Encrypted Block Code

Ahmed S. Hadi *Ali H. Mahdi*
Department of Information and Communication Engineering
Al_Khawarizmi College of Engineering
University of Baghdad

Abstract

All coding algorithms including the linear block code provides explicit ways of ensuring that message remains legible even in the presence of errors, but without security. So a modified method to the linear block code that provides both error free and encryption will be present.

The information are encoded and encrypted at the same time. The encryption will be done by using both permutation and Hill cipher, while the decryption will be done by using Hill cipher only.

Keywords : Error Free Coding, Security, Linear Block Code, permutation, and Hill cipher

الخلاصة

جميع خوارزميات الترميز بما في ذلك ترميز الكتلة الخطية يوفر طرقا واضحة لضمان أن تبقى الرسالة سليمة حتى في وجود الأخطاء ولكن من دون حماية. لذلك تم تحسين ترميز الكتلة الخطية لتوفر كلاً من تصحيح الأخطاء والتشفير في آن واحد.

حيث سوف يتم ترميز المعلومات وتشفيرها في نفس الوقت. التشفير سيتم باستخدام كلاً من التقليب وشفرات هيل، في حين سوف يتم فك التشفير باستخدام شفرات هيل فقط.

1. Introduction

The recent developments in the wireless communication and internet makes the data vulnerable to unauthorized use and has caused significant economical losses for the contents producers and rights holders. This push the data owners to increase the security of their data. This tight security means more losses to the data owner, because they have to increase the channel capacity, which mean more money to be given to the channel owner.

Therefore, a recent research and development efforts have been proposed for solve this problem. One solution is to encrypt the compressed data, where it's first encrypt and then compressed the data [3], This method will not change the channel capacity. [2] and [1] use both encryption and source coding at the same time, by splitting the intervals of arithmetic code. [4] and [5] encrypts part of the data instead of encrypting all the data, which is also applied to the source coding too. Our proposed method is to be applied to the channel coding not to the source coding, this method have no effect on the data compression gained by the source coding.

The proposed method encrypts the encoder it self. This method will encrypt and encode the data at the same time, which will leads to merging both the encoder and encrypter blocks into one block.

The organization of this paper is as follows. Section 2 illustrates the proposed method. The Illustrative example for the proposed method is presented in section 3. Some concluding remarks are given in section 4.

2. The Proposed Method

Before proposing our method, we have to know the structure of the systematic linear block code, as shown below:

$$C_{sys} = [m]_{1*k} \cdot [G_{sys}]_{k*n} \qquad (1)$$

$$= [m]_{1*k} \cdot [P_{k*(n-k)} : I_k] \qquad (2)$$

$$= [m_{1*k} P_{k*(n-k)} : m_{1*k} I_k] \qquad (3)$$

$$= [b_{1*(n-k)} : m_{1*k}] \qquad (4)$$

$$C_{sys} = [b_0 b_1 \ldots b_{n-k-1} : m_0 m_1 \ldots m_{k-1}] \qquad (5)$$

Thus the systematic linear block code is consisting of two parts, the parity check part and the message part, as shown in 5.

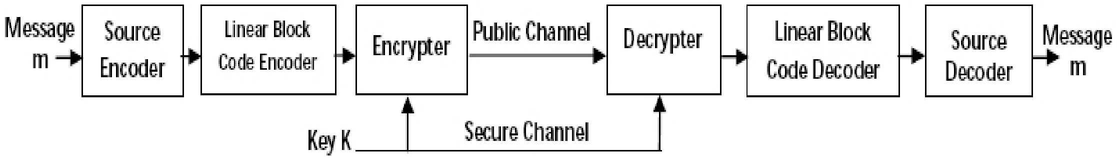

***Figure 1: The Conventional system**.*

Where b is the parity bits that responsible of error free coding, m is the message bits, k and n is the length of the message bits before and after encoding. More details about the linear block code can be found in [6] - [10].

The conventional methods was accomplish by encoding the message to produce the systematic code as in 5, then encrypt the code, as shown in fig. 1.

In order to keep the code without error the parity bits must be not changed, so we will not encrypt the parity bits. Our proposed method is to encode and encrypt the message at the same time, by encrypting the message bits $m_0\, m_1 \ldots. m_{k-1}$ of the systematic code. This can be done indirectly by encrypting the identity matrix of the generator matrix Gsys that responsible about making the message appear at the end of the code, or replacing the identity matrix by encrypting matrix, as follows:

$$C(encrypted)_{sys} = [m]_{1*k} \cdot [P_{k*(n-k)} : E_k] \quad (6)$$

$$= [m_{1*k} P_{k*(n-k)} : m_{1*k} E_k] \quad (7)$$

$$= [b_{1*(n-k)} : m(encrypted)_{1*k}] \quad (8)$$

Where E is the encrypting matrix.

The encryption of the identity matrix will tend to encrypt the message by its turn. Thus, the encoder will simultaneously encode and encrypt the message bits only.

So, the proposed system will not need an encryption algorithm to encrypt the message; the message will be encrypted by the encoder, as shown in fig. 2.

