IOSR Journal of Engineering (IOSRJEN)
ISSN: 2250-3021 Volume 2, Issue 6 (June 2012), PP 28-32
www.iosrjen.org

Combining Cryptography with Channel Coding

Sunaina Sharma
Lovely Professional University Jalandhar, India

ABSTRACT : - *Cryptography is a form of hiding the text so to increase the security of the information. It can also be defined as the process of converting the valuable information into some form of non-scene information which can be understand able by the sender and the intended receiver only. On the other hand the main purpose of using coding is to reduce the error probability and to increase the efficiency of the channel. There are mainly two types of coding used in every system i.e. source coding and channel coding. On may not confuse between the two coding technique because the purpose of using two technique is very much different as source coding is used to reduce the redundancy while in channel coding redundant bits are being added in known manner to reduce error.*

Keywords *– Channel Coding, Cryptanalysis, Cryptography, Cryptology, Source Coding***.**

I. INTRODUCTION

This paper provides the information how to merge channel coding with the cryptography to provide more security to the signal. The general communication system has been shown below:

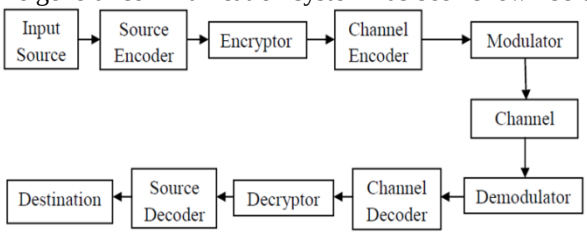

Fig 1.1: Communication System

In this age of information there is increasing importance not only of speed, but also of accuracy in the storage of, retrieval and transmission of the data. The channel over which the messages are transmitted often imperfect. Error correcting codes are a kind of safety net – the mathematical insurance against the vagaries of imperfect material word. All the real life channels are affected by the noise. Noise causes discrepancies (error) between the input and the output data sequences of a digital communication system. For a typical noisy channel, the probability of bits error rate may be as high as 10^{-2}. This means that, on average, 1 bit out of 100 bits that are transmitted over this channel gets flipped. For most application, this is far from adequate level. Since World War I and the advent of the computer, the methods used to carry out cryptology with channel coding have become increasingly complex and its application more widespread. During this time when the Internet provides essential communication between tens of millions of people and is being increasingly used as a tool for commerce, security and error free communication becomes a tremendously important issue to deal with. This paper deals with a system to increase the security and to decrease the battery usage. The purposed block dig is shown below [6] [8]:

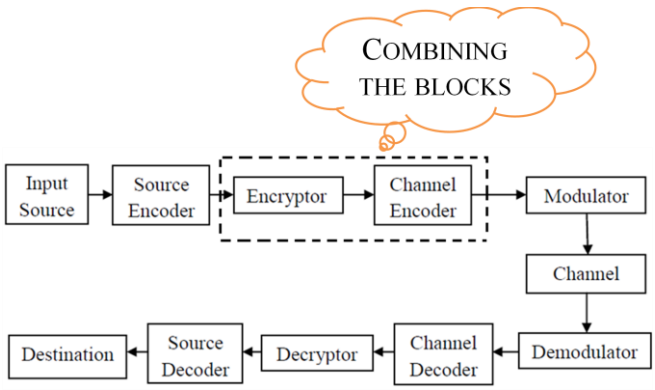

Fig 1.2: Purposed Model

II. CRYPTOGRAPHY

Cryptography is the study of secret (crypto) writing (graph). Attempt to retrieve plain text or key is called Cryptanalysis. Cryptanalysis and Cryptography together are called Cryptology. Cryptanalysis to the science and art of breaking them with the knowledge of the sender; while cryptology, often shortened to just crypto, is the study of both. The input to an encryption process is commonly called the plaintext, and the output the cipher-text [1]. Within the context of any application-to-application communication, there are some specific security requirements, including [7]:

- Authentication: The process of proving one's identity. (The primary forms of host-to-host authentication on the Internet today are name-based or address-based, both of which are notoriously weak.)
- Privacy/confidentiality: Ensuring that no one can read the message except the intended receiver.
- Integrity: Assuring the receiver that the received message has not been altered in any way from the original.
- Non-repudiation: A mechanism to prove that the sender really sent this message.

Secrecy is the heart of the cryptography. Encryption is a practical means to achieve information secrecy, which is the transformation of original "meaningful message" called plain text to "unintelligible message" called Cipher text. In order to restore information, an encryption transformation must be reversible and it is called Decryption. A secret key is required for decryption also. An encryption algorithm and decryption algorithm plus the description on the format of the message and a key form a cryptographic system or cryptosystem. There are two types of ciphers:

Transposition cipher: - here the rearrangement of the word is done. For example "Hello" becomes "elohl".

Substitution cipher: - Here the word or the letter is being replaced by some other consecutive world or letter. For example "fly at once" becomes "gmz au podf"

III. CODING

There are two type of coding used when the signal/ informa- tion is send from one place to another.

