][15]. Also, satellite navigation systems such as the global positioning system (GPS) are affected by similar propagation conditions. Typically L- (1–2 GHz) and S-bands (2–4 GHz) are used for land mobile satellite (LMS) services.LMS propagation is affected in different ways by the ionosphere, the troposphere and the environment surrounding the mobile receiver.

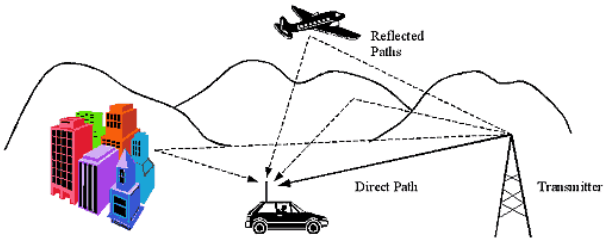

Fig 6: Land Mobile Satellite Channel model.

Also the modeling of environmental effects that is shadowing and multipath using Raleigh and Rician channels are addressed. In the above diagram 6, the component r2 reaches the mobile by reflection from the ground. Its strength depends on the constitutive parameters and roughness of the ground. Since this ray normally arrives with a negative elevation, it is not always received by a directional terminal antenna [14]. Similarly the diffuse components r3 and r4 account for the small scale fading in the received signal, which occurs due to the vector addition of reflections, diffractions and scattering from restricted objects. All the channel effects are multiplicative; however Additive White Gaussian Noise (AWGN) is also present in the system, as shown in figure 7.

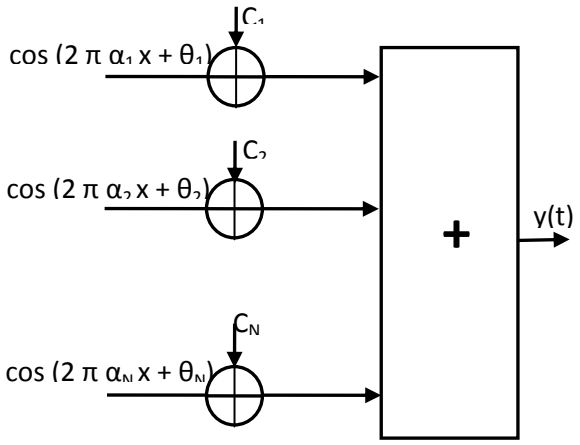

Fig 7: sum-of-sinusoids principle.

5. CRYPTO-CODING

A Crypto-coding as the one step algorithm in which two fields such as error correction and encryption functionalities are combined together is proposed.

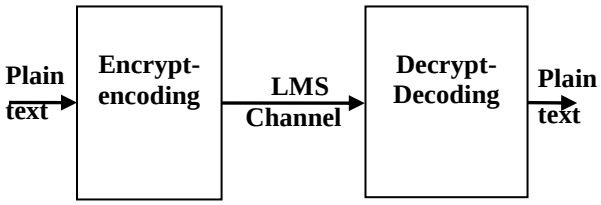

Fig. 8: BER Performance of AES-Turbo with code rate ½ over LMS and AWGN Channels.

The figure 8 gives the projected idea of crypt-coding, in which error-correction is embedded in encryption as a single primitive. It has a pair of algorithms ***(E, D)*** where ***E*** is called encrypt-coding algorithm and ***D*** is called decrypt-coding algorithm. ***(E, D)*** Satisfy the following conditions:

- Encryption ***(E, D)*** is a secure encryption scheme, which means it satisfies the correctness and the security conditions.
- Encoding ***(E, D)*** is an error-correction scheme and satisfies the coding condition also [7].

In cryptcoding if ***E*** and ***D*** to denote the encrypt-coding and decrypt-coding algorithm, respectively, the cryptcoding is realized in following two steps [10]:

1. ***E (K, M) = C,*** Encrypt-coding step in which an error resistant ciphertext C is created using the encryption key K.

2. ***D (K, C) = M,*** Decrypt-coding step in which the original message M is restored from the erroneous ciphertext C after transmission (Hamming – $C,C' \leq t$).

