Audio Engineering Society

Convention Paper 6930

Presented at the 121st Convention
2006 October 5–8 San Francisco, CA, USA

THE ORIGINS OF DSP AND COMPRESSION:

Some Pale Gleams From The Past; A Historical Perspective On Early Speech Synthesis And Scramblers, And The Foundations Of Digital Audio

Jon D. Paul
Vice President, Scientific Conversion, Inc.
Curator, Crypto-Museum
California, USA
crypto-museum@verizon.net

ABSTRACT

This paper explores the history that led to modern day DSP and Audio Compression. The roots of modern digital audio sprang from Dudley's 1928 VOCODER, and the WWII era SIGSALY speech scrambler. We highlight these key inventions, detail their hardware and block diagrams, describe how they functioned, and illustrate their relationship to modern day DSP and compression algorithms.

INTRODUCTION

The origins of modern digital audio can be traced to this first electronic speech synthesizer in 1928 and to a secure speech scrambler used during WWII. Homer Dudley's VOCODER paved the way towards modern audio compression and synthesis.

Bell Telephone Laboratories' (BTL) SIGSALY secure communications system marked the invention of a number of techniques that lie at the foundation of virtually all DSP and signal processing for coding and audio transmission today.

1. DUDLEY'S PIONEERING WORK

Homer Dudley at Bell Telephone Laboratories, Fig. 1 applied signal analysis to determine speech variation in time and frequency domains. He started with the goal of compressing speech bandwidth down from 2-3 kHz to 200-300 Hz for transmission over transcontinental telegraph cables (speech capable transcontinental cables were not available until 1956!). He conceived of the first working speech analyzer and synthesizer in 1928: the VOCODER.

1.1. Dudley's VOCODER

The VOCODER is a technique of speech analysis and synthesis based on the carrier nature of speech, see Fig. 2 [1]. First, it determines whether a speech sample is voiced or unvoiced. If it is voiced, the pitch is extracted, fig. 3.

The frequency spectrum of the speech sample is then divided into sub-bands by a filter bank, and the amplitude of each sub-band is detected. The output of the VOCODER analyzer consists of a voiced/unvoiced binary, a pitch signal and about 10 detected sub-bands. These signals each have ~25 Hz bandwidth. The VOCODER analyzer output contains the original speech information in ~300 Hz bandwidth. The result is a 10X compression of the speech bandwidth.

Speech can be reconstructed from these signals using the VOCODER synthesizer, which performs the inverse process. The VOCODER's synthesizer has a noise generator and a variable-frequency relaxation oscillator rich in harmonics. The voiced/unvoiced bit selects either the oscillator or the noise generator. The oscillator frequency is controlled by the pitch signal.

The output of the voiced/unvoiced selector is applied to a filter bank whose sub-bands are varied in gain according to the synthesizer sub-band outputs. The filter bank dynamically modifies the harmonic spectrum of the oscillator. Inter-syllable pauses are inserted by muting control signal. The result is reconstructed and synthesized speech, however speaker recognition is lost in the process.

The analyzer signals can be sampled in time and quantized. Good speech quality requires a sample rate of 20 ms. Recognizable speech can be reproduced with as little as 6 levels of quantization on the sub-band detector outputs. The pitch signal requires higher resolution, ~36 levels. Applications include speech research, speech compression and speech encryption, by scrambling the VOCODER analyzer outputs.

1.2. Dudley's VODER

In 1939, Dudley designed the VODER, Figs. 4,5 (Voice Operating Demonstrator) for generating synthetic speech using the VOCODER's synthesizer hardware under manual control. The VODER occupied a rack of equipment and used a console similar to that of an organ. It required a year of practice for an operator to achieve good quality speech synthesis. A well-publicized VODER demonstration was at the 1939 World's Fair.

2. SECRET TELEPHONY DEVELOPMENT

A number of interesting patents show the development of secret telephony. Details of these patents are in the References section at the end.

2.1. Generalized Secrecy Systems

Codes and ciphers have been in use since the Roman Empire (Caesar cipher). The basic principles of secret transmission [2] apply for manual (e.g. codebooks), mechanical, or modern computer encryption. A message and key are input to a cipher system, Fig. 6. The key is sent via a secure method to the recipient. The enciphering device mixes the message and key to produce unrecognizable output.

The ciphered message or cryptogram can be transmitted over a channel, subject to eavesdropping by the enemy, e.g. a radio transmission to a ship at sea. The ciphered message and the key are combined at the receiving station in a deciphering device. The decryption process recovers the original message only if the correct key is used.

The essence of cryptology is the design of an enciphering algorithm and the generation, transmission, synchronization and destruction of a sufficiently unique key.

2.2. Espenschied Patent: Secret Telephone System, Band splitting Frequency Inversion: ATT A-3

This is an early (1920) speech encryption system [3]. Incoming speech is divided into several sub-bands by band-pass filters, Figs. 7,8. A double-balanced mixer, whose modulation frequency is either 600 or 1200 Hz, modulates the output of each filter. The mixer outputs go to another bank of band-pass filters selecting the difference frequency of the mixer output.

The band-pass filter outputs are summed together. The result has the same bandwidth as the speech input. The frequency order of the sub-bands is scrambled, and the sub-bands themselves are inverted. The receiver performs the reverse process, reconstructing the original sub-bands. The patent includes full duplex transmission.

This system was realized in the AT&T A-3 speech scrambler. Although it worked, it did not provide a good level of secrecy. A listener could interpret the scrambled speech after some training.

2.3. Dudley Patent, Signal Transmission

This is the VOCODER, combined with Espenschied's frequency band shifting idea [4]. The sub-bands are shifted by DSBSC modulation with a sub-audible component of the input, Fig. 9. The sub-audible component is unpredictable and serves as a random cipher key. The key component can be extracted at the receiver and the process is reversed to reconstruct the original speech.

2.4. Potter Patent, Secret Telephony, Band splitting and multiplexing concept

Potter [5] started with the same type of sub-band system as Dudley, but uses a 1-bit digital representation of the VOCODER outputs, Fig. 10. The analyzer outputs are sampled in time and relays serve as comparators, providing a one-bit digitalization of the sub-band filter outputs. The 1-bit outputs are enciphered by exclusive-OR (XOR) technique with a separately derived key source (Vernam cipher).

At the transmit-side, signal and key are applied to an XOR implemented with relays. The receive-side applies the ciphered signal and key to another XOR, recovering original digital signal. The 1-bit recovered signals are filtered to obtain analog outputs which the synthesizer. The same key must be present at the receive-side and in perfect synchronization with the transmit-side key.

2.5. Dudley Patent, Secret Telephony

Dudley approached the secrecy problem in 1941 [6] by using his VOCODER combined with a random key stored on a phonograph record. The output of the record is analyzed with a filter bank into a number of sub-bands, which are detected as in a VOCODER.

The detected key sub-bands are sampled in time, summed with the VOCODER output, and transmitted via time-division multiplex, Fig. 11. The reconstruction process requires an identical key record and a multiplex switch precisely synchronized with the transmitter key and multiplex switch. Details of key generation and synchronization are shown in this patent. Dudley uses a resistive noise source, which is sampled to generate the key, which is then stored by recording on a record. It requires a special purpose, custom made vacuum tube for the multiplex switch. The deciphered sub-band and pitch signals run the VOCODER's synthesizer to reconstruct the speech.

2.6. Mathes Patent, Speech Component Coded Multiplex Carrier Wave Transmission

Mathes [7] includes the techniques mentioned above, with a combination of frequency-division multiplex and spread-spectrum techniques to increase security, and decrease susceptibility to fading and distortion of radio channels, Fig.12. This was the first practical application of spread spectrum technique (note: the Hedy Lamarr patent of 1941 [8] preceded Mathes, but was not developed into a practical spread spectrum device).

3. THE SIGSALY SYSTEM

Before WWII, the USA and Britain used transatlantic high-frequency radio for high-level conferences. An ATT A-3 scrambler provided security. This band shifting cipher was extremely vulnerable to enemy eavesdropping. Despite this, A-3 was used early in the war, as nothing better was available. A German listening post in Holland intercepted the radio channel and unscrambled the speech in real time! [8A]

The U.S. National Defense Radio Communications Committee decided to develop a totally secure speech encryption system with highest priority, and contracts were signed with Bell Telephone Laboratories. The final design was reviewed by a number of independent cipher and mathematics experts including Nyquist, and Alan Turing, and found to be unbreakable. The SIGSALY system was ready for deployment by 1943.

3.1. SIGSALY Basic Block Diagram and concepts

SIGSALY (not an acronym; just a cover name, with SIG as in Signal) used many of the concepts in these patents, with the innovation of 6-level quantization of the analyzer outputs and a complex Vernam cipher with modulo-6 addition of the input and a one-time key, Fig. 13 [9].

3.2. SIGSALY Vernier Quantizing Concept for the Pitch Channel

BTL engineers chose 6-level quantization for the 10 sub-bands of SIGSALY, Fig. 14. The analog signal was quantized using a set of 5 thyratrons, each set to conduct at a different voltage level, thus quantizing to six levels including zero. These were called "stepper tubes".

The pitch channel of a VOCODER's analyzer requires higher resolution than the frequency sub-bands. The pitch signal is first quantized to 6 levels. Then the 6-level quantization is subtracted from the original analog pitch signal to yield an error signal. This difference or "residue" is amplified X6 and applied to another 6-level quantizer.

