KRIEG IM AETHER

Vorlesungen an der Eidgenössischen Technischen Hochschule in Zürich
im Wintersemester 1985/1986
Leitung:
Bundesamt für Übermittlungstruppen
Divisionär J. Biedermann, Waffenchef der Übermittlungstruppen

Chiffrierung der Sprache

Referent: S. Horvath, Dr. sc. techn. ETH.

CHIFFRIERUNG DER SPRACHE

S. Horvath, Dr. sc. techn. ETH

INHALTSVERZEICHNIS

Adresse des Autors:

S. Horvath, Dr.sc.techn.ETH
GRETAG AG
8105 Regensdorf

"Krieg im Aether", Folge XXV

0. ZUSAMMENFASSUNG

Dieser Beitrag beschreibt den aktuellen Stand auf dem Gebiete der Sprachchiffrierung. Es wird gezeigt, warum Sprachchiffrierung im Gegensatz zur Sprachverschleierung eine beliebig hoch wählbare Abhörsicherheit gewährt, und warum dabei eine Bandbreiten-effiziente Sprachdigitalisierung von zentraler Bedeutung ist. Vier besonders wichtige, neue Sprachcodierungsverfahren werden besprochen: Parametrische Sprachcodierung nach der linearen Prädiktion (LPC-Vocoder), Teilbandsprachcodierung (Subband-Coding), Restfehlerangeregter LPC-Vocoder und Multipulsangeregter LPC-Vocoder.

Verschiedene in Frage kommende Chiffrierverfahren werden vorgestellt und die Einführung der Sprachchiffrierung in einem analogen und in einem digitalen Kommunikationsnetz diskutiert. Zum Schluss wird ein neues Sprachchiffriergerät als Beispiel beschrieben, das zusammen mit einem geeigneten Modem eine abhörsichere Sprachübertragung über das weltweite Wählnetz oder über Kurzwellenkanäle erlaubt.

1. EINLEITUNG UND UEBERBLICK

Sprache ist die natürlichste und wichtigste Form der menschlichen Kommunikation. Sie erlaubt einen schnellen und präzisen Informationsaustausch (Dialog mit Rückfragen und Präzisierungen) mit gleichzeitiger Meldungsauthentisierung via Sprechererkennung. Abhörsichere Sprachübertragung nimmt aus diesem Grund in der modernen Verteidigung eine wichtige Stellung ein. Sprachchiffrierung gewährt die grösste Kommunikationssicherheit. Dank der grossen Fortschritte der digitalen Sprachverarbeitung, der Modem-Technologie und der Halbleitertechnologie ist eine chiffrierte Sprachübertragung auf allen in Frage kommenden Kanälen mit vertretbarem Aufwand möglich geworden. Sprachchiffriergeräte werden daher heute vermehrt nicht nur zur Sicherung strategischer, sondern auch zur Sicherung taktischer Kommunikation auf dem Schlachtfeld eingesetzt.

Ziel dieses Beitrages ist es, über den Stand der Technik auf dem Gebiete der Sprachchiffrierung zu berichten und neue Trends aufzuzeichnen. Der Beitrag ist wie folgt gegliedert:

Das zweite Kapitel gibt einen Ueberblick über die Probleme der Sprachkommunikationssicherheit. Dabei werden die Zielsetzungen (Abhörsicherheit, kryptologische Sicherheit), die Grenzen der Sprachverschleierung und das zentrale Problem bei der chiffrierten digitalen Sprachübertragung (Bandbreite) beschrieben.

Das Kapitel 3 ist der Sprachdigitalisierung und der Redundanzreduktion gewidmet und beschreibt den Stand der Technik auf diesem sehr aktuellen Forschungsgebiet.

Das Kapitel 4 behandelt die Chiffrierung der mittels CODEC digitalisierten Sprache. Es wird dabei gezeigt, warum die kryptologischen Daten so wichtig sind und wie man eine beinahe absolute Sprachkommunikationssicherheit dank Sprachchiffrierung erreichen kann.

Im Kapitel 5 wird die Einführung der Sprachchiffrierung in einem analogen und in einem digitalen Kommunikationsnetz besprochen.

Das Kapitel 6 beschreibt als Beispiel den neuen GRETACODER® 220. Dieses Sprachchiffriergerät ermöglicht, zusammen mit einem geeigneten Modem, eine chiffrierte Sprachübertragung im Vollduplex-Betrieb über das weltweite Wählnetz oder über Kurzwellenkanäle.

2. WARUM SPRACHCHIFFRIERUNG

Um gesprochene, vertrauliche Informationen auf dem Uebertragungsweg gegen unbefugtes Abhören zu schützen, kann man die analogen Sprachsignale entweder verschleiern oder sie chiffrieren, letzteres nachdem eine redundanzmindernde Sprachdigitalisierung vorgenommen worden ist. Es sollte die geforderte Kommunikationssicherheit sein, die in erster Linie die Wahl zwischen Sprachverschleierung und Sprachchiffrierung bestimmt. In diesem Kapitel wird gezeigt, warum Sprachverschleierungsverfahren grundsätzlich nur kleinen bis mittleren Schutz gegen unbefugtes Abhören bieten können (und man deshalb, wo immer möglich,Sprachchiffrierung verwenden sollte) und wo das Hauptproblem beim Einsatz der Sprachchiffrierung liegt. Wir verwenden dabei drei wichtige Begriffe: Abhörsicherheit, Restverständlichkeit und kryptologische Sicherheit, die im nächsten Abschnitt definiert werden.

2.1 ABHOERSICHERHEIT, RESTVERSTAENDLICHKEIT UND KRYPTOLOGISCHE SICHERHEIT

Das Ziel aller Verfahren zur Sprachkommunikationssicherheit ist es, möglichst grosse Abhörsicherheit zu gewähren. Abhörsicherheit umfasst zwei Merkmale: Erstens die Sicherheit gegen einfaches, direktes Abhorchen (passive Attacke), die man mit der (noch) vorhandenen Restverständlichkeit misst, und zweitens die kryptologische Sicherheit gegen Kryptanalyse (aktive Attacke).

"Beste Abhörsicherheit" bedeutet demnach "keine Restverständlichkeit" und "hohe Dekryptierfestigkeit" (hohe Resistenz gegen Dechiffrierversuche).

Sprachverschleierungsverfahren versuchen das zu übertragende, analoge Sprachsignal derart zu verändern, dass das resultierende, verschleierte Sprachsignal möglichst unverständlich ist und trotzdem die Eigenschaften des Original-Sprachsignals bezüglich Bandbreite und Robustheit gegenüber Kanalverzerrungen beibehält. Die Restverständlichkeit ist allein von der Art der durchgeführten "Veränderungen" abhängig, die kryptologische Sicherheit dagegen von der Anzahl der möglichen "Veränderungen".

Sprachchiffrierung (oft auch Sprachverschlüsselung genannt) setzt eine Sprachdigitalisierung (und eine geeignete Redundanzreduktion) des zu übertragenden, analogen Sprachsignals voraus. Obwohl allein schon der aus der Sprachdigitalisierung entstandene Bitstrom, wie ein Datenstrom, für den Menschen direkt total unverständlich ist (Restverständlichkeit Null!), ist keine Abhörsicherheit ohne Chiffrierung vorhanden. Die "Abhörsicherheit" ist in diesem Falle mit "kryptologischer Sicherheit" gleich zu setzen und hängt allein von der Güte des verwendeten Chiffrierverfahrens ab.

2.2 GRENZEN DER SPRACHVERSCHLEIERUNG

Bevor wir uns der Sprachchiffrierung zuwenden, soll kurz begründet werden, warum Sprachverschleierungsverfahren grundsätzlich nur kleine bis mittlere Abhörsicherheit bieten können und warum sie nur eine Halbduplex-Sprachübertragung erlauben.

Um eine hohe Abhörsicherheit zu erreichen, sollte man beim Entwurf eines Sprachverschleierungsverfahrens versuchen, nicht nur eine möglichst kleine Restverständlichkeit, sondern auch eine möglichst grosse "Verwürfelungsmannigfaltigkeit" zu erreichen. Dieses Ziel ist leider nur bedingt realisierbar, denn der Anzahl Möglichkeiten zur Sprachverschleierung sind physikalische und zeitliche Grenzen gesetzt. Die Grenzen aus zeitlichen Gründen sind durch die für Verschleierung und Entschleierung dem Benützer maximal zumutbare Zeitverzögerung gegeben; die physikalischen Grenzen sind durch die grosse Redundanz des Sprachsignals und durch das zu erfüllende Kausalitätsgesetz bei der Realisierung bestimmt. Um diese Grenzen zu zeigen, betrachten wir etwas näher, wie die Sprachverschleierung durchgeführt wird.

