ISSN No. 0976-5697

Volume 7, No. 1, January-February 2016

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

System Identification &Clustring

Prof. Saroj Singh
Dept. Computer Science & Engineering
Delhi Engineering College
Ladiyapur, Faridabad, India

Abstract: If you think technology can solve your security problems, then you don't understand that problems and you don't understand the technology. Speech is the most common means of communication and cryptography is the mean of achieving secure communication in the presence of the third party. Secure voice is the term in cryptography for encryption of voice communication over a range of communication types such as ratio or telephone.

Keywords: **c**ommunication; technology; cryptography; decryption; encryption;

I. Introduction

Speech is most common means of communication and cryptology is a means of achieving secure communication in the presence of a third party. Secure voice is a term in cryptology[1] for encryption of voice communication over a range of communication types such as ratio or telephone.

A. Cryptology of speech signals

- Narrowband Systems
- Wideband Systems
- Speech Scrambling
  a) Baseband Inversion
  b) Variable band Inversion
  c) Split band inversion

- Speech Encryption
  a) Hardware based encryption scheme
  b) Software based encryption scheme

B. Voice channel attributes

C. Channels

D. Scramblers

II. Cryptology of Speech Signals

Definition: Cryptology is also known as cryptography is the practice of techniques and methods that are used for providing secure communication. Cryptography is performed in the presence of a third party. Application of cryptology varies from passwords to electronic commerce.

Speech is most common means of communication and cryptology is a means of achieving secure communication in the presence of a third party. Secure voice is a term in cryptology for encryption of voice communication over a range of communication types such as ratio or telephone.

The cryptology of speech signals[2] makes use of two types of systems namely narrowband and wideband.

- Narrowband Systems: In narrowband systems bandwidth of the message does not exceed the channel's coherence bandwidth. The channel under consideration is extremely narrow such that its frequency responses are flat. These are used in telephony and audio spectrum.
- Wideband Systems: wideband systems are used for short range bandwidth communication. The transmission occurs in such a manner that it does not interfere with other narrowband systems that are using the same frequency.

III. Speech Scrambling

Definition: Scrambler is a device that inserts the signals at the transmitter end to make the message unintelligible at the receiver end. The operations of this device are carried out in an analog domain.

Basically scrambler[3] is a device that used for inverting the signals so that they are not recognizable at the receiver's end. There are three types of inversions.

A. Base band inversion:

Base band inversion inverts the signals around a pre-set frequency. The principal disadvantage of this scheme is that the frequency never changes. This scheme is not much in use.

B. Variable band inversion:

Variable band inversion inverts the signals around a constantly changing frequency.
Disadvantage:

Modem noise at the beginning of transmission[4].
Repeated checking sounds as the inverter frequency changes.

C. Split band inversion:

Split band inversion splits the signal into two frequencies and then inverts them separately. This is the most secure method.

IV. Speech Encryption

Speech encryption[5] is a secure and much stronger method. These can be classified as:

Hardware based encryption scheme: this employs hardware to encrypt the conversation and requires no computer device.

Advantage: It is simple to use.
Disadvantage: It is expensive
Uses: Used in cellular phones and radio.

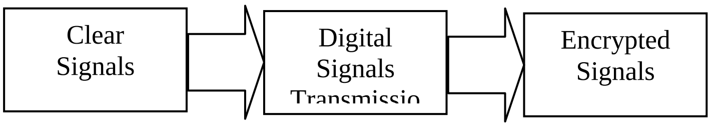

Figure1. Uses in cellular phones and radio.

Software based encryption scheme: these requires computers and are free of cost.

V. Voice Channel Attributes

The voice systems are made up of various subsystems that process the voice information. Voice channel[6] attributes depends on whether the voice is digitized or is presented in an analog format. The users of the data channels are not concerned with the packets delays of up to two to three seconds while the users of the voice channels are aware of such delays. In many multi channel systems, the voice and data signals are multiplexer and are treated identical in the communication pipeline.

Throughput delay:

Definition: Throughput delay is the sum of all time delays ranging from coders/decoders or any other digitization techniques that are introduced to a communication channel.

A. Digital voice encryptor

The digital voice encryptor[7] is similar to a data encryptor and uses a vocoder (voice coder/decoder) to achieve maximum bandwidth.

- Components of digital voice Encryptor

The digital voice encryptor uses two components:

- Digitizer: it is used to convert between the speech signals and digital signals.
- Encryption System: It is used to provide confidentiality.

The encrypted process can be explained in the following steps:

- Convert the voice signal into digital data stream.
- The digital data stream is then XOR – ed with the key stream generator's output bit stream.
- The encrypted data stream signal is transmitted over the communication channel.
- Advantages: Security level depends upon the security of the key stream generator.
- Disadvantages: Poor quality channels
- Recognition of voice channel bandwidth

B. Analog voice encryptor

The analog voice encryptor is a combination of digital encryptor and voice scrambler. Analog vocoder uses various frequency channels. The analog to digital reconstruction is performed in a bandwidth constrained manner thus maintaining the energy and voice characteristics. Digital processing portion is executed on a high speed digital signal processor (DSP). Role of DSP is to handle the digitized audio as sub elements of the original captured video. The sub elements are randomly manipulated in time and frequency domains. The destination end processing performs reverse time and frequency manipulation.

- Advantage:
- It provides high voice quality.
- Security level depends upon the level of signal processing and security of the key stream generator.
- Disadvantage:
- Limited number of signal permutations.