The result is a 2-part quantization, 6 levels for the first (coarse) quantization, and another 6 level Vernier quantization of the residue. These 2 quantized signals represent a 36-level (~5 bits) quantized pitch signal. This is sufficient resolution for good quality speech reconstruction. This 2 step Vernier quantization principle has been applied ever since to many types of A/D conversion and precision measurement.

3.3. Vernam Cipher Algorithm, Companded, Quantized Input and 6-Level Random Key Added Modulo-6

SIGSALY transmitted 12 6-level quantized signals, which represented the 10 frequency sub-bands from the speech analyzer, and the coarse and Vernier pitch signals. The 6 amplitude levels were nonlinear, a first use of companding!

A random, one-time key signal was 6-level quantized with the same 20 ms quantization interval. The quantized signals and the keys were added; however, this could result in one of 12 possible levels.

Because the transmission and modulation system required 6-level quantization, a “re-entry” or modulo-6 addition was used; any result greater than 5 would have a voltage equivalent to 6 subtracted, Fig. 15. The original values can be recovered after transmission by performing the inverse operation, in the manner of the Vernam XOR cipher with binary inputs.

3.4. SIGSALY Characteristics and Specifications

SIGSALY, Fig. 16 satisfied the requirement for secure and unbreakable speech encryption over radio-telephone channels [10 - 15]. The system was in use from 1943 until 1946 and 12 terminals were built worldwide, manned 24 hrs/day. SIGSALY was never broken by the enemy. Over 3,000 Top Secret war conferences were held over SIGSALY. It was a gargantuan assembly comprising 40 racks, consuming 30 kW and weighing 100,000 pounds. SIGSALY required 13 technicians to operate it. Cooling was a major issue, handled by a huge air conditioning system.

3.5. National Cryptographic Museum SIGSALY Reconstruction

The National Security Agency's (NSA) National Cryptographic Museum (NCM) wanted to make a SIGSALY exhibit but lacked the historical details. Don Mehl, a technician and operator of the original system, supplied his books [12, 13] and other information to the NSA resulting in a complete modern reconstruction of SIGSALY, Fig. 17.

The NSA made a computer simulation of SIGSALY's processing to provide samples of enciphered and reconstructed speech for use in the Museum exhibit.

3.6. Random One Time Key, Mercury Tube Noise Source, Key Distribution on Phonograph Records

A truly secure encryption system requires a source of unique, one-time key equal in length to the input data to be transmitted. SIGSALY used 6 mercury vapor discharge tubes, Fig. 18. The resulting random noise was combined into a 6-level quantized signal in the same manner as the sub-band and pitch channels. Because there were 12 channels enciphered at a 50/sec rate, (10 sub-bands and 2 pitch channels, coarse and vernier), 600 unique keys were required per second of transmission.

The quantized key signal was recorded on 16" records (transcription discs) with a precision turntable, Fig. 18. A gold master was used to make just 3 pressings. One pressing was kept at the Army Security Agency in case of loss, the other two were sent to the receiving terminals by highly secure means. Two different key records were played for each SIGSALY conference, the two turntables automatically sequenced by an end of record pulse, thus providing up to 25 minutes of key per conference.

The key records had to be precisely synchronized at each terminal. A 100 kHz, national laboratory-standard quartz crystal oscillator was divided down to drive the synchronous motor of the turntables and other circuitry. A short-wave receiver tuned to radio time signals (e.g. WWV) provided time signal ticks used for synchronization and simultaneous start-up of turntables on both sides of the communication channel. Final synchronization to within 200 us was done by manually adjusting the timing signal phase for best intelligibility, while listening to the reconstructed speech.

3.7. SIGBUSE Pseudorandom Key Source

The lengthy and difficult process of generating and distributing the random key records led to design of an alternate pseudo-random key system, SIGBUSE (a codeword, not an acronym) for personnel training, setup, testing and adjustment of SIGSALY. SIGBUSE used existing cipher machine rotors similar to the Enigma machine rotors. The rotors had 26 contacts on each face and scrambled wiring connecting the two faces of a rotor, Fig. 19.

A bank of 5 rotors was turned by a stepping motor, with the set moving like an odometer: Each rotor would mechanically increment the adjacent rotor at a rate 1/26 its speed of rotation, like an odometer. This is the same method used in manually operated mechanical cipher machines such as the Enigma machine.

5 signals were applied in parallel to each rotor and each signal underwent a different scramble by each of the 5 rotors. The result was a 5 bit pseudorandom binary output, which in turn operated hundreds of telephone stepping relays. These relays generated the pseudo-random key.

The rotor motion and exact setup were duplicated and synchronized to a similar unit on the other end of the radio-link resulting in reconstruction of the exact same key. The key pattern was eventually repeated as the rotors rotated so SIGBUSE was not considered sufficiently secure for operational use. The noise of the stepping relays gave SIGBUSE the nickname "threshing machine".

3.8. SIGSALY Terminals 1943 – 1946

After SIGSALY was proved reliable and completely secure, the Army Signal Corps ordered BTL to construct terminals worldwide. This formed a secure network of 12 communications terminals for Top Secret use by Army and Navy chiefs of staff and heads of state. One terminal was constructed onboard a ship, which followed McArthur in his campaign through the South Pacific. After the War ended, new terminals were constructed in postwar Germany, among other places. SIGSALY was used until 1946. Newer secret telephony systems were based on SIGSALY techniques (see section 4).

3.9. SIGSALY Clients

The most famous user of SIGSALY was Winston Churchill, Fig. 20. A special telephone room was built in the Cabinet War Room, a secure underground bunker from which Churchill directed the War effort in blitz-plagued London. Due to its enormous size, the SIGSALY terminal was located some distance away, in a basement of Selfridges Department Store. Eisenhower, Fig. 20 once used SIGSALY to talk with his wife, Mamie; the technicians shifted the pitch generator to simulate her higher pitch-range.

Generals George C. Marshall and Douglas McArthur, Fig. 21, made extensive use of SIGSALY for conferences to direct and manage the War effort. Over 3,000 telephone conferences were handled by the system during WWII.

3.10. SIGSALY Innovations

SIGSALY was the result of many years of research by dozens of scientists and engineers at Bell Laboratories; 32 patents resulted, Fig. 22. Some of these were classified secret until 1975 or 1976. SIGSALY was the first digital voice system. Ten fundamental innovations can be traced to SIGSALY.

1. Unbreakable enciphered telephony
2. Quantized speech transmission
3. Speech transmission by pulse code modulation
4. Companded PCM
5. Multilevel Frequency Shift Keying (FSK)
6. Realization of 10X bandwidth compression
7. FSK-FDM transmission over a fading medium
8. Multilevel "eye pattern" adjusts sampling intervals
9. Two step vernier (residue) quantization
10. Spread spectrum transmission [16]

These advances are in constant use in today's communication, speech, and DSP technology.

3.11. SIGSALY User Instructions

This interesting placard provided instructions and precautions to SIGSALY users.

"1. This means of communications is sufficiently secure to permit information the discussion of the most highly secret with absolute safety and protection.

2. Please remember that actual voices are not transmitted. This artificial voice which system is based upon the creation of an artificial voice which resembles that of the speaker only in basic qualities. For this reason you may not readily recognize the voice of the person with whom you are conversing. A certain amount of background noise may be noticeable; this, however, will not seriously interfere with the conversation.

3. In order to realize the full benefit of this system it is requested that the following points be observed:

A. Prepare in advance the material to be discussed.

B. Speak slowly and distinctly.
C. Do not shout. Speak as though you were using a local telephone.

D. Use the phonetic alphabet where necessary in spelling proper names; Ask the person to whom you are speaking to spell when you do not understand a word.

4. The mere existence of this means of communication with Washington is secret. Persons having occasion to use this service will refrain from discussing the fact that such service exists. Any discussion of the Service must be limited to those few officers whose Official duties require a knowledge of the service."

4. LINKS TO CURRENT TECHNOLOGIES

4.1. Modern Speech Encryption and Compression Using Vocoders

A number of modern speech encryption systems use various compression and cipher techniques that find their roots in the VOCODER and SIGSALY:

1. LPC-10, FIPS Pub 137, 2400 bit/s.

2. Code Excited Linear Prediction, (CELP), 2400 and 4800 bit/s, STU-III.

3. Continuously Variable Slope Delta-modulation (CVSD), 16 Kbit/s, KY-57.

4. Mixed Excitation Linear Prediction (MELP), MIL STD 3005, 2400 bit/s, FNBDT.

5. Adaptive Differential Pulse Code Modulation (ADPCM), ITU-T G.721, 32Kbit/s STE.

4.2. CELP: Code-Excited Linear Prediction: digital cell phones and VOIP

Code-excited linear prediction, Fig. 23 is used in digital cell phones. The basic Dudley speech synthesis with voiced and unvoiced generation and shaping of the resultant signals is a characteristic of CELP. The CELP analyzer uses FFT techniques to realize the filter bank concept of Dudley. Modern DSP provides the pitch estimation and other parameter generation.

4.3. MPEG-1 Layer 3

This type of compression, Fig. 24, uses the filter bank concept of Dudley, without the pitch channel and voiced/unvoiced switching characteristic of Dudley's VOCODER. With 32 sub-bands, it achieves substantial compression of music bandwidth.