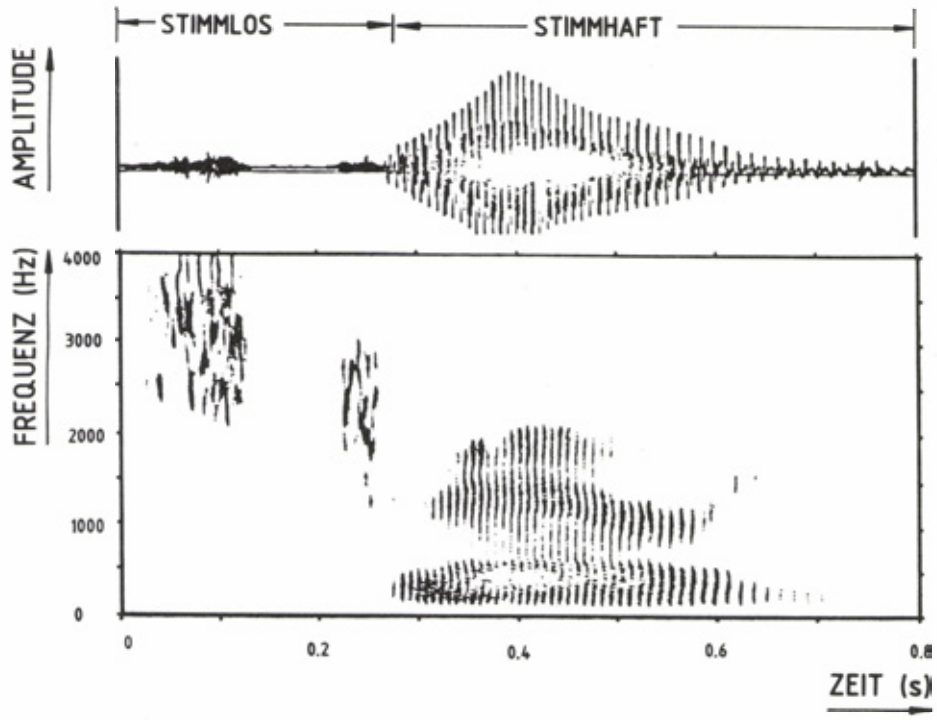


Fig. 1 Zeit- und Frequenzbereich-Darstellung eines Sprachsignals. Man beobachte die Unterschiede zwischen stimmhaften und stimmlosen Lauten.

Bekanntlich lassen sich Sprachsignale im Zeitbereich und,unter Annahme der Kurzzeitstationarität, im Frequenzbereich beschreiben (Fig. 1). Sprachverschleierungsmethoden haben zum Ziel, den zeitlichen Verlauf und/oder die Struktur des Kurzzeitfrequenzspektrums des Sprachsignals durch Umordnung (Verwürfelung) zu zerstören, um hierdurch die Sprache für den Menschen unverständlich zu machen /1/ - /4/.

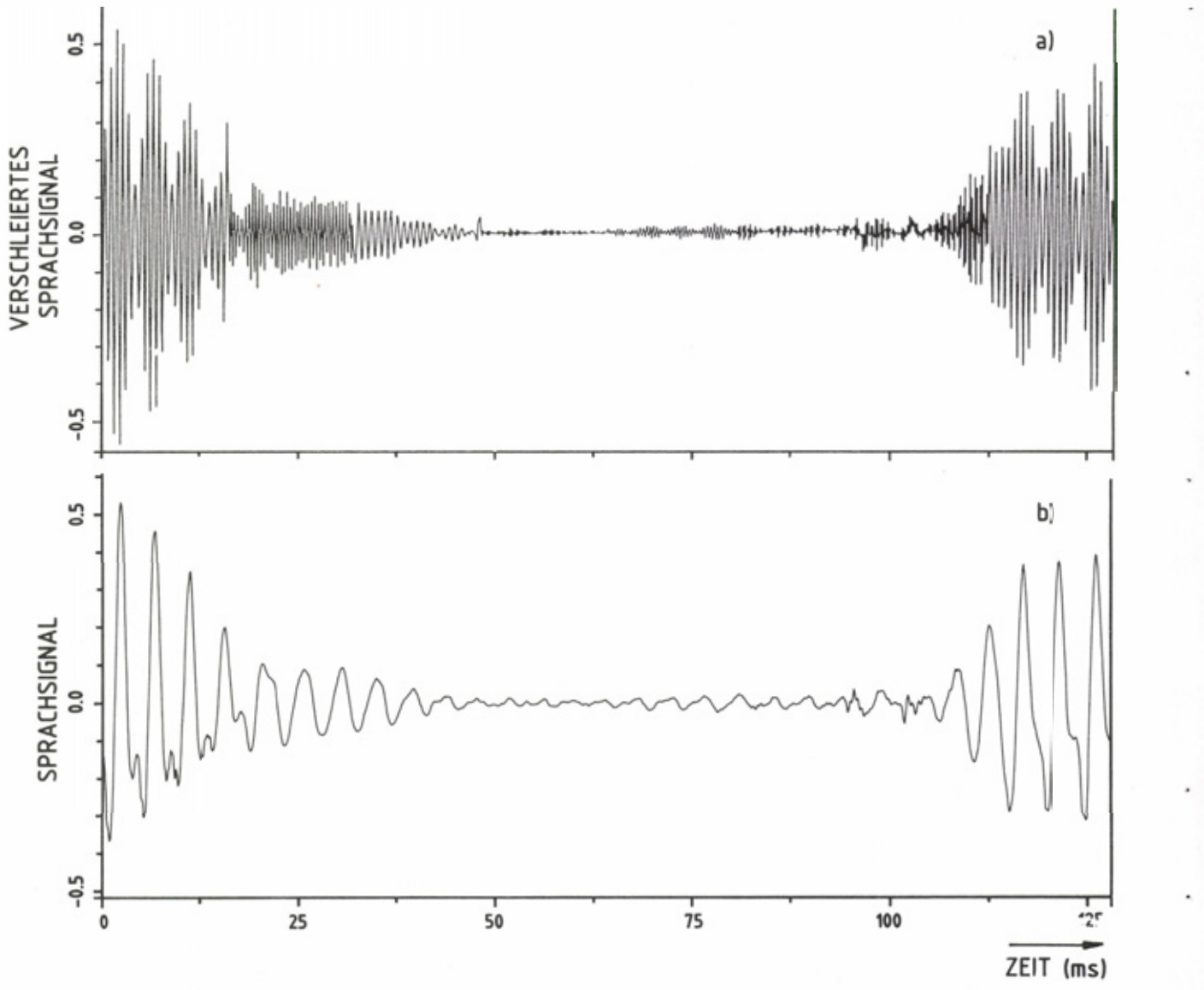


Fig. 2 Ein nach einem Frequenzbereichsverfahren verschleiertes Sprachsignal (a) und das Original-Sprachsignal (b).

Wenn die Verschleierung ausschliesslich auf der Zeit- oder Frequenzachse erfolgt, spricht man von einem 1-dimensionalen, wenn sie auf beiden Achsen erfolgt von einem 2-dimensionalen Verfahren. Am wirksamsten für eine erste Reduktion der Restverständlichkeit sind Frequenzbereichsmethoden, denn sie zerstören die Kurzzeitspektren der einzelnen Laute (Vokale, Diphtonge und Konsonanten). Allerdings bewirken diese Methoden keine Veränderung des Sprachrythmus, so dass der Signalverlauf (zeitlich und meistens auch amplitudenmässig) unverändert bleibt (Fig. 2). Aus diesem Grund, und wegen der aus Kausalitätsgründen (Einschwingvorgänge der Trennfilter) stark begrenzten Verwürfelungsmannigfaltigkeit (= zu kleine kryptologische Sicherheit) werden Frequenzbereichsmethoden meistens nur zusammen mit Zeitbereichsmethoden benützt.

Zeitbereichsmethoden zerstören den Sprachrythmus, vorausgesetzt, dass die zeitliche Versetzung der einzelnen Sprachausschnitte gross genug ist. Nachteil dieser Methoden ist es, dass die meistens 20 ms und grösseren Sprachausschnitte leider noch zu viel unverändertes Originalsprachsignal beinhalten. Da 20 ms ungefähr 1,5 - 2 Pitchperioden eines Mannes mit normaler Stimme (75 - 100 Hz) entsprechen und 4 Pitchperioden einer Frauenstimme, enthält es genügend Information, so dass die Methoden der digitalen Sprachanalyse aussagefähig angewendet werden können. Um die Struktur der einzelnen Laute zu zerstören, müsste die Zeitverwürfelung mit Sprachausschnitten von höchstens 1 - 2 ms (d.h. mit einigen Abtastwerten) erfolgen! Dies hätte aber eine Bandbreiteexpansion und eine starke Reduktion der Robustheit gegen Kanalverzerrungen zur Folge.