A new type of Encryption and Error Correction scheme which is named here as "A Combined Encryption and Error Correction Scheme: DES-Convolution" has been introduced [9]. This combined system is presented in Fig. 8.

This Combined system will help in modernized mono-blocks in a single step [8].

6. EXPERIMENTAL RESULTS

The bit error rate performance of overall Crypto-Coding system is compared with conventional Crypto-Coding over land mobile satellite channel in Figures 9 and 10.

Figure 9, demonstrates AWGN and LMS channel performances for AES-Turbo technique. The turbo coding of this single step algorithm has relative prime interleaver. Turbo code of this crypto-coding has code rate ½. Because of multipath fading the performance of LMS channel is poorer than AWGN as demonstrated.

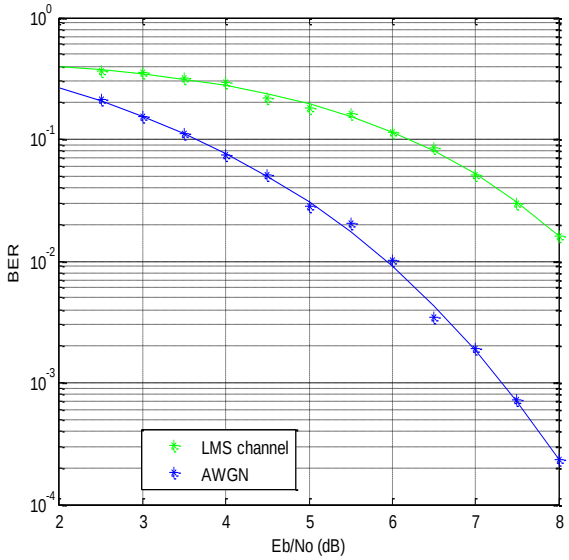

Fig. 9. BER Performance of DES-Convolution with code rate ½ over LMS and AWGN Channels.

Figure 10, demonstrates BER performance of DSE-convolution over Raleigh and Rician channels and observed that the implemented LMS channel gives better performance over individual channels.

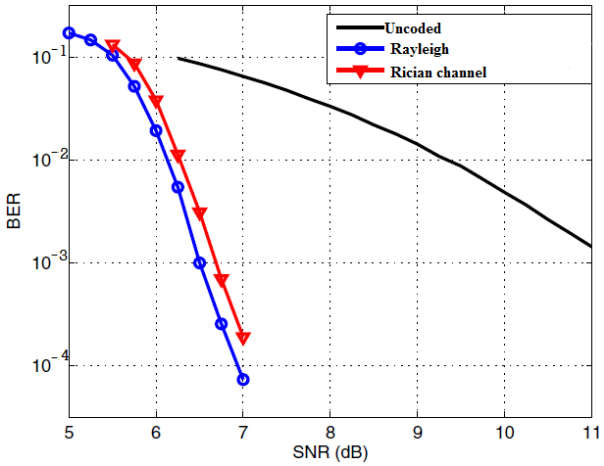

Fig 10: BER Performance of DES-Convolution with code rate ½ over Rayleigh and Rician Channels.

Figure 11, demonstrates bit error rate performance for DES-Convolution as a single technique and traditional approach. With signal to noise ratio of 10db having code rate of convolutional code ½ the results are almost similar.

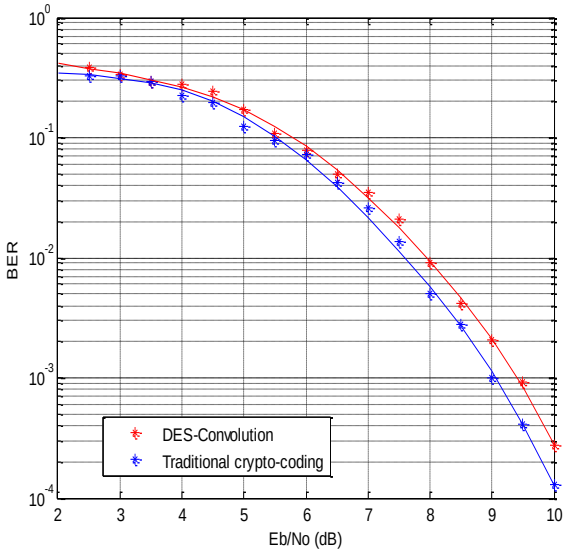

Fig 11: BER Performance of DES-Convolution with code rate ½ over LMS and AWGN Channels.