4.4. MPEG-2 AAC

MPEG-2 AAC is similar to MPEG-1 Layer 3, using a filter bank and perceptual modeling, Fig. 25.

5. SUMMARY

Dudley’s 1928 VOCODER was the first successful electronic speech analyzer and synthesizer. Modern speech and signal processing and compression began with Dudley’s inventions and SIGSALY. SIGSALY represented the first use of frequency-division multiplex and spread-spectrum techniques.

SIGSALY’s many innovations are still used in current technologies. Modern speech scramblers are partly based on SIGSALY's principles. Despite many attempts, SIGSALY was never broken by the enemy and was secure enough for Top Secret conferences at the highest levels of military and executive government. These inventions were so important that much of their technology and the patents were classified secret until 1976. It is impossible to find any DSP digital or signal processing for coding, compression or transmission of audio, which does not have at least some roots in Dudley's VOCODER and SIGSALY.

REFERENCES

[1] The Carrier Nature of Speech, Dudley, Homer Bell System Technical Journal, Vol. 19, p. 495 to 515, Oct. 1940

[2] Shannon, Claude., Communication Theory of Secrecy Systems", Bell System Technical Journal, vol.28-4, page 656--715, 1949.

[3] Espenschied, Lloyd. Secret Telephone Service, U.S. Patent 1,546,439, Jul 21,1925

[4] Dudley, Homer. Signal Transmission, U.S. Patent 2,151,091, Mar 21, 1939

[5] Potter, Ralph. Secret Telephony, U.S. Patent 3,967,067, Jun 29, 1976

[6] Dudley, Homer. Secret Telephony, U.S. Patent 3,985,958, Oct 12, 1976

[7] Mathes, Robert. Speech Component Coded Multiplex Carrier Wave Transmission, U.S. Patent 3,991,273, Nov 9, 1976

[8] Markey, Hedy (Hedy Lamarr), U.S. Patent 2,292,387 Secret Communication System. Aug 11, 1942

[8A] Mehl, Donald E., private communication to Author.

[9] Shannon, Claude., Analogue of the Vernam System for Continuous Time Series, Paper #15 in Claude Shannon: Collected Papers, John Wiley and Sons. 1993, ISBN 0-7803-0434-9

[10] Bell Telephone Laboratories, Inc., A History of Engineering and Science in the Bell System, National Service in War and Peace (1925-1975), 1978 ISBN 0-932764-00-2

[11] Mehl, Donald E., SIGSALY, The U.S. War Department's World War II General Staff Secret Communications System, Kansas City, MO, 1997 (private publ.)

[12] Mehl, Donald E., The Green Hornet: America's Unbreakable Code for Secret Telephony: The Untold Story of World War II, The U.S. Army Signal Corps SIGSALY System, D.E. Mehl, (private publ.) 1997 *

[13] Mehl, Donald E., Top Secret Communications of World War II: Unbreakable Encryption for Secret High-Level Conferences, SIGSALY-The Green Hornet, Secure Telephone Conferences, SIGTOT, Teletype Cryptographic System, The Beginning of the Digital Age, Raymore, MO, 2002 (private publ.) *

[14] Zorpette, Glenn., Breaking the Enemy's code IEEE Spectrum, September 1987, Pg 47

[15] Kruh, Louis., Shhh! The Green Hornet
Cryptologia, Quarterly, Volume: 24 Issue: 2 Page: 171 April 30, 2000

[16] Bennett, William R., Fellow, Secret Telephony as a Historical Example of Spread-Spectrum Communications, IEEE Transactions on Communications, Vol. COM-31, No. 1, January 1983, 99.

* Note: please contact the Author at crypto-museum@verizon.net for information on these books.

WEBSITES

www.nsa.gov/publications/publi00019.cfm

www.nsa.gov/publications/publi00020.cfm

www.nsa.gov/museum/museu00022.cfm

www.bell-labs.com/org/1133/Heritage/VOCODER/

ptolemy.eecs.berkeley.edu/~eal/audio/VODER.html

www.wendycarlos.com/VOCODERs.html

www.obsolete.com/120_years/machines/VOCODER/

mambo.ucsc.edu/psl/smus/smus.html

www.bell-labs.com/org/1133/Heritage/VOCODER/

ACKNOWLEDGEMENTS

Many thanks for the kind assistance and support!

Lt. Donald Mehl, retired, 805th Signal Corps, Army Communications Service

Dr. James (Andy) Moorer, Adobe, Inc. San Jose, CA

Ms. Lucy Murphy, Cabinet War Rooms, Imperial War Museum, London, U.K.

National Cryptologic Museum, NSA, Ft. Meade, MD

Dr. Richard Redl, ELFI S.A., Switzerland

Scientific Conversion, Inc., California

Crypto-Museum, California

Figure 1. Homer Dudley, Helen Harper and VODER.

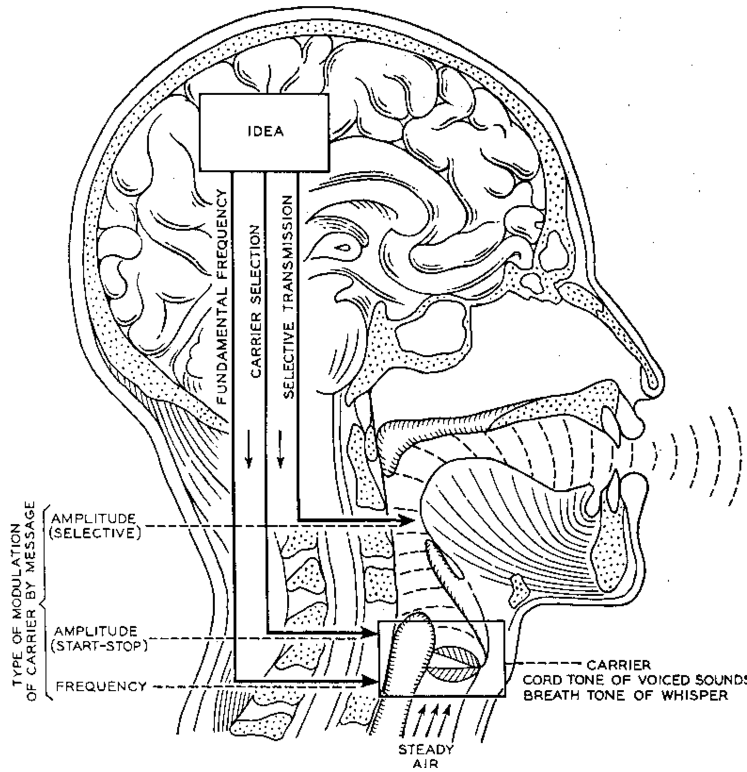

Figure 2. Mechanical analog of speech.

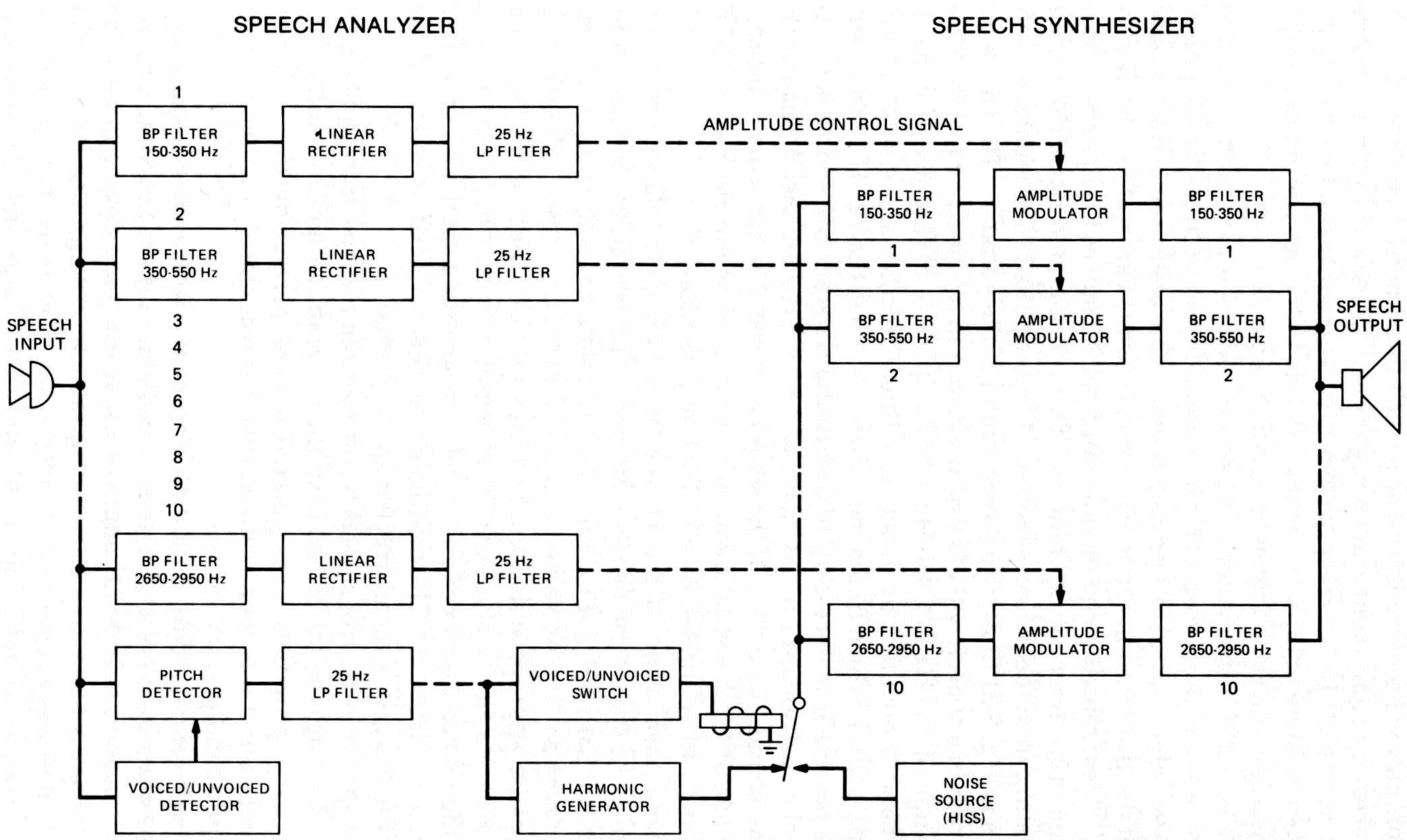

Figure 3. Block diagram of VOCODER.