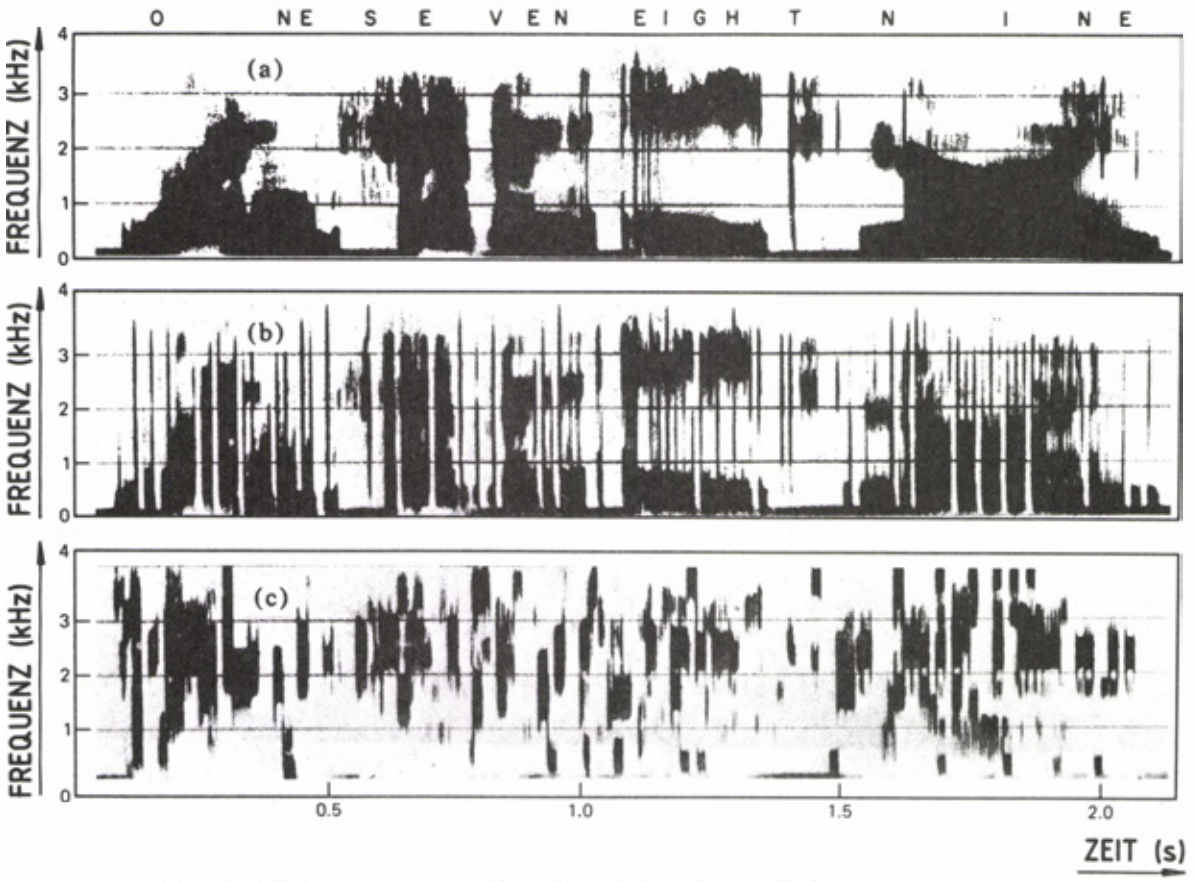


Fig. 3 Spektrogramm vom Original-Sprachsignal (a) und von einem 1-dimensional (b) bzw. von einem 2-dimensional verschleierten Sprachsignal (c) aus /3/

Die 2-dimensionalen Sprachverschleierungsmethoden gewähren einen besseren Schutz gegen unbefugtes Abhören als 1-dimensionale (Fig. 3). Dennoch sind auch hier Grenzen gesetzt. Kausalität, unwirksame Permutationen, beschränkte zeitliche Versetzung (gegeben durch die bereits erwähnte, maximal zumutbare Zeitverzögerung im Betrieb), reduzieren stark die für eine gute Sicherheit nötige Anzahl brauchbarer Verwürfelungsmöglichkeiten. Bei einer ungenügend grossen Vertauschungsmannigfaltigkeit ist aber die Möglichkeit einer erfolgreichen Kryptanalyse nicht mehr mit grosser Wahrscheinlichkeit ausschliessbar. Mit der Sprachverschleierung kann aus diesen Gründen prinzipiell nur eine beschränkte Abhörsicherheit erreicht werden /2/.

Der Einsatz von Sprachverschleierungsgeräten ist somit nur dann verantwortbar, wenn die zu schützenden, gesprochenen, vertraulichen Informationen einen stark zeitbegrenzten Wert haben. Die Abhörsicherheit muss auf jeden Fall hinreichend sein, damit die verschleierten Sprachsignale nicht innert nützlicher Frist dekryptierbar sind. Dies bedeutet, dass nicht nur die Restverständlichkeit klein, sondern auch die kryptologische Sicherheit gross genug sein muss. Fig. 4 zeigt einen Fall, wo diese Forderung nicht erfüllt war: Die Restverständlichkeit war zwar klein (Frequenzverwürfelung), aber eine erfolgreiche Dekryptierung in Folge zu kleiner Verwürfelungsmannigfaltigkeit möglich.

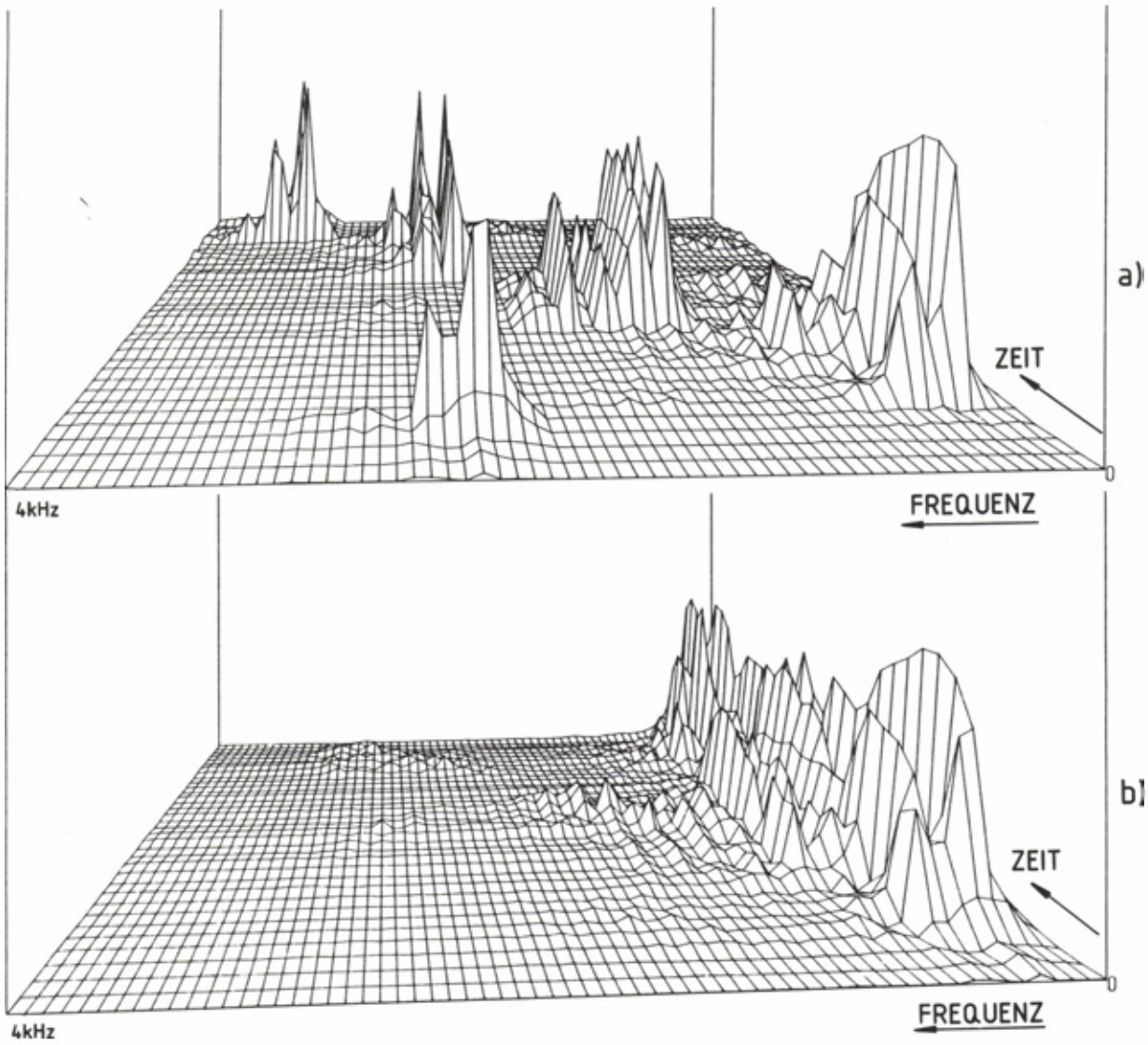


Fig. 4 3-dimensionale Darstellung eines nach einem 4-Band-Verwürfelungsverfahren verschleierten Sprachsignals (a) und das Original-Sprachsignal in der gleichen Darstellung (b).