The figure 12, demonstrates the analysis of conventional crypto-coding with code rate ½ and crypto-coding. Over land mobile satellite channel the BER performance is upto 10^{-3} for single iteration. as number of iterations increases the performance.

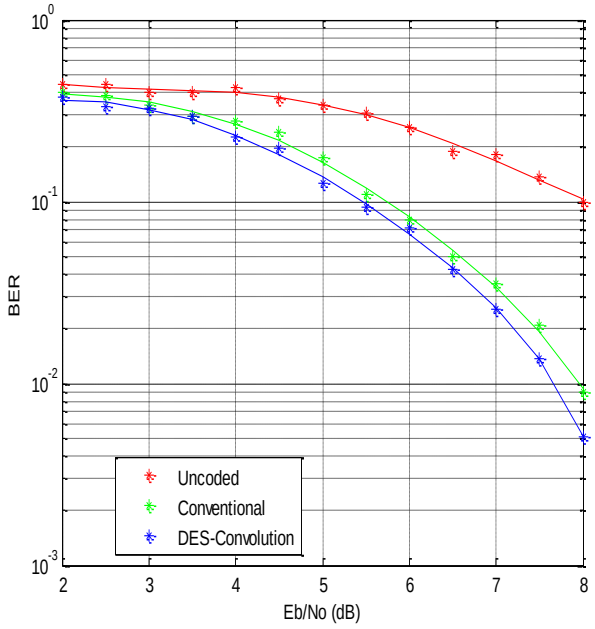

Fig. 12. BER Performance of Conventional Crypto-Coding at the rate of ½ over land mobile satellite channel.

In figure 13, the conventional crypto-coding is observed for lower bit error rate till up to 10^{-6} to 10^{-7} by making burst error to random error with different interleavers. The semi-random interleaver known as S-random interleaver shows better performance than relative prime and random interleavers as shown. The code rate has also impact on BER performance improvement.

The following BER performances of Crypto-Coding, in a single step are obtained with code rate 1/3 after 5 iterations.

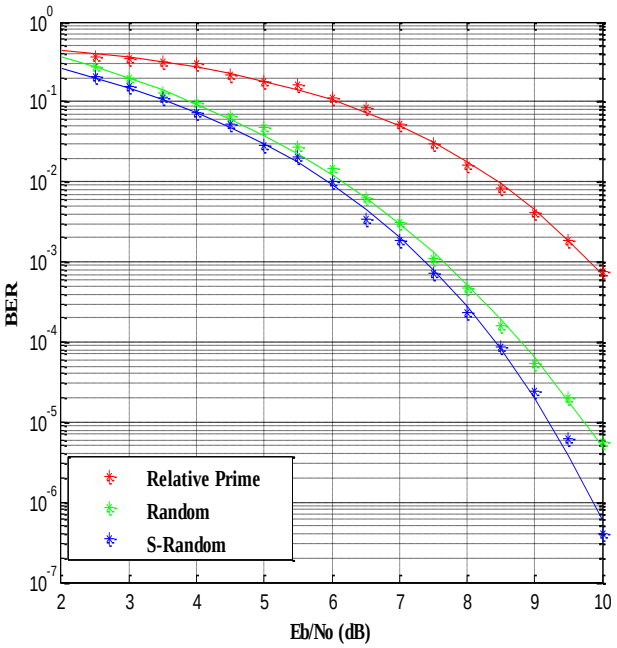

Fig. 13. BER Performance of Conventional Crypto-Coding at the rate $^{1}/_{3}$ over land mobile satellite channel

7. CONCLUSION

In this paper, the concept of combining cryptography-error correction as a single algorithm, which is called here as "Crypto-Coding" has been investigated. In the algorithm called DES-convolution, for the efficient transmission convolution code is embedded in DES encryption algorithm is developed and investigated on land mobile satellite channel. The performance is analyzed in conventional way i.e. encryption/encoding and decryption/decoding sequentially, and also using single step, the BER result is found to be 10^{-4}.