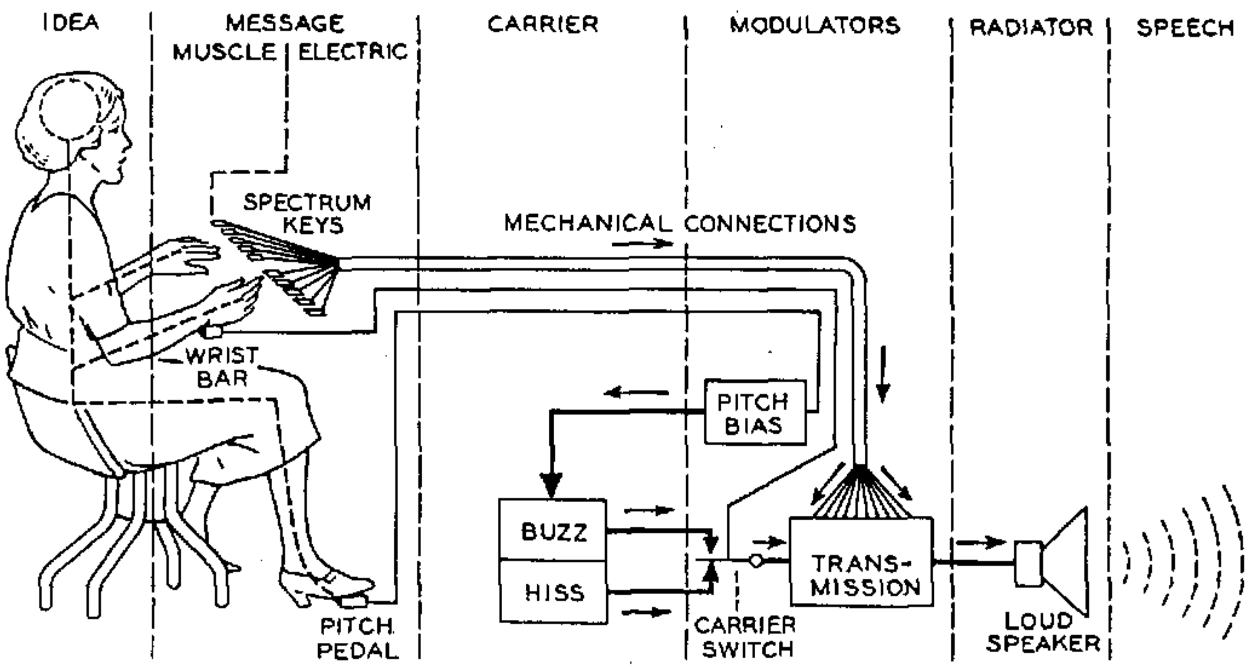

Figure 4. VODER block diagram.

Figure 5. Helen Harper plays the VODER.

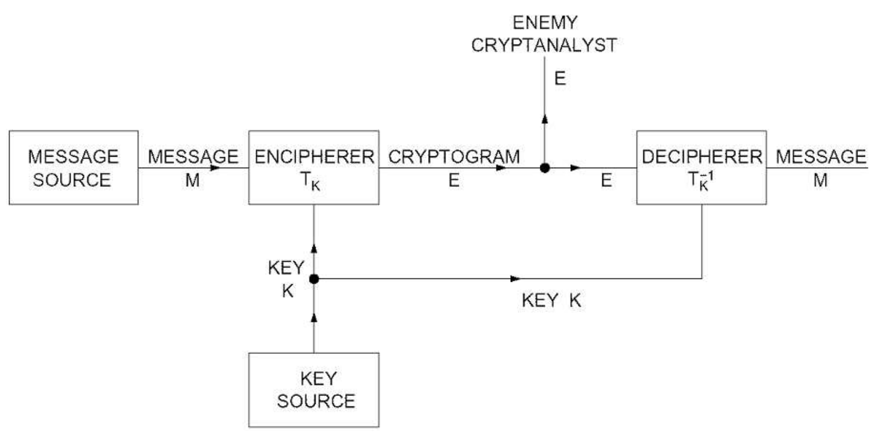

Figure 6. Generalized secrecy system by Shannon.

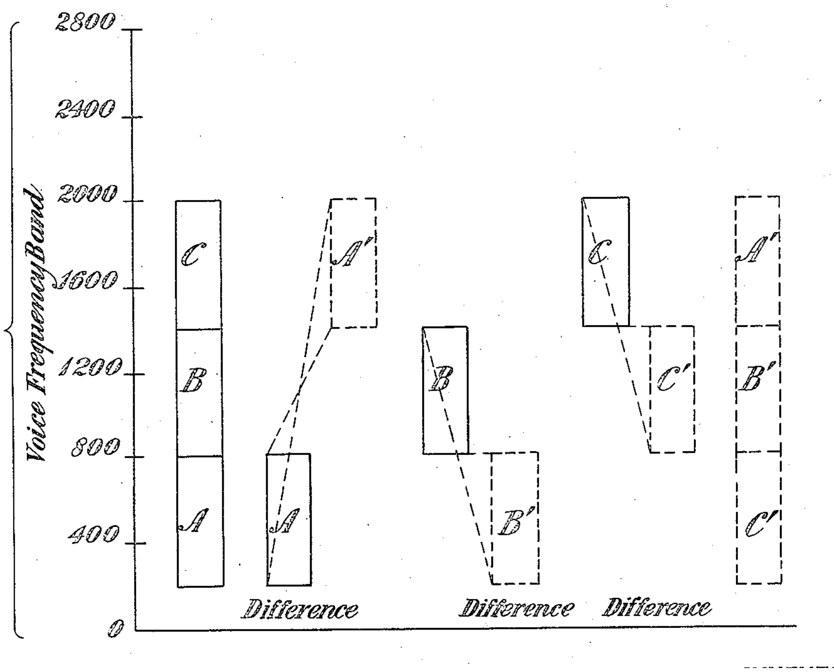

Figure 7. Early band-splitting speech encryption.

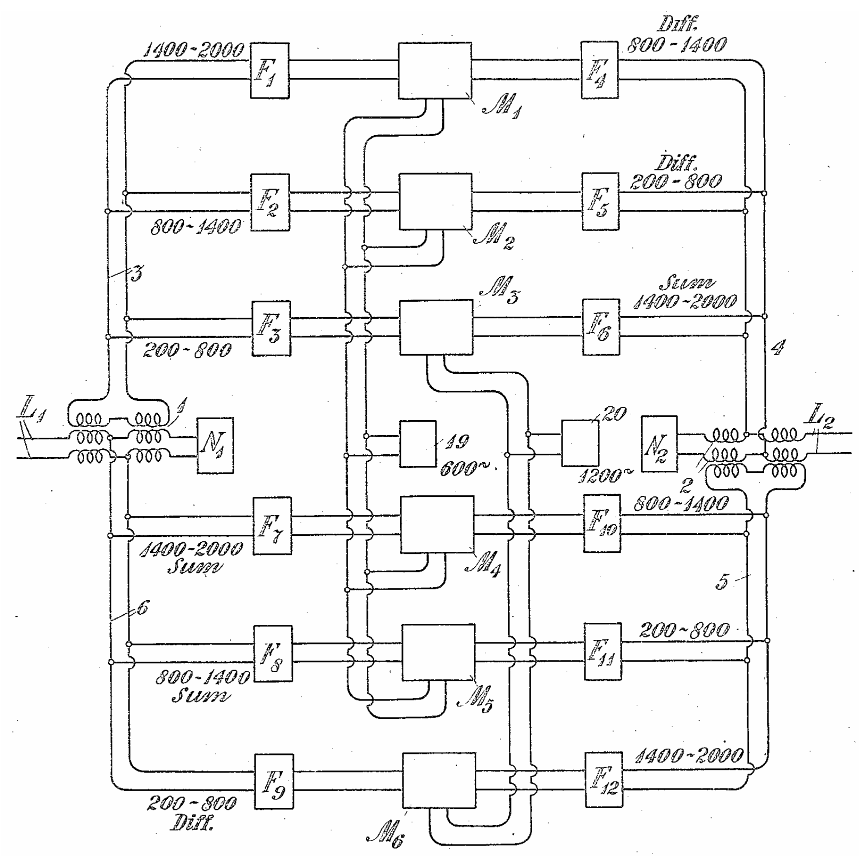

Figure 8. Band-splitting speech block diagram.