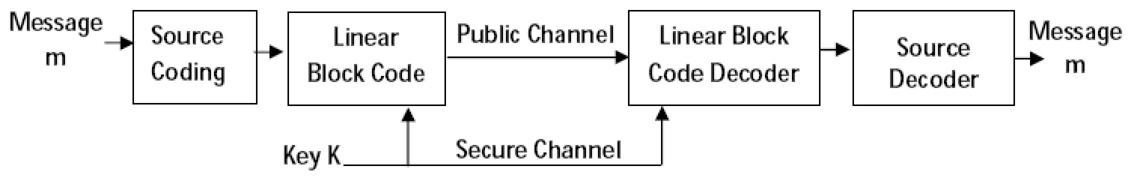

Figure 2: the proposed system

The encryption of identity matrix can be applied by the following processes:

- Permutation of the identity matrix in order to perform the transposition cipher technique. The permutation will be done according to predetermined key K, as shown in fig. 3.
- Consider the resulting matrix as a Hill Cipher matrix, which is a substitution cipher technique. This matrix will be considered as an encryption key, which will be used to get the encrypted message. So, the encoder will encode and encrypt the message simultaneously.

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \xrightarrow[\text{According to the Key} \; K=[3, 1, 2]]{\text{Columns Permutation}} \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

The receiver will not need any key to decrypt the message, because the inverse of the Hill Cipher matrix will be used to decrypt the encrypted message

$$\begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix} \xrightarrow[\text{According to the Key} \; K=[k\,1\,.\,.\,.\,2]]{\text{Columns Permutation}} \begin{bmatrix} 0 & 1 & \cdots & 0 \\ 0 & 0 & \cdots & 1 \\ \vdots & \vdots & \vdots & \vdots \\ 1 & 0 & \cdots & 0 \end{bmatrix}$$

Figure 3: Permutating the rows of identity matrix according to the key K

3. Illustrative Example

Consider a (6,3) linear block code that have a generator matrix in systematic form $\boldsymbol{G_{sys}}$

$$G_{sys} = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

This generator matrix have 3*3 identity matrix, so we will use key of length three, K=3, 1, 2. The identity matrix will be permutated as shown in fig. 4.

Then the generator matrix after permutating the identity matrix will be

$$G_{per\_sys} = \begin{bmatrix} 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 \end{bmatrix}$$

The code after permutating the identity matrix is shown in table 1.

Message $m_0m_1m_2$	**Code** $c_0c_1c_2c_3c_4c_5$
0 0 0	0 0 0 0 0 0
0 0 1	1 1 0 1 0 0
0 1 0	1 0 1 0 0 1
0 1 1	0 1 1 1 0 1
1 0 0	0 1 1 0 1 0
1 0 1	1 0 1 1 1 0
1 1 0	1 1 0 0 1 1
1 1 1	0 0 0 1 1 1

Consider that we received the code r =101110, which is corresponding to the message “101”, which is picked up from table 1. First of all we have to check if this code have an error or not, as follows,

a) If we don’t have the key, then the parity check matrix will be

$$H^T = \begin{bmatrix} I_3 \\ P_{3*3} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

The Superscript $^{\text{“T”}}$ means the transpose. Then the syndrome will be

$S=r\,.H^T =011$

This means that the received code is in error, while the code is correct. This will make the eavesdropper to imagine that he had received a wrong code that need to be corrected. So, he will correct the code and then take the last three bits as the message, thus the original data will be hidden for the observer.

b) If we have the key, then we will permutate the identity matrix, so that the parity check matrix will be :

$$H^{T} = \begin{bmatrix} I_{per\_2} \\ P_{3*3} \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

Then the syndrome will be

S= r .H^{T} =000

This is meaning that the received code has no error, so we will take the last three bits "110" as the message (but before encryption). In order to decrypt the message, there must be the inverse of the Hill Cipher matrix

$$I_{per} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$

$$I_{decryption} = Inverse\ (I_{per}) = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

$$m = [c_3 \quad c_4 \quad c_5] * I_{decryption}$$

$$= [1 \quad 1 \quad 0] \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

$$= [1 \quad 0 \quad 1]$$

After applying the message to the inverse Hill matrix, we will get the original message "101".

4. Conclusions

We proposed a method that encrypt and encode the linear block code at the same time, without effecting on the capability of the code to correct the errors. The proposed method merges the encoder and encrypter blocks into one block. The encryption is done first by permutation the identity matrix of the generator matrix of the linear block code according to a key known to the encoder, while the decoder uses Hill cipher in order to get the original message. The proposed system used the Hill Cipher technique, which considered very strong substitution technique against a cipher-only attack.

References

1. J. Wen, H. Kim and J. D. Villasenor, “Binary Arithmetic Coding with Key-Based Interval Splitting”, IEEE Processing Letters, Vol. 13, No.2, February 2006.

2. J. Wen, H. Kim and J. D. Villasenor, “Secure Arithmetic Coding”, IEEE Transactions on Signal Processing, Vol. 55, No. 5, May 2007.

3. M. Johanson, P. Ishwar, V. Prabhakaran, D. Schonberg, and K. Ramchandran, “On Compressing Encrypted Data”, IEEE Transactions on Signal Processing, Vol. 52, No. 10, October 2004.

4. H. Cheng and X. Li, “Partial Encryption of Compressed Images and Videos”, IEEE Transactions on Signal Processing, Vol. 48, No. 85, August 2000.

5. A. Servetti and J. C. De Martin, “Perception-Based Partial Encryption of Compressed Speech”, IEEE Transactions on Speech and Audio Processing, Vol. 10, No. 8, November 2002.

6. J. H. V. Litt, Introduction to Coding. New York: Springer-Verlag, 1982.

7. Richard W. Hamming, Coding and Information Theory. Second Edition, Prentice-Hall, 1986.

8. M. Y. Rhee, Error-Correcting Coding Theory. McGraw-Hill, 1989.

9. S. G. Wilson, Digital Modulation and Coding. Prentice-Hall, 1996.

10. Robert M. Morelos, The Art of Error Correcting Coding. John Wiley and Sons, 2002.