Sprachverschleierungsverfahren waren die ersten Verfahren, die zum Schutze der Sprachinformation auf dem Uebertragungsweg gegen unbefugtes Abhören entwickelt worden sind. Sie traten in folgender historischer Reihenfolge auf: Frequenzbereichsverfahren, Zeitbereichsverfahren, 2-dimensionales Verfahren, "Multi-dimensionale"-Verfahren /6/. Lange waren sie die einzige Möglichkeit, Sprachübertragung über schmalbandige Kanäle,wie Telefon- und Kurzwellenkanäle zu schützen, bis die ersten kostengünstigen Vocoder mit akzeptabler Sprachqualität entwickelt worden sind. Keines der heutigen Sprachverschleierungsgeräte erlaubt einen echten Vollduplex-Betrieb, denn je besser die Verschleierung der Sprachsignale,desto weniger robust sind sie gegenüber Kanalverzerrungen. Ihr Einsatz ist nur mit Sprechtaste oder mit VOX-Control, das einen Quasi-Vollduplex-Betrieb erlaubt, möglich, so dass dem Benützer betriebliche Einschränkungen auferlegt sind /4/ - /5/.

2.3 DAS ZENTRALE PROBLEM DER SPRACHCHIFFRIERUNG: DIE ZUR VERFUEGUNG STEHENDE BANDBREITE

Im Gegensatz zur Sprachverschleierung gewährt die Sprachchiffrierung eine beinahe absolute Abhörsicherheit, die allein von der Güte des verwendeten Chiffrierverfahrens abhängt. Die Chiffrierung setzt eine vorherige Digitalisierung der zu übertragenden, analogen Sprachsignale voraus (Fig. 5).

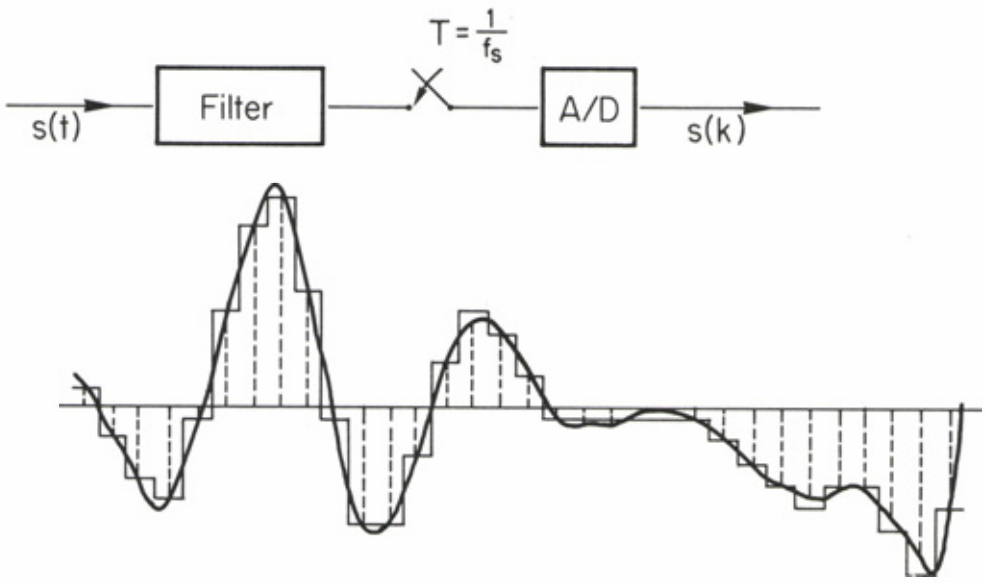


Fig. 5 Die Digitalisierung von Sprachsignalen

Fig. 6 Chiffrierung von Sprache und Daten

Der durch Abtastung, Analog-/Digital-Wandlung und geeignete Codierung entstehende Bitstrom wird wie ein üblicher Datenstrom chiffriert (Fig. 6). Chiffrierte digitalisierte Sprache ist also ein Datenstrom, wie er auf chiffrierten Verbindungen zwischen Computer und Terminals vorzufinden ist. Zu seiner Uebertragung über analoge Kanäle, wie z.B. das Telefonnetz, werden daher Modems benötigt (Fig. 7). Das auf einer analogen Uebertragungsstrecke vorzufindende Signal ist somit ein,vom Modem geeignet moduliertes, chiffriertes Datensignal, das für den Menschen unverständlich ist. Die Restverständlichkeit ist Null und die kryptologische Sicherheit hängt ausschliesslich vom verwendeten Chiffriergenerator ab. Das Spektrogramm chiffrierter Sprache ist weiss (Fig. 8), unabhängig, ob dabei gesprochen wurde oder nicht (Verkehrssicherheit).

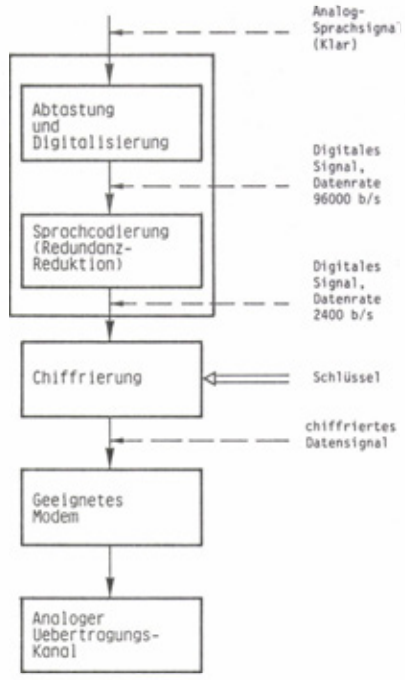


Fig. 7 Chiffrierte Sprachübertragung über schmalbandige, analoge Uebertragungskanäle

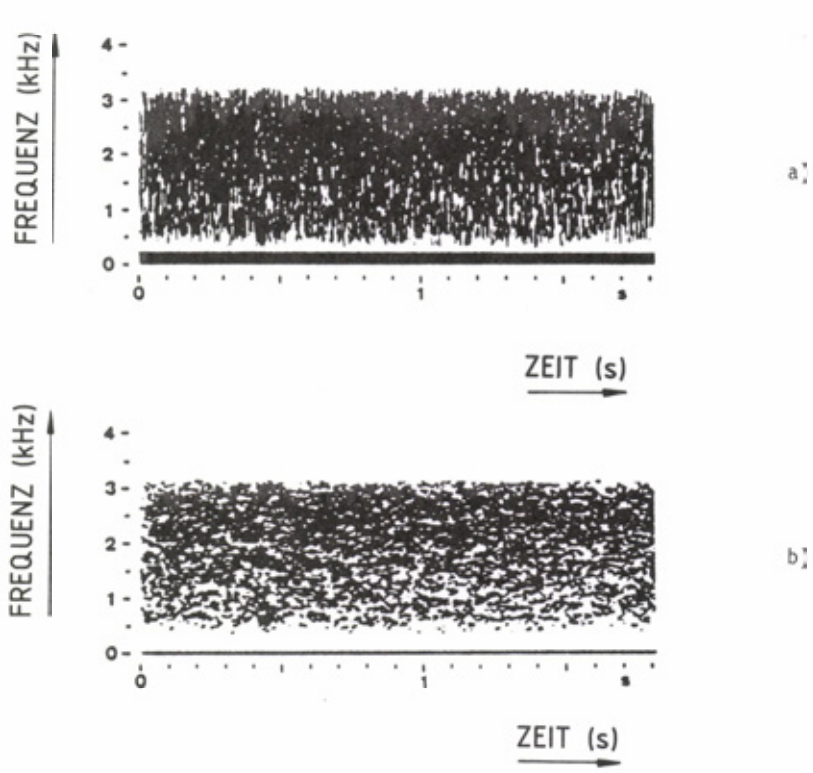


Fig. 8 Das Spektrogramm der chiffrierten Sprache auf der Leitung (vergl. mit Fig. 3)

(a) Breitband: Δf = 300 Hz
(b) Schmalband: Δf = 45 Hz

Das zentrale Problem der Sprachchiffrierung ist, dass der Bandbreitebedarf für die Uebertragung digitaler Sprachsignale wesentlich höher ist, als für die Uebertragung analoger Sprachsignale. Um eine chiffrierte, digitale Sprachübertragung über gegebene Kanäle zu ermöglichen, ist daher oft eine beachtliche Reduktion der benötigten Bitrate (Redundanzminderung) erforderlich.