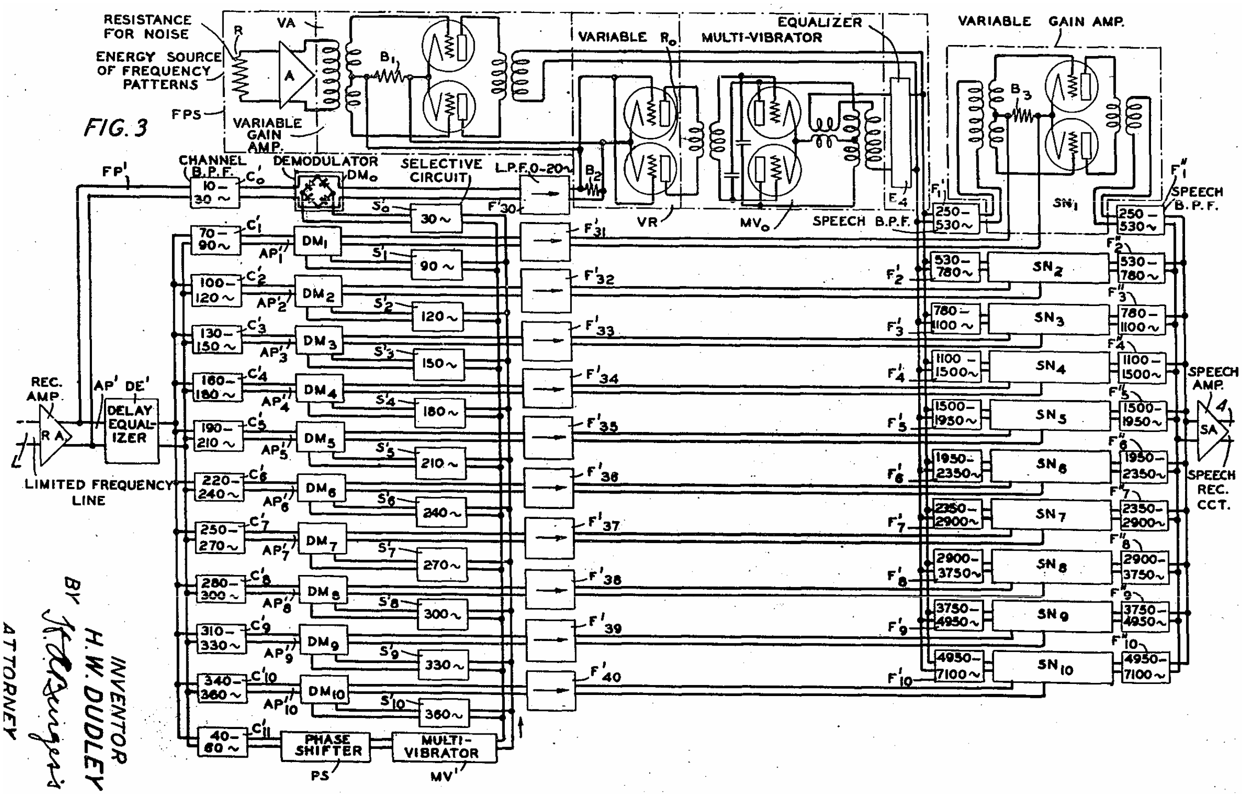

Figure 9. Dudley patent, signal transmission.

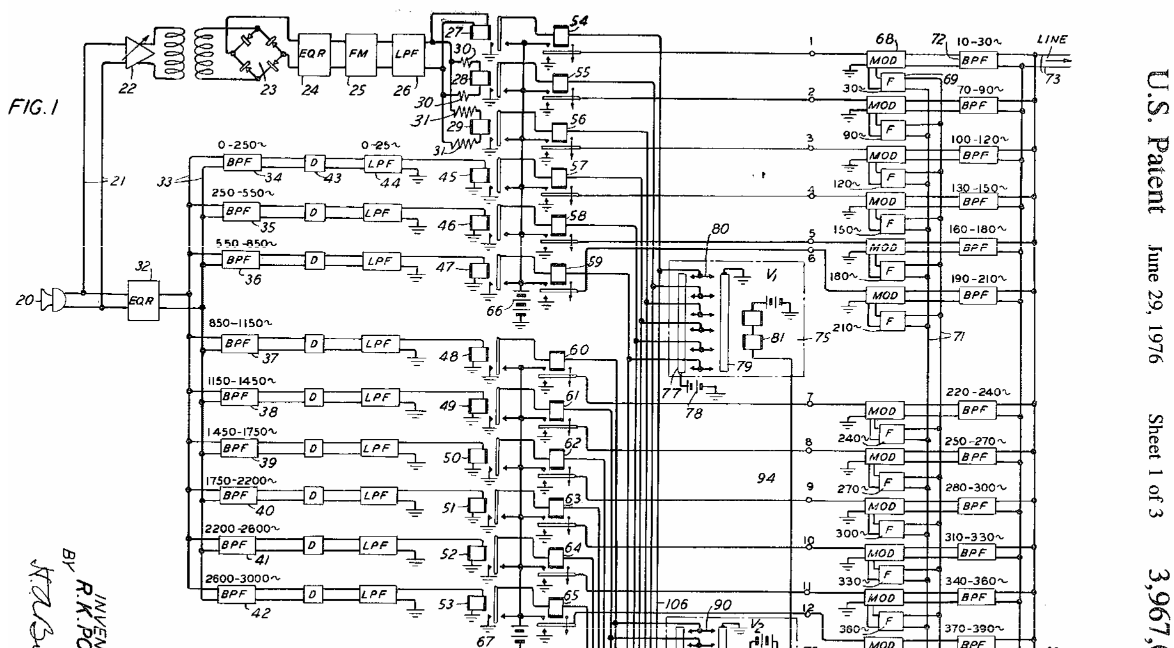

Figure 10. Potter patent, Secret Telephony.

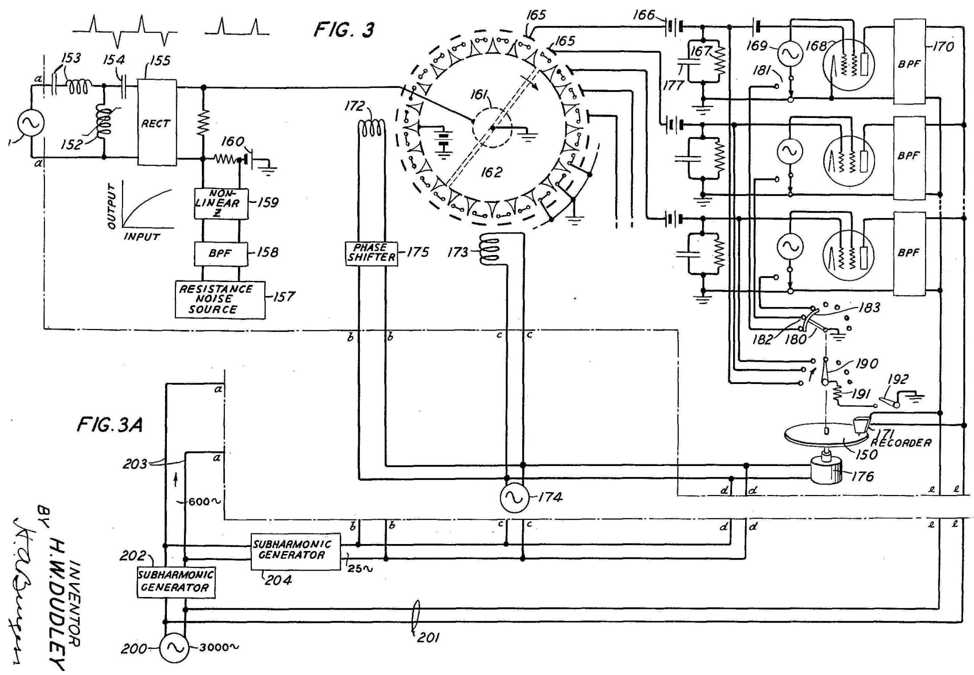

Figure 11. Dudley patent, Secret Telephony.