3.1 SOURCE ENCODER

The information transmitting rate should be smaller than the so-called channel capacity. In order to reduce the information rate, source coding schemes are used which are implemented by the **SOURCE ENCODER** in the transmitter and the source decoder in the receiver. Suppose ZEBRA is to be send [2]. First step is to convert the word into ASCII format which is a fixed length format. ASCII for ZEBRA is "1010101 0110110 0010110 0010111 0001110". Now using Huffman source encoder one has to find the probability of each word i.e.

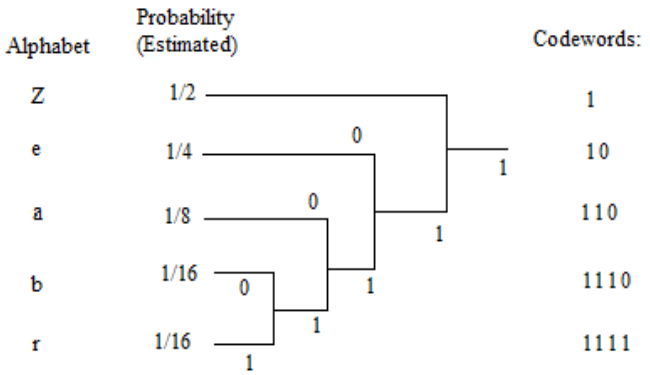

Fig 2.1: Huffman coding

Similarly for run-length the code becomes (1,1) (1,0) (1,1) (1,0) (1,1) (1,0) (1,1) (1,0) (2,1) (1,0) (2,1) (3,0) (1,1) (1,0) (2,1) (3,0) (1,1) (1,0) (3,1) (3,0) (3,1) (1,0).

3.2 CHANNEL ENCODING

Error control coding is a method to detect and possibly correct errors by introducing redundancy to the stream of bits to be sent to the channel [3]. The **CHANNEL ENCODER** will add bits to the message bits to be transmitted systematically. After passing through the channel, the Channel decoder will detect and correct the

errors. A simple example is to send '000' ('111' correspondingly) instead of sending only one'0' ('1' correspondingly) to the channel. Due to noise in the channel, the received bits may become '001'. But since either '000' or '111' could have been sent. By majority logic decoding scheme, it will be decoded as '000' and therefore the message has been a '0'.

In general the channel encoder will divides the input message bits into blocks of k messages bits and replaces each k message bits block with a n-bit code word by introducing (n-k) check bits to each message block. Some major codes include the Block Codes and Convolution Codes. Rather, we have not yet found general methods to find good nonlinear codes. There are good linear codes, however, and they are attractive for many reasons. Almost all of the best codes we know are linear. Most of the strongest theoretical techniques are useful only for linear codes. It is a type of block code. A code to be linear has to follow the following condition:

i) The sum of two codewords belong to a codeword belonging to code is also a codeword belonging to a code
ii) The all zero codeword is always a codeword.
iii) The minimum hamming distance between two codewords of linear code is equal to the minimum weight of any non-zero codeword, i.e., d*=w* [5].

IV. DRAWBACKS OF LINEAR CODES

There are mainly two draw backs of a linear code i.e.

i) To decode a linear code it is important to detect the whole block before start decoding so little bit time consuming.
ii) In linear codes the complete block is subtracted by the error vector of the code. It might happen in some cases that error vector may change from codeword to codeword [5].

V. HOW TO ENCODE AND ENCRYPT

The following steps should be followed to encode and encrypt the signal.

i) First take any signal (voice, image, random bits etc) and convert it into binary.
ii) Now encode the signal by multiplying the binary signal with the G matrix.

$$G = \begin{bmatrix} 0\,0\,1\,1\,1\,0 \\ 0\,1\,0\,1\,0\,1 \\ 1\,0\,0\,0\,1\,1 \end{bmatrix}$$

Codeword = information* G

Messages (D)	Code words (C)
0 0 0	0 0 0 0 0 0
0 0 1	0 0 1 1 1 0
0 1 0	0 1 0 1 0 1
0 1 1	0 1 1 0 1 1
1 0 0	1 0 0 0 1 1
1 0 1	1 0 1 1 0 1
1 1 0	1 1 0 1 1 0
1 1 1	1 1 1 0 0 0

iii) As the channel adds some noise one can add noise by awgn command in Matlab.
iv) For encryption a key is given and according to that key no of keys are generated by LFSR (Linear Feedback Shift Register).
v) And every time the block of information is multiplied with the particular G matrix only [6].