Diese Aufgabe ist, je nach der für die Sprachübertragung gegebenen Kanalbreite, mehr oder weniger schwierig. Neue Sprachcodierverfahren ermöglichen heute ohne grosse Sprachqualitätsverminderung, die für die Uebertragung chiffrierter, digitalisierter Sprache benötigte Datenrate auf 2'400 b/s zu reduzieren. Die heutigen Telefon- und Kurzwellenmodems können eine solche Datenrate über das weltweite Telefonnetz und Kurzwellenkanäle im Vollduplex-Betrieb übertragen. Damit ist eine beinahe absolut sichere Sprachübertragung über solch schmalbandige Kanäle möglich. Auch gibt es für den Benützer keine betrieblichen Einschränkungen, wie z.B. Sprechtaste.

3. SPRACHDIGITALISIERUNG UND -CODIERUNG

Sprachsignale sind analoge Signale, kontinuierlich in der Zeit und in der Amplitude. Durch die Sprachdigitalisierung werden sie in zeitdiskrete und amplitudendiskrete Signale umgewandelt und gleichzeitig komprimiert zur effizienten Uebertragung. Ein 3,4 kHz-bandbegrenztes Sprachsignal muss gemäss Abtasttheorem mindestens mit 6,8 kHz abgetastet werden. Benutzt man für die Abtastung 8 kHz und verwendet man für die Quantisierung und Codierung einen logarithmischen 8-bit-Wandler nach A-Kennlinie, so muss man 64'000 Bit pro Sekunde übertragen. Dies ist der Fall bei der verbreiteten (logarithmischen) Pulscodemodulation (PCM Codierung), wie sie z.B. im Integrierten Fernmeldesystem (IFS) der Schweizer PTT verwendet wird. Solche CODEC's erhält man auf dem Markt in einem Chip. Fig. 9 zeigt zur Illustration eine 4-Bit lineare PCM.

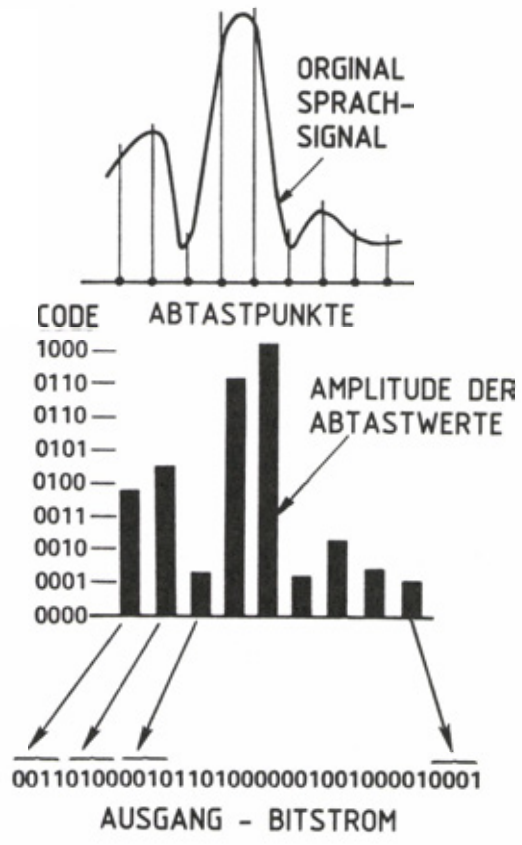


Fig. 9 Lineare 4-Bit-Pulscodemodulation (4-Bit PCM) und der dabei entstehende Sprachbitstrom

Die verschiedenen Sprachdigitalisierungsverfahren werden in drei Gruppen eingeteilt, je nach den zur Redundanzverminderung verwendeten Ansätzen:

- Signalformcodierungsverfahren
- Parametrische (Vocoder-) Verfahren
- "Hybride" Sprachcodierungsverfahren

Jede dieser drei Verfahrensgruppen ist für einen bestimmten Datenraten-Bereich die Bestgeeignetste. Je kleiner die über den gegebenen Kanal übertragbare Datenrate (je schmalbandiger der gegebene Uebertragungskanal), desto grösser ist die zu realisierende Redundanzreduktion und desto komplexer (und teurer) ist das Sprachcodierungsverfahren.

Signalformcodierungsverfahren setzen keine Annahmen betreffend der Sprachsignalerzeugung voraus und benützen lediglich die statistischen Eigenschaften der Sprachsignale für eine optimale Quantisierung und Codierung /8/. Vertreter dieser Gruppe sind die bereits erwähnte Pulscodemodulation PCM, die (Adaptive) Differenz-Pulscodemodulation (A)DPCM, die (Adaptive) Deltamodulation (A)DM, aber auch neuere Sprachcodierungsverfahren wie Teilbandcodierung (Subband Coding SBC) /9/ und Adaptive Transformationscodierung (ATC) /10/. Die für die digitale Sprachübertragung benötigten Datenraten liegen mit diesen Verfahren zwischen 64 kb/s und 9,6 kb/s. Sie erlauben eine digitale Sprachübertragung über Breitbandkanäle mit relativ kleinem Aufwand und guter Qualität. Als konkretes Beispiel sei hier die in militärischen digitalen Teilnehmerstationen (DTS) verwendete 32 kb/s "Continuously Variable Slope Delta-Modulation" (CVSD) erwähnt /11/. Hier wird das Sprachsignal mit 32 kHz abgetastet, mit dem Ziel, die Abweichung zwischen zwei nachfolgenden Abtastwerten derart klein zu halten, dass sie mit nur einem Bit beschrieben werden kann (Fig. 10).

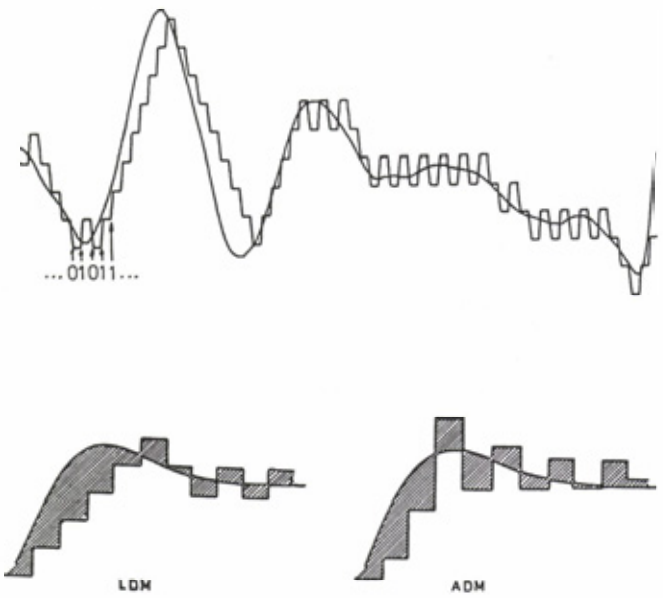
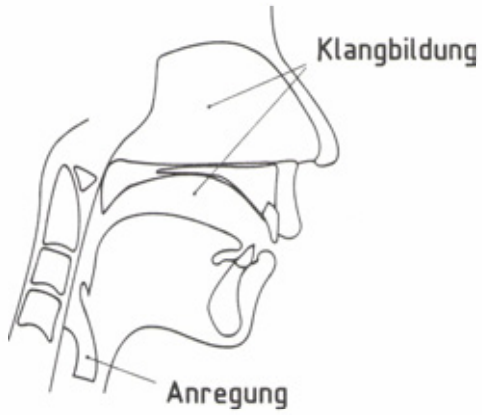


Fig. 10 Adaptive Deltamodulation. Man vergleiche ADM (adaptiv) mit LDM (linear).

Parametrische (Vocoder-) Verfahren ermöglichen eine wesentlich grössere Reduktion der zur chiffrierten digitalen Sprachübertragung benötigten Datenrate und Bandbreite /12/ - /13/. Sie setzen ein parametrisches Modell der menschlichen Spracherzeugung voraus. Wichtige Vertreter dieser Gruppe sind die linearen Prädiktions-(LPC) Vocoder. Fig. 11 zeigt das dabei verwendete parametrische Modell, das im Abschnitt 3.1 ausführlich beschrieben wird. Solche Vocoder ermöglichen eine chiffrierte Sprachübertragung über schmalbandige Kanäle (z.B. Telefonnetz). Die dabei verwendeten Datenraten sind 2,4 kb/s, 3,6 kb/s und 4,8 kb/s. Der Aufwand für die Realisierung von Vocodern ist wesentlich grösser als für Signalformcodierungsverfahren. Doch sind die Kosten für die dafür gebotene Sicherheit heute vertretbar.