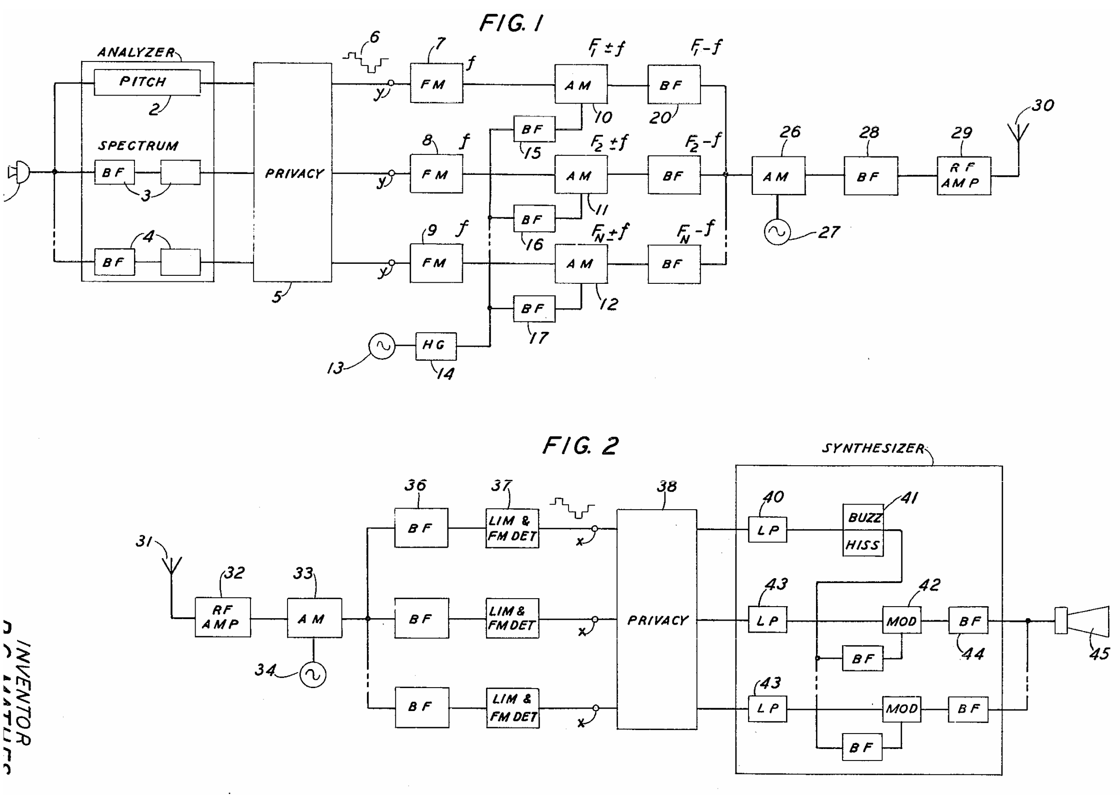

Figure 12. Mathes patent, Speech component coded multiplex carrier wave transmission.

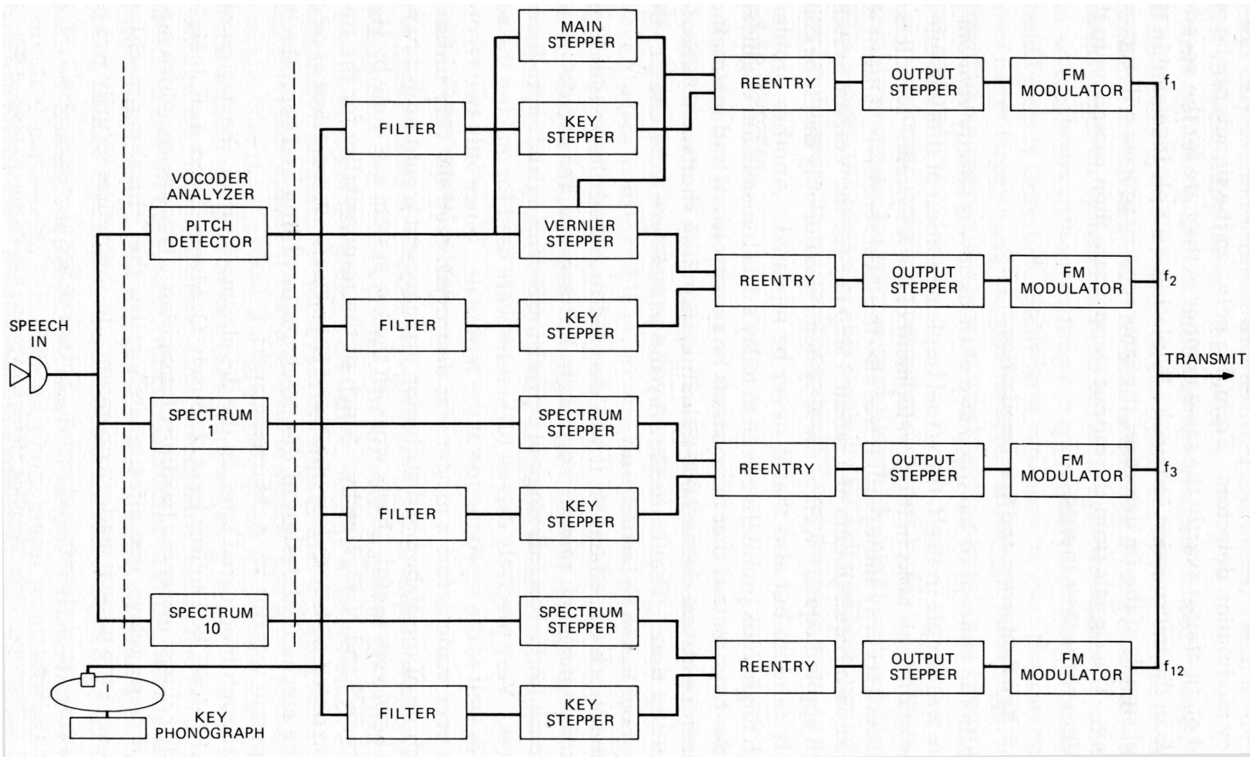

Figure 13. SIGSALY basic block diagram.

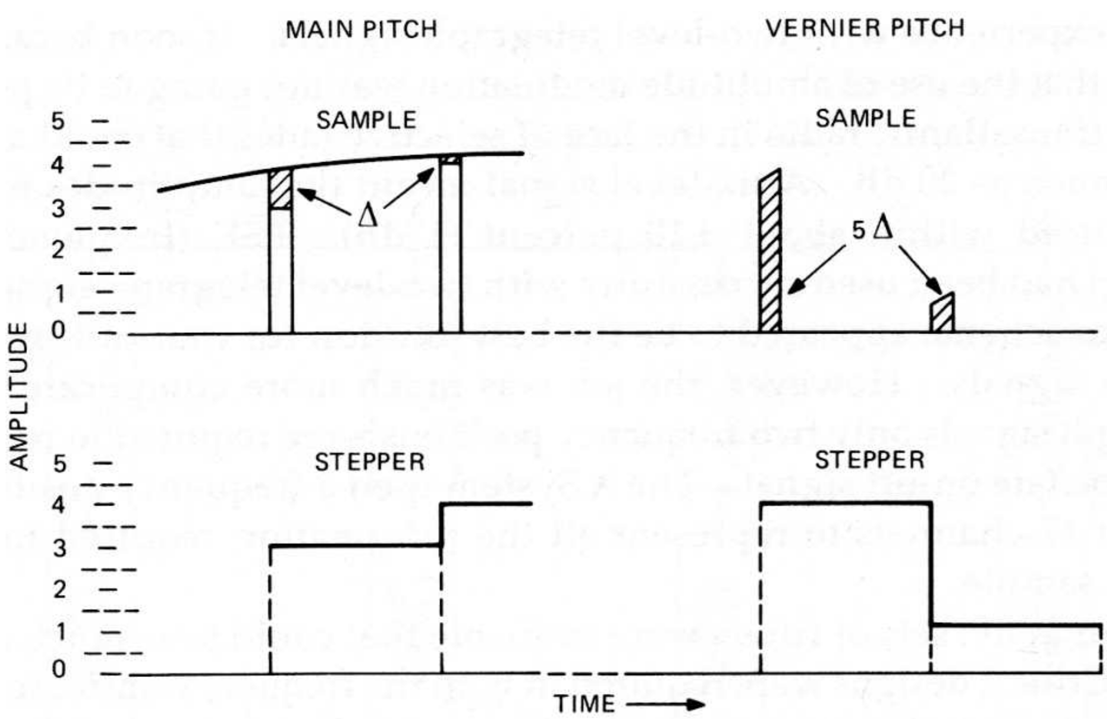

Figure 14. Vernier quantizing for pitch channel.

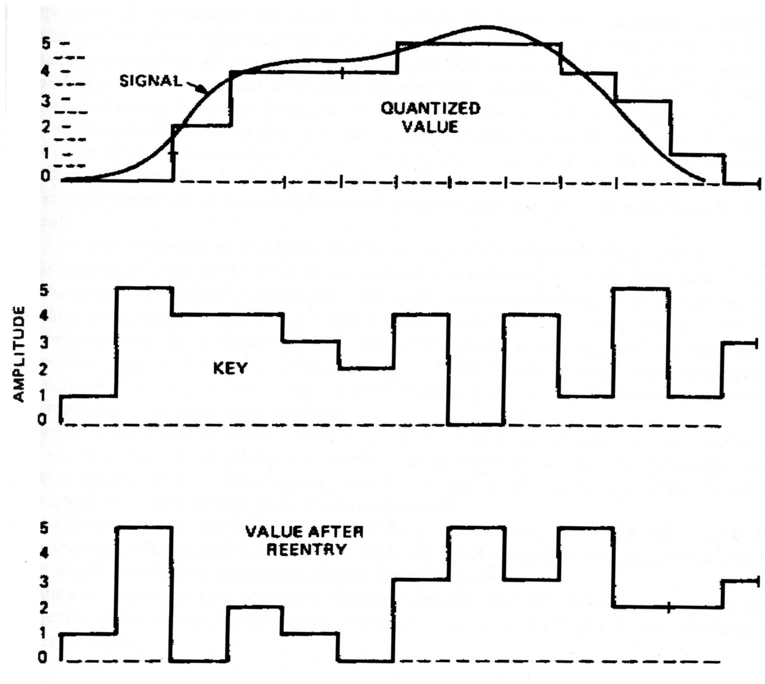

Figure 15. Vernam cipher and modulo-6 addition.