VI. Channels

The voice channel encryptor[8] operates on three channels:

- Single channel half duplex: these are found on ratio channels with push to talk features and are used to send voice traffic across the ratio link. Here data encryptors are found on the ratio channels.
- Singles Channel Full Duplex: It uses special software within the telephones itself provides end to end voice encryption. Cryptographic device is separated from the actual instrument by some distance. Both the analog and digital encryption uses key generator to produce key stream.
- Multi channel Full Duplex: Encryption is performed on station to station basis and digital trunk encryption methods are used. Digital voice trunks are encrypted in the same manner like digital data trunks. The architecture of the system decides where the encryption device is to be placed. Encryption device can either be placed between voice channel multiplex equipment, de-multiplex[9] equipment or communication link. The level of security depends on security of the physical channels between multiplexer equipment and audio channel increment e.g. telephone.

VII. Scremblers

A. Additive Scramblers

Definition: additive scramblers transform the input data stream by applying a pseudo random binary sequence. These are also as synchronous scramblers.

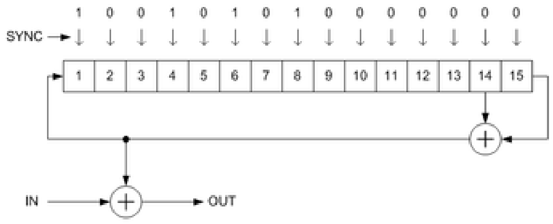

Figure 2. Additive scrambler (descrambler)

B. Multiplicative Scramblers

Definition: Multiplicative[10] scramblers performs multiplicative operation by using the scrambler’s transfer function. These are also known as self synchronizing scramblers.

A multiplicative scrambler used in V.34 recommendation.

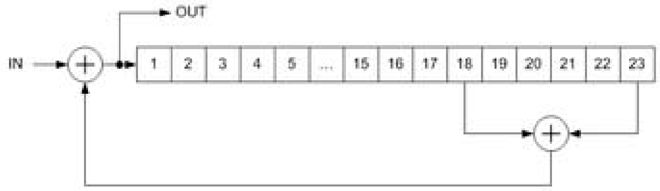

Figure 3. Multiplicative scrambler.

A multiplicative descrambler used in V.34 recommendation

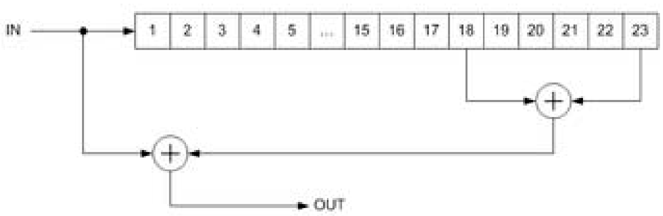

Figure 4. Multiplicative descrambler

Multiplicative scramblers (also known as feed-through) are called so because they perform a multiplication of the input signal by the scrambler's transfer function in Z-space. They are discrete linear time-invariant systems. A multiplicative scrambler is recursive and a multiplicative descrambler is non-recursive. Unlike additive scramblers, multiplicative scramblers do not need the frame synchronization that is why they are also called self-synchronizing. Multiplicative scrambler/descrambler is defined similarly by a polynomial for the scrambler on the picture it is

$$1 + x^{-18} + x^{-23}$$

This is also a transfer function of the descrambler.

VIII. Comparison of scramblers

Scramblers have certain drawbacks:

- Both types may fail to generate random sequences under worst case input conditions.
- Multiplicative scramblers lead to error multiplication during descrambling (i.e. a single bit error at the descrambler's input will result into w errors at its output, where w equals the number of the scrambler's feedback taps).
- Additive scramblers must be reset by the frame sync if this fails massive error propagation will result as a complete frame cannot be descrambled.
- The effective length of the random sequence of an additive scrambler is limited by the frame length, which is normally much shorter than the period of the PRBS. By adding frame numbers to the frame sync, it is possible to extend the length of the random sequence, by varying the random sequence in accordance with the frame number.

IX. References

[1] Merriam-Webster's Collegiate Dictionary "Cryptology definition". Retrieved 26 March 2015.

[2] Diffie, Whitfield, Hellman, Martin."Multi-user cryptographic techniques". AFIPS Proceedings 8 June 1976 45: 109–112.

[3] Rosenoer, Jonathan "CRYPTOGRAPHY & SPEECH". CyberLaw. 1995 Archived December 1, 2005 at the Wayback Machine

[4] Al-Kadi, Ibrahim A "The origins of cryptology: The Arab contributions" April 1992 Cryptologia 16 (2): 97–126. doi:10.1080/0161-119291866801.

[5] Sefik Ilkin Serengil, Murat Akin. "Attacking Turkish Texts Encrypted by Homophonic Cipher" Proceedings of the 10th WSEAS International Conference on Electronics, Hardware,

[6] Wireless and Optical Communications, pp. 123–126, Cambridge, UK, February 20–22, 2011.

[7] Computer Security Resource Center "FIPS PUB 197: The official Advanced Encryption Standard"(PDF). National Institute of Standards and Technology. Retrieved 26 March 2015.

[8] Rivest, Ronald L. Shamir, A. Adleman L.). "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems" 1978.Communications of the ACM (Association for Computing Machinery) 21

[9] Specifications for Data Broadcasting, European Telecommunications Standards Institute (ETSI) EN 301 192, 2004.

[10] Support for use of scrambling and Conditional Access (CA) within digital broadcast systems, European Telecommunications Standards Institute (ETSI) ETR 289, 1996.