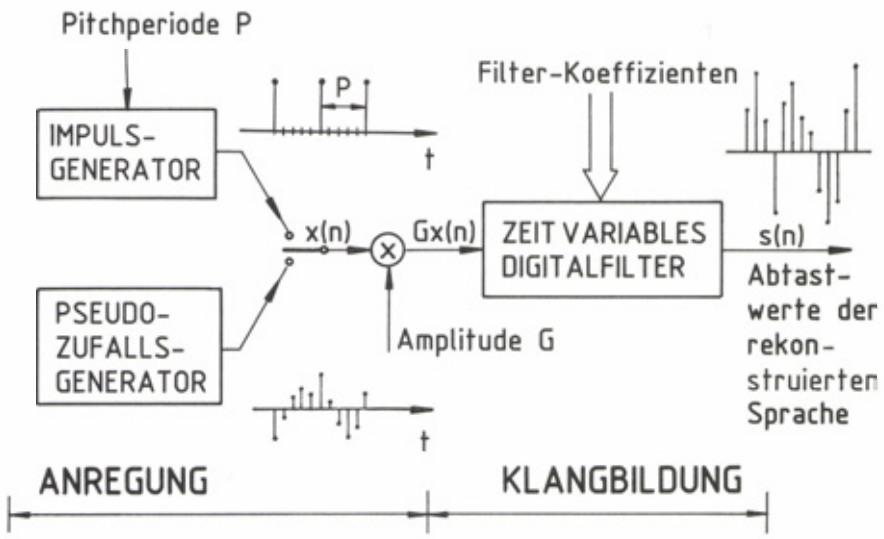


Fig. 11 Parametrisches Modell der Spracherzeugung beim Menschen

Hybride Sprachcodierungsverfahren verwenden eine Kombination von Signalformcodierung und parametrischer Sprachsignalcodierung /14/ - /15/. Sie haben zum Ziel, eine digitale Sprachübertragung mit möglichst guter ("transparenter") Sprachqualität bei einer mittleren Datenrate (zwischen 16 und 4,8 kb/s) zu ermöglichen. Dies ist zur Zeit ein sehr aktuelles Forschungsgebiet. Wichtige Vertreter dieser Gruppe sind:

- Restfehler-angeregter Vocoder (RELP, Residual-Excited LPC-Vocoder)
- Multipuls-angeregter Vocoder (MELP, Multipulse-Excited LPC-Vocoder)

Diese Verfahren sind, zusammen mit der Teilbandcodierung (Subband Coding), die ein neueres Signalformcodierungsverfahren ist, potentielle Kandidaten für den neuen 16 kb/s - 9,6 kb/s-Sprachdigitalisierungsstandard der CCITT. Diese drei Verfahren werden im folgenden daher ausführlich beschrieben.

3.1 PARAMETRISCHE SPRACHCODIERUNG NACH DER METHODE DER LINEAREN PRAEDIKTION (LPC-VOCODER)

Der LPC-Vocoder wird heute für militärische, schmalbandige (chiffrierte) digitale Sprachübertragung (2'400 b/s) in den USA und in den NATO-Ländern als Standard unter der Bezeichnung LPC 10 verwendet /16/ - /17/. Die mit dieser Sprachcodierung, trotz niedrigster Datenrate, erreichbare Sprachverständlichkeit und Sprechererkennung waren bei seiner Wahl zum Standard entscheidend.

Fig. 11 zeigt das dieser Sprachcodierung zugrundeliegende parametrische Modell der Spracherzeugung beim Menschen. Dabei werden Anregung durch die Stimmbänder oder durch Luftturbulenz von den Lungen und die eigentliche Klangbildung durch den Hals- und Mundtrakt separat modelliert. Die Anregung ist stark idealisiert. Sie ist bei stimmhaften Lauten wie /a/, /o/, /u/, /i/ eine Pulsfolge, deren Frequenz die Stimmbandgrundfrequenz (Pitch-Frequenz) ist. Bei stimmlosen Lauten wie /f/, /s/ ist sie eine Pseudozufallsfolge (weisses Rauschen), idealisierend für die Luftturbulenz im Hals, wenn die

Stimmbänder nicht angeregt werden. Das für die Klangbildung verantwortliche lineare Uebertragungssystem wird durch ein zeitvariables, rekursives Digitalfilter mit z.B. 10 Koeffizienten modelliert. Der Verstärkungsfaktor G schliesslich kontrolliert die Lautstärke.

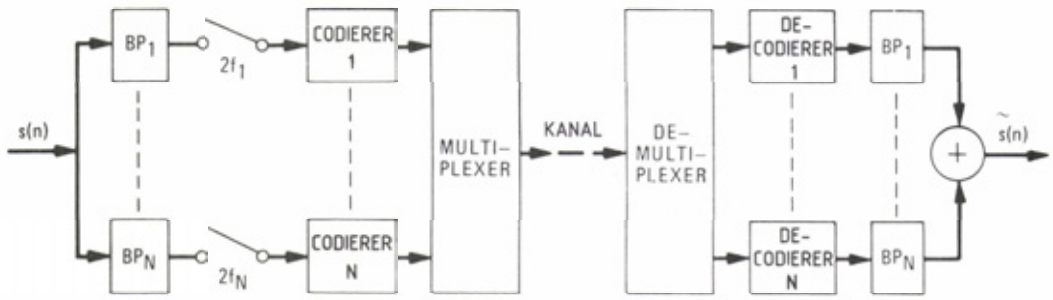
Die beachtliche Redundanzreduktion wird nun dadurch erzielt, dass für jeden Sprachsignalausschnitt von z.B. 22,5 ms (180 Abtastwerte) 12 Modellparameter berechnet, effizient codiert und anstelle der 180 12-Bit-Abtastwerte übertragen werden (10 Filterkoeffizienten, Pitch-Periode P und der Verstärkungsfaktor G) /18/.

Empfängerseitig werden die 12 Parameter im Sprachmodell eingesetzt und dieses liefert 180 12-Bit Sprachabtastwerte, die (meistens) nur wenig von den 180 Abtastwerten des Original-Sprachsignals abweichen.

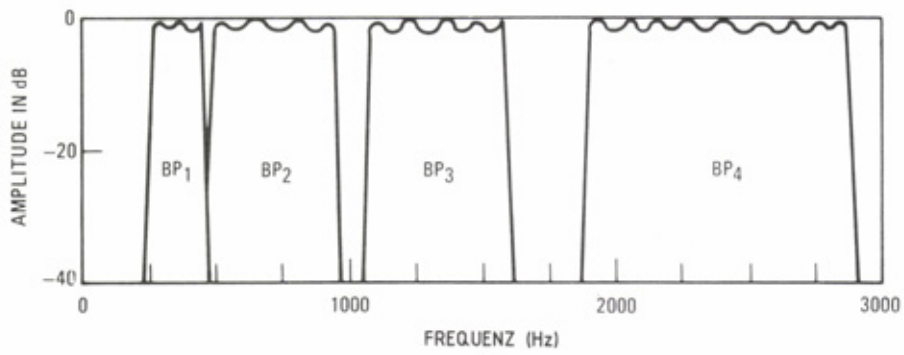
Auf diese Art und Weise kann Sprache bei Datenraten zwischen 2'100 b/s und 4'800 b/s ohne grosse Qualitätseinbusse übertragen werden. Im Kapitel 6 wird ein Sprachchiffriergerät beschrieben, das einen LPC-Vocoder zur Sprachdigitalisierung benützt.

3.2 DIE TEILBANDSPRACHCODIERUNG (SUBBAND-CODING)

Bekanntlich ist der Hauptanteil der Sprachsignalenergie bei tiefen Frequenzen konzentriert. Die Teilbandsprachcodierung macht von dieser Eigenschaft der Sprachsignale Gebrauch. Das analoge Sprachsignal wird dabei mit vier bis sechs Bandpassfiltern filtriert.



(a)



(b)

Fig. 12 Die Teilbandsprachcodierung aus /9/

Die resultierenden vier bis sechs Signale werden abgetastet, mit Adaptiver Pulscodemodulation einzeln codiert und miteinander multiplexiert für die Uebertragung (Fig. 12). Empfängerseitig werden sie zuerst demultiplexiert, dann decodiert und anschliessend mit den gleichen Bandpassfiltern filtriert. Die Rekonstruktion der Sprachsignale erfolgt durch Aufaddition der Ausgangssignale der Bandpassfilter.

Die Datenreduktion wird durch eine subjektiv optimale Bitzuteilung in den einzelnen Teilbändern erreicht (vgl. untenstehende Tabelle). Dieses Verfahren erlaubt eine sehr gute Sprachqualität bei 16 kb/s und "Kommunikations"-Qualität bei 9,6 kb/s (beide Male besser als z.B. Adaptive Deltamodulation bei gleichen Datenraten).

Die nachstehende Tabelle zeigt als Beispiel die technischen Daten eines Subband-Codecs aus /9/. Dabei werden 470 Bits für Rahmensynchronisierung verwendet.