Figure 16. 1944 SIGSALY terminal.

Figure 17. National Cryptographic Museum SIGSALY reconstruction.

Figure 18. Mercury tube (2051) noise source, gold master and distribution key records.

Figure 18A. Precision crystal controlled turntables.

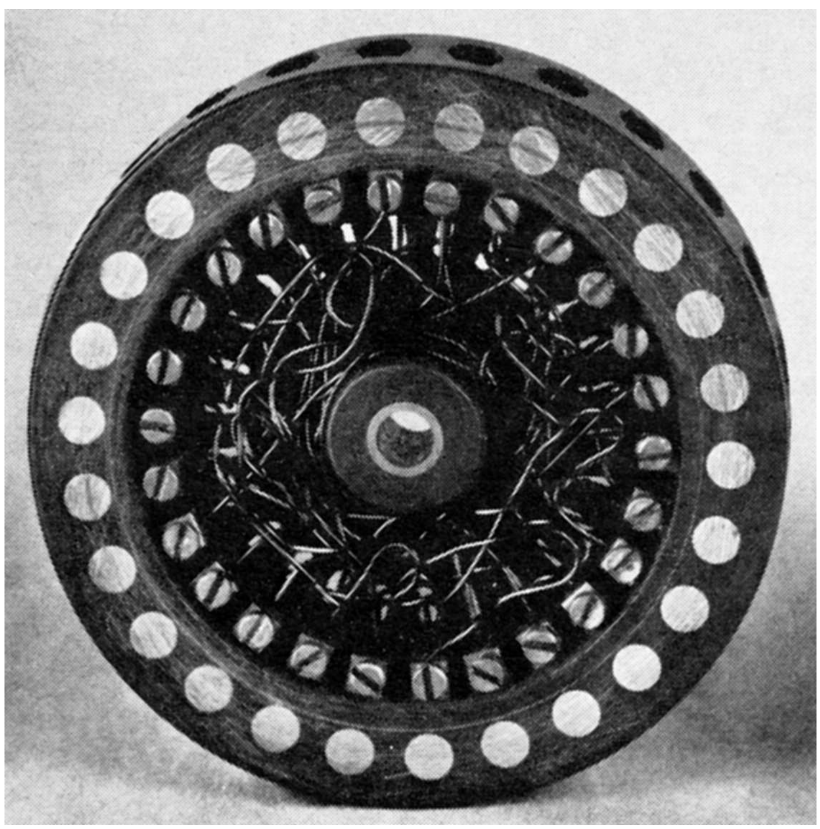

Figure 19. SIGBUSE pseudorandom key rotor.

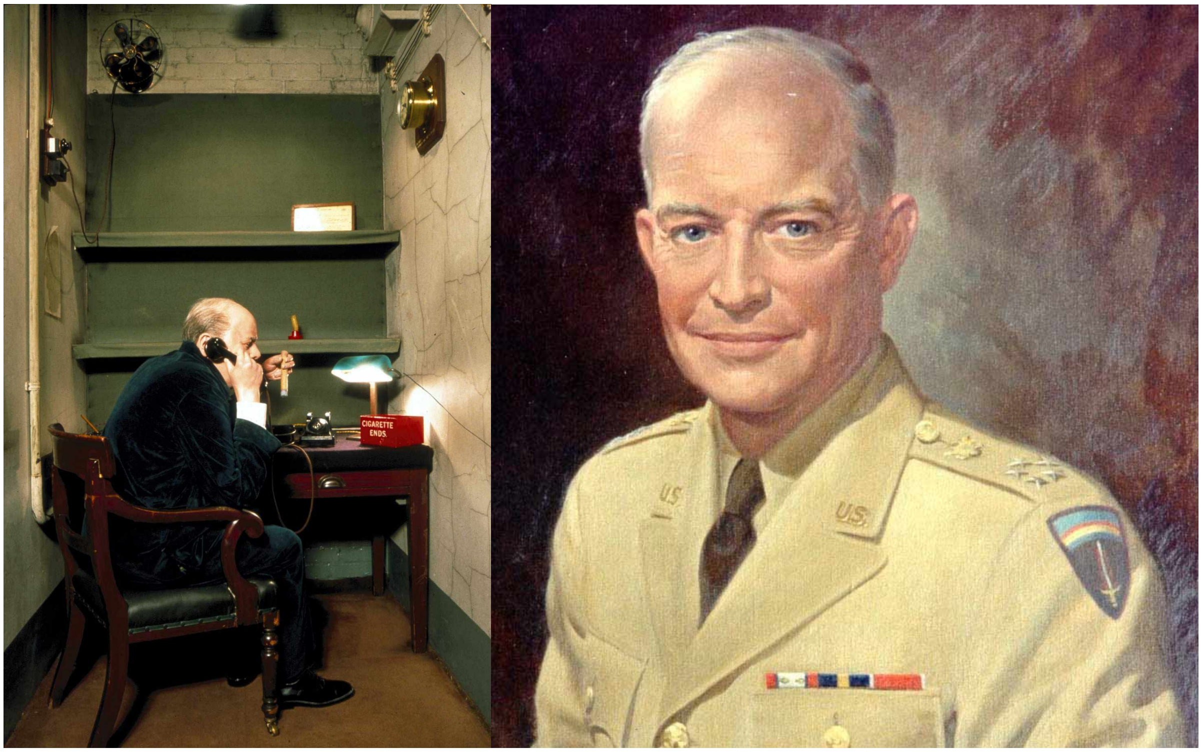

Figure 20. Winston Churchill in Cabinet War Rooms and Dwight D. Eisenhower.

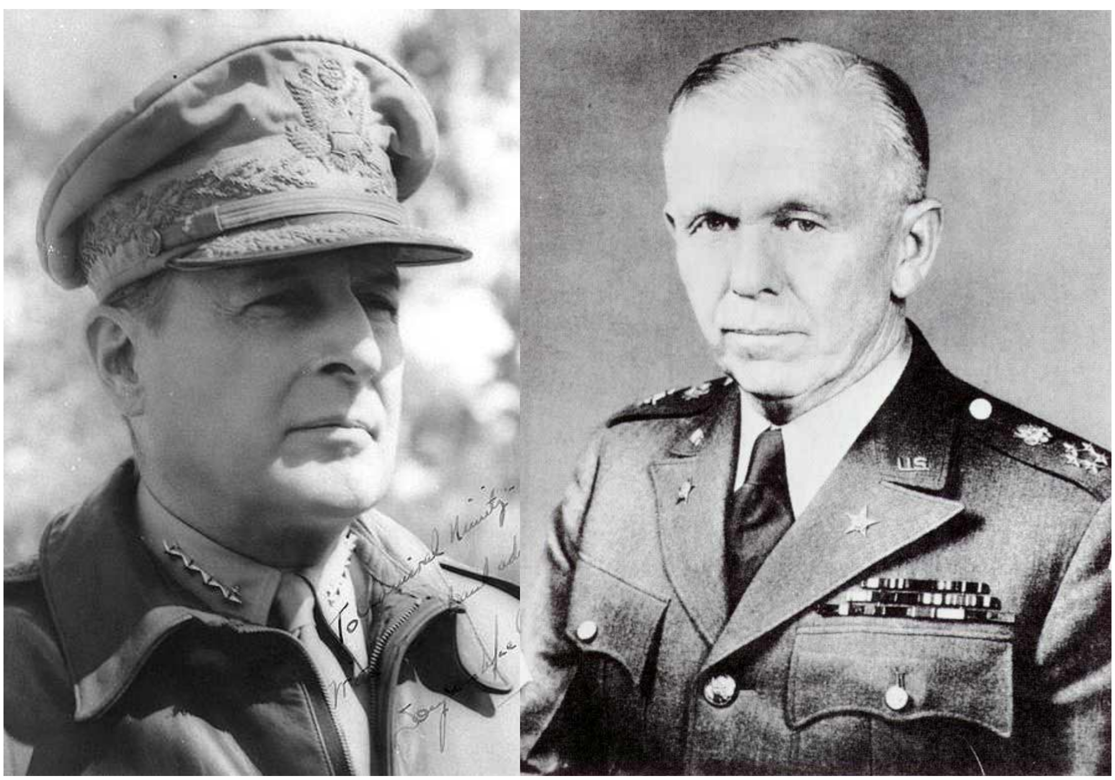

Figure 21. Douglas McArthur and George C. Marshall.