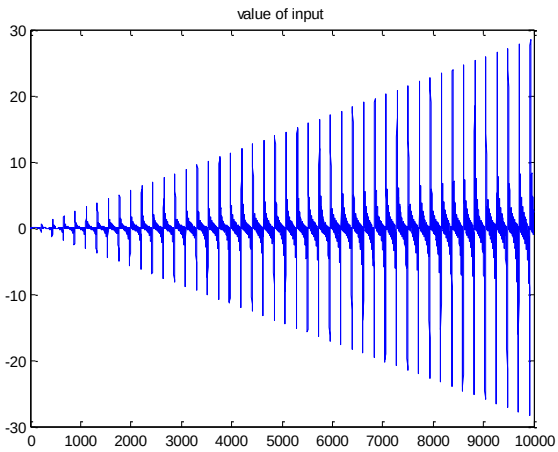

Fig 5.1: Sound Signal

5.1 Decoding

First the error is find out by multiplying the received signal by the parity matrix if at the resultent is zero that means no error is there and if resultent is not zero then the standard array is prepared which is defined in next section. The first row of the array is coset leader. Than this error is being subtracted for every coset leader and then this value is decoded. While decoding the received signal is multiplied by the H matrix and then the multiplied signal is back converted into sound [6].

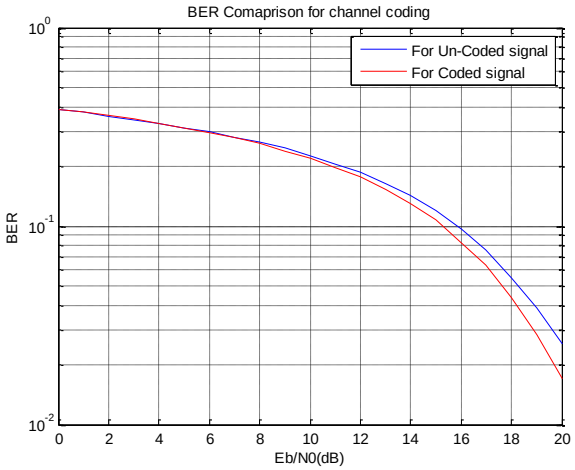

Fig 5.2: BER Comparison for between coded and un-coded signal.

Note: It must be noted that there is no reverse process of recovering signal back by rounding process. So if rounding is done then there will be some signal error at the receiver.

VI. STANDARD ARRAY

The standard array is a way of tabulating all decoding spheres. Let **0**, **c**2, **c**3, . . . , $\mathbf{c}_q^k$ be the q^k codewords in an (n, k) linear code. Form the table of Figure 6.1 as follows. Write all the codewords in the first row. Of the non codewords in $GF(q)^n$ lying closest to the all-zero codeword, choose any word and call it **v**1. Write $\mathbf{0} + \mathbf{v}_1$, $\mathbf{c}_2 + \mathbf{v}_1$, $\mathbf{c}_3 + \mathbf{v}_1$, . . . , $\mathbf{c}_q^k + \mathbf{v}_1$ in the second row. Continue in this way to form additional rows. At the j^{th} step, choose $\mathbf{v}_j$ as close as possible to the all-zero word and previously unused, and write $\mathbf{0} + \mathbf{v}_j$, $\mathbf{c}_2 + \mathbf{v}_j$, $\mathbf{c}_3 + \mathbf{v}_j$, . . . , $\mathbf{c}_q^k + \mathbf{v}_j$ for the j^{th} row. Stop when no unused element of GF(q)n remains to start a new row. The words in the first column are called coset leaders [4].

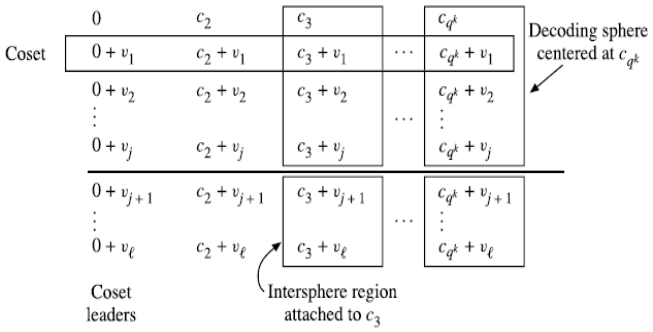

Fig 6.1: Standard Array

References

Journal Papers:

[1] G. Julius Caesar, John F. Kennedy, Security Engineering: A Guide to Building Dependable Distributed Systems.

[2] Anonym, Coding In Communication System.

[3] Natasa Zivic And Christoph Ruland, Channel coding as cryptographic Enhancer, *Wseas Transactions On Communications*, Issue 2, Volume 7, February 2008.

[4] Gary C. Kessler, An Overview of Cryptography, *Auerbach*, September 1998.

Books:

[5] Richard E. Blahut, *Algebraic code for data transmission* (Cambridge University Press, 2003).

[6] Ranjan Bose, *Information theory, Coding and Cryptography* (Tata McGraw Hill, 2008).

Theses:

[7] Sunaina Sharma, Combining Cryptographic Operation for complexity reduction, Lovely Professional University Jalandhar, M.Tech, 2012.

[8] Ravi Shankar, Combining cryptographic operations for complexity reduction, NIIT, M.Tech, 2008.

Website:

[9] WWW.WEKIPEDIA.COM.