The performance is also examined on Rayleigh and Rician channels, both are found almost similar.

Investigating the result analysis of figure 13 indicates that the performance of Viterbi is improved by using different interleavers. The crypto-coding with s-random interleaver lowers the BER up to 10^{-7}.

This overall modification is devised to enhance the efficiency of the system as a single block.

8. REFERENCES

[1] A. Mahmood, "Method to Improve Channel Coding Using Cryptography," world academy of science, Engineering and Technology, pp. 525-528, 2008.

[2] N. Zivic, "Concatenation and Turbo Principle of Channel Coding and Cryptography," IJCSNS International Journal of Computer Science and Network Security, VOL. 8,October 2008.

[3] A. J. Viterbi, "Error Bounds for Convolutional Codes and an Asymptotically Optimum Decoding Algorithm," IEEE Trans. Inf. Theory, IT-13, pp. 260–9, 1967.

[4] N. Zivic and C. Ruland "Parallel Joint Channel Coding and Cryptography," International Journal of Electrical, Computer, and Systems Engineering, pp. 140 -144, 2010.

[5] D. Gligoroski, S. J. Knapskog, and Suzana Andova, "Crypto-coding - Encryption and Error-Correction Coding in a Single Step," 2007.

[6] S. J. Knapskog, "New Cryptographic Primitives (Plenary Lecture)," 7th Computer Information Systems and Industrial Management Applications IEEE computer society, pp. 3-7, 2008.

[7] C. N. Mathur, K. Narayan, and K.P. Subbalakshmi "High Diffusion Cipher: Encryption and Error Correction in a Single Cryptographic Primitive," pp. 1-16.

[8] H. CAM, V. OZDURAN, and O. N. UCAN," A combined encryption and error correction scheme: AES-Turbo," Journal of electrical and electronics engineering year:, vol. 9, Number 1, pp. 891-896, 2009.

[9] D. A. Moghadam and V. T. Vakili, "Enhanced Secure Error Correction Code Schemes in Time Reversal UWB Systems", Wireless Personal Communications , Volume 64, Issue 2, pp 403-423, Springer , May 2012,

[10] J. Gwak, S. KimShin and H. M. Kim, "Reduced Complexity Sliding Window BCJR Decoding Algorithms for Turbo Codes", Cryptography and Coding , Lecture Notes in Computer Science Volume 1746, , pp 179-184, Springer , 1999.

[11] H. Kaneko, and E. Fujiwara, " Joint Source-Cryptographic-Channel Coding Based on Linear Block Codes", Applied Algebra, Algebraic Algorithms and Error-Correcting Codes ,Lecture Notes in Computer Science Volume 4851, pp 158-167, Springer , 2007.

[12] M. Padmaja and S. Shameem, "Secure Image Transmission over Wireless Channels", International conference on Computational Intelligence and Multimedia Applications, Vol. 4, pp. 44 – 48, dec. 2007.

[13] M. A. El-lskandarani, S. Darwish, and S. M. Abuguba," A robust and secure scheme for image transmission over wireless channels", 42nd Annual IEEE International Carnahan Conference on Security Technology(ICCST) , pp. 51 – 55, 2008.

[14] Qian Mao, Chuan Qin," A Novel Turbo-Based Encryption Scheme Using Dynamic Puncture Mechanism", Journal of Networks, Vol 7, No 2 , pp. 236-242, Feb 2012

[15] M. A. El-Iskandarani, S. Darwish, and S. M. Abuguba ," Reliable wireless error correction technique for secure image transmission", 43rd International Carnahan Conference on Security Technology, pp. 184 – 188, Oct. 2009.

[16] Y. Liang , H. V. Poor and S. Shamai," Secure communication over fading channel", IEEE Trans. On Information Theory, 2006.

[17] W. Stallings, "Cryptography and network security principles and practice", fifth edition, Prentice Hall, 2011.

[18]