U.S. Patent No.	Inventor	Filing Date	Issue Date
3,024,321	K. H. Davis, A. C. Norwine	12/29/44	3/ 6/62
3,076,146	M. E. Mohr	12/27/45	1/29/63
3,188,390	M. E. Mohr	12/20/43	6/ 8/65
3,193,626	H. L. Barney	12/29/44	7/ 6/65
3,340,361	R. K. Potter	7/ 9/45	9/ 5/67
3,373,245	N. D. Newby, H. E. Vaughan	8/27/42	3/12/68
3,394,314	L. G. Schimpf	7/17/43	7/23/68
3,405,362	R. H. Badgley, L. G. Schimpf	12/20/43	10/ 8/68
3,470,323	H. W. Dudley	6/30/44	9/30/69
3,967,066	R. C. Mathes	9/24/41	6/29/76
3,967,067	R. K. Potter	9/24/4	6/29/76
3,985,958	H. W. Dudley	12/18/41	10/12/76
3,897,591	A. A. Lundstrom, L. G. Schimpf	8/27/42	7/29/75
3,912,868	R. H. Badgley, R. L. Miller	7/17/43	10/14/75
3,937,888	O. Myers	7/17/43	2/10/75
3,991,273	R. C. Mathes	10/ 4/43	11/ 9/76
3,979,558	E. Peterson	6/30/44	9/ 7/76
3,976,839	R. L. Miller	6/30/44	8/24/76
3,965,296	R. L. Miller	6/30/44	6/22/76
3,887,772	R. L. Miller	6/30/44	6/ 3/75
3,891,799	A. E. Melhose	9/27/44	6/24/75
3,893,326	D. K. Gannett	9/27/44	9/28/76
3,968,454	A. J. Busch	9/27/44	7/ 6/76
3,944,744	D. K. Gannett	5/10/45	3/16/76
3,944,745	D. K. Gannett	5/10/45	3/16/76
3,953,677	D. K. Gannett	5/10/45	4/27/76
3,953,678	D. K. Gannett	5/10/45	4/27/76
3,924,074	E. Peterson	5/19/45	12/ 2/75
3,983,327	D. K. Gannett, A. C. Norwine	7/ 9/45	9/28/76
3,934,078	D. K. Gannett	5/ 1/46	1/20/76
3,965,297	D. K. Gannett	5/ 1/46	6/22/76
3,924,075	D. K. Gannett	3/20/47	12/ 2/75

Figure 22. SIGSALY patents, some secret till 1976!

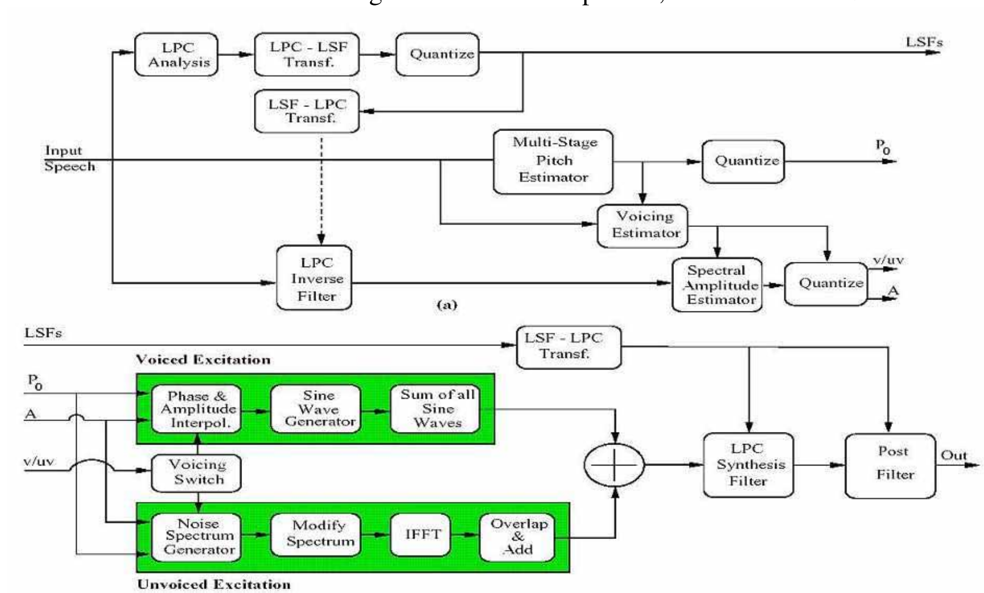

Figure 23. CELP: code-excited linear prediction.

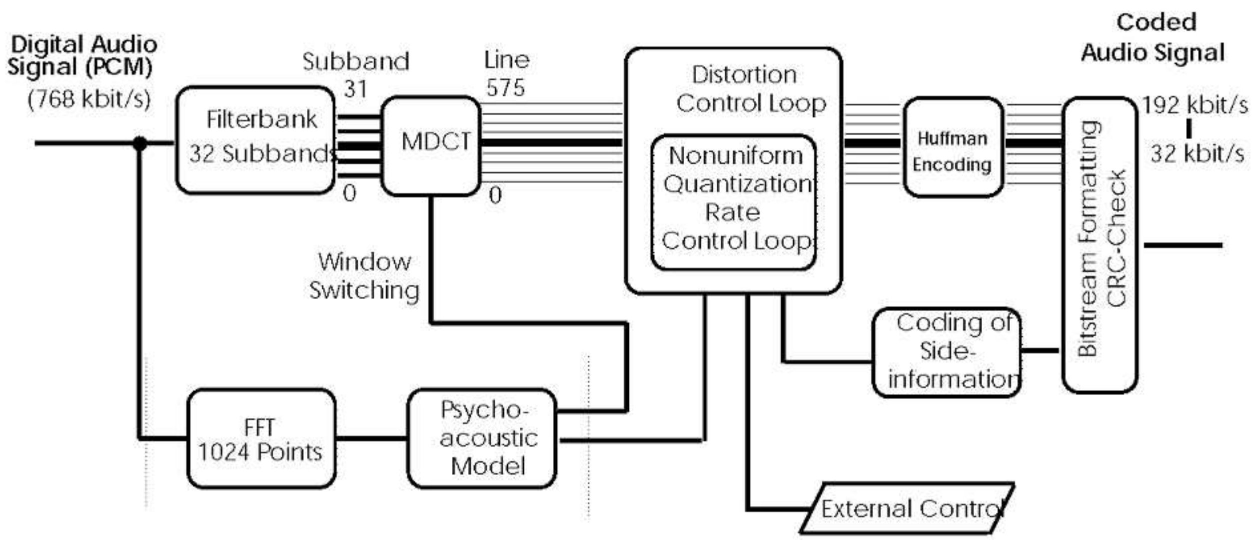

Figure 24. Block diagram MPEG-1 layer 3.

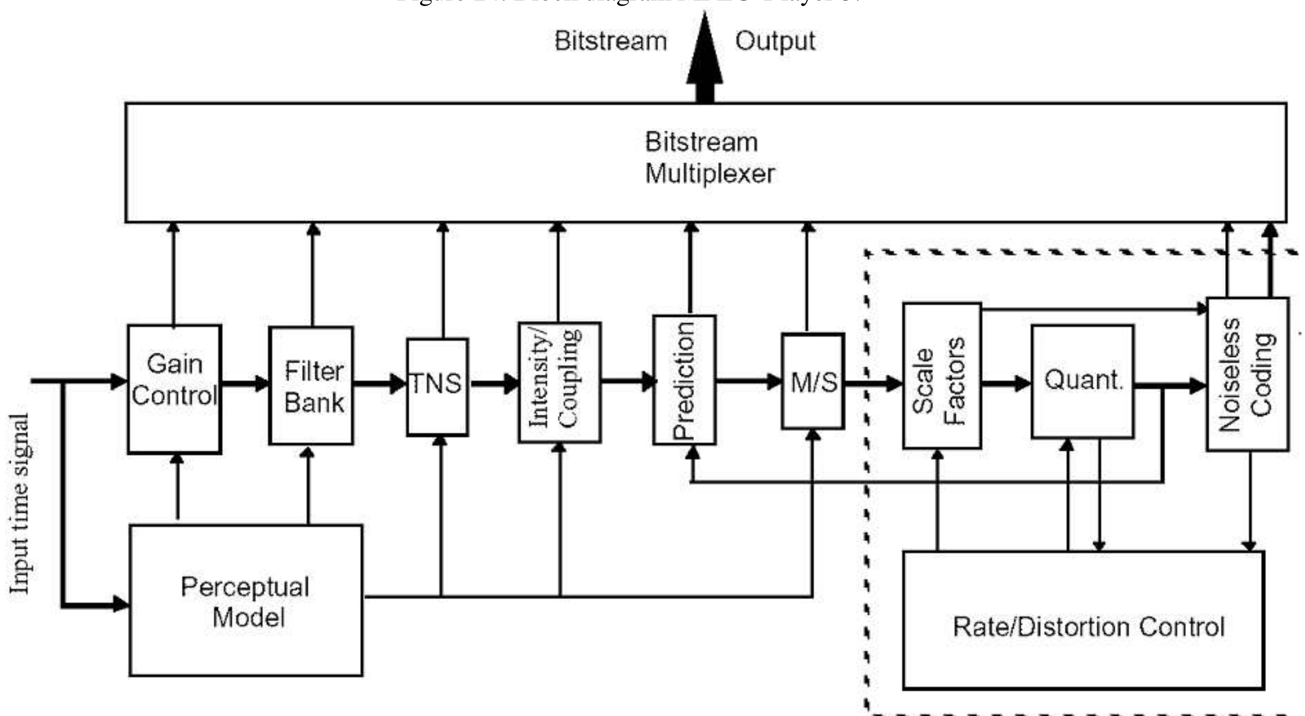

Figure 25. MPEG-2 AAC block diagram.