Band	Bandgrenzen	Abtastrate (Hz)	Bits	kb/s
1	178- 356	356	4	1,42
2	296- 593	593	4	2,37
3	533-1062	1067	3	3,20
4	1067-2133	2133	2	4,27
5	2133-3200	2133	2	4,27
SYNC				0,47
Total				16,00

3.3 RESTFEHLER- UND MULTIPULS-ANGEREGTE LPC-VOCODER (RELP UND MELP-CODECS)

Die in LPC-Vocodern zur Sprachsynthese verwendeten Anregungssignale (Pulsfolge bei stimmhaften Lauten; Pseudozufallsfolge bei stimmlosen Lauten) sind starke Vereinfachungen des Restfehlersignals aus der Sprachanalyse. In der Tat beinhaltet das restliche Prädiktionsfehlersignal neben dem im Ansatz definierten Anregungssignal auch ein Fehlersignal aus der unvollkommenen Modellierung von Hals- und Mundtrakt mit einem zeitvariablen Digitalfilter (Fig. 11).

Für eine verbesserte Natürlichkeit der synthetisierten Sprache sollte man deshalb das rekursive Digitalfilter des Sprachmodells mit dem restlichen Prädiktionsfehler anregen. Um dies tun zu können, muss dieses Signal auch vom Sender zum Empfänger übertragen werden. In RELP Vocodern wird das restliche Prädiktionsfehlersignal effizient codiert und anstelle der Pitchinformation übertragen (Fig. 13). Der Preis ist eine beachtliche Erhöhung der Datenrate von 2,4 kb/s auf 9,6 kb/s /19/ - /20/.

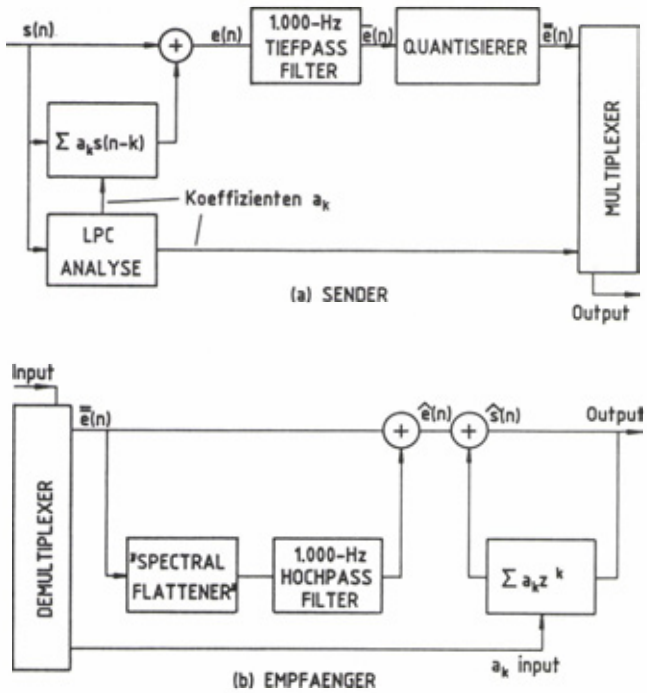


Fig. 13 Der Restfehler-angeregte LPC-Vocoder. In diesem Typ wird das Restfehlersignal auf 1 kHz bandbegrenzt, dezimiert und die verbleibenden 2'000 Abtastwerte pro Sekunde mit 3-Bit-PCM codiert.

Die neuen MELP-Vocoder (Multipulse-Excited LPC-Vocoder) stellen eine vielversprechende Alternative zu den RELP Vocodern dar. Sie lösen das Problem der effizienten Uebertragung des Anregungssignals wie folgt (Fig. 14):

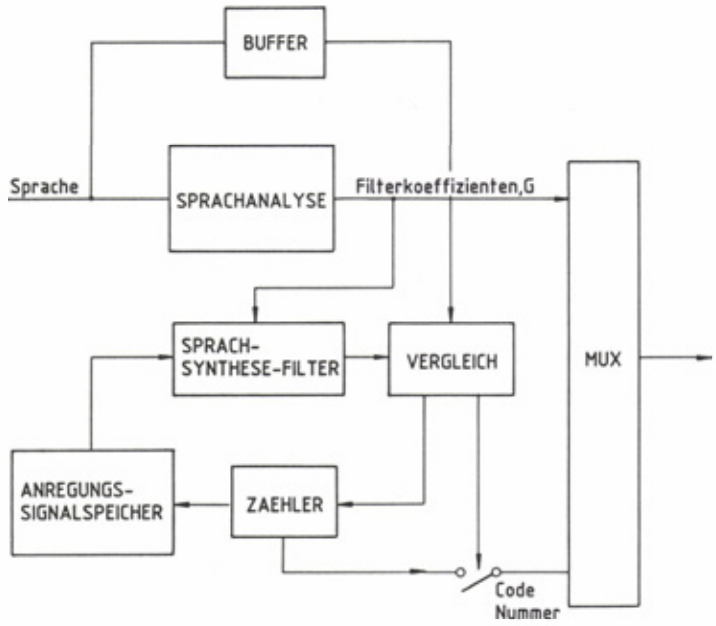


Fig. 14 Der Multipuls-angeregte LPC-Vocoder

Nachdem sendeseitig die Filterkoeffizienten berechnet worden sind, werden sie im Sprachmodell (des Senders) eingesetzt. Dieses wird dann von einer bestimmten Anzahl von abgespeicherten Anregungssignalen angeregt (z.B. 1024). Nach jeder neuen Anregung vergleicht man das entstandene sythetisierte Sprachsignal mit dem Original. Dasjenige Anregungssignal, das zu den kleinsten Abweichungen gegenüber dem Original-Sprachsignal führt, wird gewählt und seine Code-Nummer wird mit den Filterkoeffizienten und dem Verstärkungsfaktor G übertragen /21/ - /23/.

Sobald die Code-Nummer eingetroffen ist, liegt, mit der gleichen Anzahl von Anregungssignalen im Empfänger, das zu benützende Anregungssignal vor. Die Sprachsynthese kann sofort erfolgen. Auf diese Weise kann eine sehr gute Sprachqualität bei 9,6 kb/s erzielt werden. Nachteil dieses Verfahrens ist vor allem der grosse Rechenaufwand bei der Auswahl der bestgeeigneten Anregungsfunktionen im Sender.

4. CHIFFRIERUNG DER DIGITALISIERTEN SPRACHE

Wie bereits betont, schützt die Sprachdigitalisierung mittels CODEC nicht gegen Abhorchen durch Unberechtigte. Digitale Sprache ist auf dem Uebertragungsweg für den unbefugten Abhörer zwar primär unverständlich (Restverständlichkeit Null!), aber es genügt, dass er den geeigneten CODEC zur Verfügung hat, um in der Lage zu sein, alles mitzuhören.

Die Kommunikationssicherheit bei der digitalen Sprachübertragung wird allein vom verwendeten Chiffrierverfahren (Chiffriergenerator) bestimmt. Es allein gewährt Abhör- und kryptologische Sicherheit. Eine einfache, digitale Verwürfelung der codierten Sprache mit einem linear rückgekoppelten Schieberegister (Digital Scrambler) kann nur beschränkte Sicherheit bieten (etwa wie ein besseres Sprachverschleierungsgerät) /24/. Daher ist bei der Evaluation von Sprachchiffriergeräten den kryptologischen Daten die höchste Aufmerksamkeit zu schenken. Im folgenden erläutern wir die Anforderungen an das verwendete Chiffrierverfahren. Gleichzeitig wird eine kurze Einführung in die Chiffrierarten gegeben (Bitstrom-/Blockchiffrierung und Kanal-/End-zu-End-Chiffrierung). Das Kapitel schliesst mit einigen Bemerkungen über die Bedeutung des Schlüsselmanagements für die chiffrierte Sprachübertragung.

4.1 CHIFFRIERARTEN

Die eigentliche Chiffrierung der codierten digitalen Sprache kann prinzipiell auf zwei verschiedene Arten erfolgen /25/ - /28/:

a) Kontinuierlich (Bit für Bit) durch Modulo-2-Addition des Chiffrierprogramms zum Sprachbitstrom. Diese Chiffrierart wird Bitstromchiffrierung (stream cipher) genannt und wird in Fig. 15 illustriert.

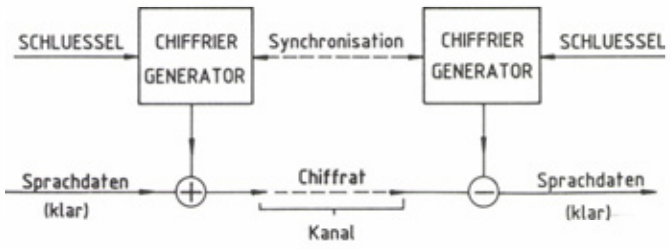


Fig. 15 Bitstromchiffrierung

b) Blockweise: die codierte, digitalisierte Sprache wird dabei in Blöcke gleicher Länge geteilt und durch Modulo-2-Addition mit Chiffrierprogramm-Blöcken gleicher Länge chiffriert (Fig. 16). Diese Chiffrierart wird Blockchiffrierung (block cipher) genannt.

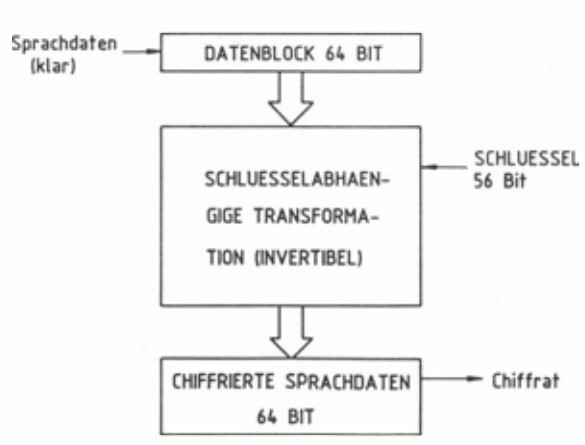


Fig. 16 Blockchiffrierung

Bitstromchiffrierung wird für die Chiffrierung der Sprache bevorzugt gebraucht. Sie hat den Vorteil, dass Uebertragungsfehler keine Fehlerfortpflanzung zur Folge haben wie bei der Blockchiffrierung. Bitstromchiffierung setzt allerdings eine gute Synchronisierung vom Sender und Empfänger voraus.

4.2 ANFORDERUNGEN AN DAS VERWENDETE CHIFFRIERVERFAHREN

Für hohe Abhörsicherheit muss der verwendete Chiffriergenerator eine hohe kryptologische Resistenz gegen Attacken der Kryptanalyse besitzen. Dies bedeutet insbesondere:

- Verwendung von nichtlinearen Verknüpfungen
- Erzeugung einer Pseudo-Zufallsfolge mit ähnlichen statistischen Eigenschaften, wie weisses Rauschen.

Von diesen Hauptanforderungen lassen sich drei Anforderungen an den Chiffriergenerator ableiten. Dies sind:

1) eine sehr lange Periode
2) eine grosse Rekursionslänge (= lineare Komplexität)
3) eine grosse Schlüsselmannigfaltigkeit

Anforderungen 1) und 2) haben zum Ziel, die Beschaffung benötigter Informationen für eine Kryptanalyse zu erschweren und mit Anforderung 3) wird eine erfolgreiche Absuchattacke praktisch verunmöglicht.

Bei der Auslegung des Chiffriergenerators muss darauf geachtet werden, dass diese geforderten Spezifikationen streng mathematisch unter Kontrolle sind und für jede Schlüsselwahl erfüllt sind.

Ist die hohe kryptologische Resistenz gewährleistet, so ist die Sicherheit der chiffrierten Sprachübertragung nur durch Aneignung eines entsprechenden Sprachchiffriergerätes und gleichzeitiger Kenntnis des verwendeten Schlüssels gefährdet. Durch die Verwendung von zwei geheimen orthogonalen Schlüsseln, kann die Gefährdung infolge Schlüsselverrates ebenfalls reduziert werden.

4.3 KANAL- UND END-ZU-END-CHIFFRIERUNG

Aehnlich wie bei der Datenchiffrierung können bei der Sprachchiffrierung zwei Grundformen der Kommunikationssicherheit unterschieden werden /26/:

End-zu-End-Chiffrierung gewährleistet die Sprachkommunikationssicherheit vom Sender zum Empfänger über die gesamte Uebertragungsstrecke, da die Chiffrierung und Codierung, bzw. Dechiffrierung und Decodierung direkt bei den Endbenützern erfolgt. Die End-zu-End-Chiffrierung wird bei der digitalen Sprachübertragung bevorzugt benützt. Sie schliesst eine netzeigene Chiffrierung nicht aus.

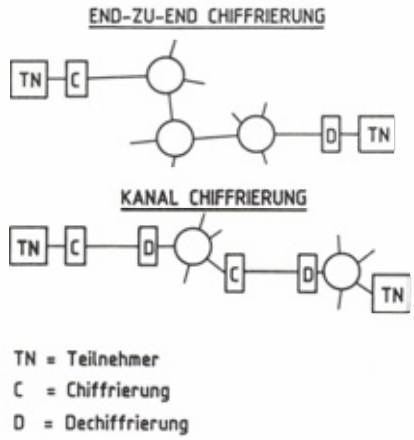


Fig. 17 Kanalchiffrierung

Kanalchiffrierung (Fig. 17) erlaubt die Sprachübertragung über besonders gefährdete Uebertragungsstrecken, wie Satelliten-, Richtstrahl- oder Kurzwellen-Kanäle, gegen Abhorchen zu schützen, falls eine End-zu-End-Chiffrierung nicht allen Benützern zur Verfügung gestellt werden kann. Kanalchiffrierung wird in integrierten digitalen Netzen eingesetzt, ist netzeigen und schliesst eine End-zu-End-Chiffrierung nicht aus.

4.4 SCHLUESSELMANAGEMENT

Durch Chiffrierung der Sprache ist der Schutz gegen Abhorchen beliebig hoch wählbar, so dass eine eigentliche Gefährdung nur durch einen Verrat des/der geheimen Schlüssel(s) entstehen kann. Deshalb muss der Erzeugung, Verteilung, Eingabe und Speicherung, sowie der Löschung der geheimen Schlüssel die höchste Bedeutung zugemessen werden. Schlüsselmanagement ist ein zunehmend wichtiger Teil der Sprachkommunikationssicherheit.

5. EINSATZARTEN DER SPRACHHIFFRIERUNG

Zur Illustration der Einsatzarten der Sprachchiffrierung werden zwei grundsätzlich verschiedene Fälle betrachtet. In einem Fall erfolgt die chiffrierte Sprachübertragung breitbandig über digitale Kanäle, im andern Fall schmalbandig, mittels geeigneter Modems über analoge Telefon- und HF-Kanäle.

5.1 CHIFFRIERTE SPRACHUEBERTRAGUNG UEBER DIGITALE KANAELE EINES INTEGRIERTEN FERNMELDESYSTEMS

Hier liegen Verhältnisse wie für eine Datenchiffrierung vor. Die digitalen Kanäle sind für die Uebertragung von 64 kb/s bzw. 32 kb/s oder 16 kb/s ausgelegt,und die Sprachcodierung ist in den digitalen Teilnehmerstationen (DTS) oft bereits realisiert. Die verwendete Sprachcodierung ist entweder Pulscodemodulation (64 kb/s) oder Adaptive Deltamodulation (32 kb/s bzw. 16 kb/s). Sowohl Kanal-, als auch End-zu-End-Chiffrierung kann eingesetzt werden. Beim Entwurf des Chiffrierverfahrens muss vor allem darauf geachtet werden, dass bestimmte Randbedingungen im Zusammenhang mit dem Netz-Protokoll erfüllt werden, dass das Schlüsselmanagement benützerfreundlich ist und doch die höchsten Sicherheitsansprüche erfüllt.

5.2 CHIFFRIERTE SPRACHUEBERTRAGUNG UEBER DAS WELTWEITE WAEHLNETZ UND UEBER HF-KANAELE

Für die Sprachübertragung über das weltweite Wählnetz und über HF-Kanäle steht eine Bandbreite von 300 Hz bis 3,4 kHz zur Verfügung, also rund 3 kHz. Für die Uebertragung von chiffrierter, digitalisierter Sprache müssen Modems eingesetzt werden. Heute sind Telefonmodems erhältlich, welche Datenraten von 2'400 b/s und 4'800 b/s über 2-Draht-Leitungen im Vollduplex-Betrieb erlauben /29/. Die höchsten Datenraten, die mit HF-Modems übertragbar sind, sind 2'400 b/s und 3'600 b/s /30/ - /31/. Der Uebertragungsaufwand (Datenrate) für die chiffrierte Sprachübertragung über das Wählnetz oder HF-Kanäle kann somit 2'400 b/s bis maximal 4'800 b/s betragen. Tastet man die zu übertragenden Sprachsignale mit 8 kHz ab und codiert man sie mit einem linearen 12-Bit-PCM-Quantisierer, so entsteht eine Datenrate von 96'000 b/s. Diese muss nun 20-fach bzw. 40-fach komprimiert werden, um eine übertragbare Datenrate (4'800 b/s bzw. 2'400 b/s) zu erreichen. Eine solche Redundanzreduktion kann aber, wie wir bereits gesehen haben, mit Hilfe von Vocodern erreicht werden. Der GRETACODER ® 220, der im folgenden beschrieben wird, realisiert eine dermassen grosse Redundanzreduktion.

6. BEISPIEL EINES SPRACHCHIFFRIERGERAETS FUER SCHMALBANDIGE UEBERTRAGUNGSKANAELE

Das Sprachchiffriergerät GRETACODER ®220 (Fig. 18) erlaubt eine abhörsichere Sprachübertragung über das weltweite Wählnetz und über Kurzwellenkanäle.

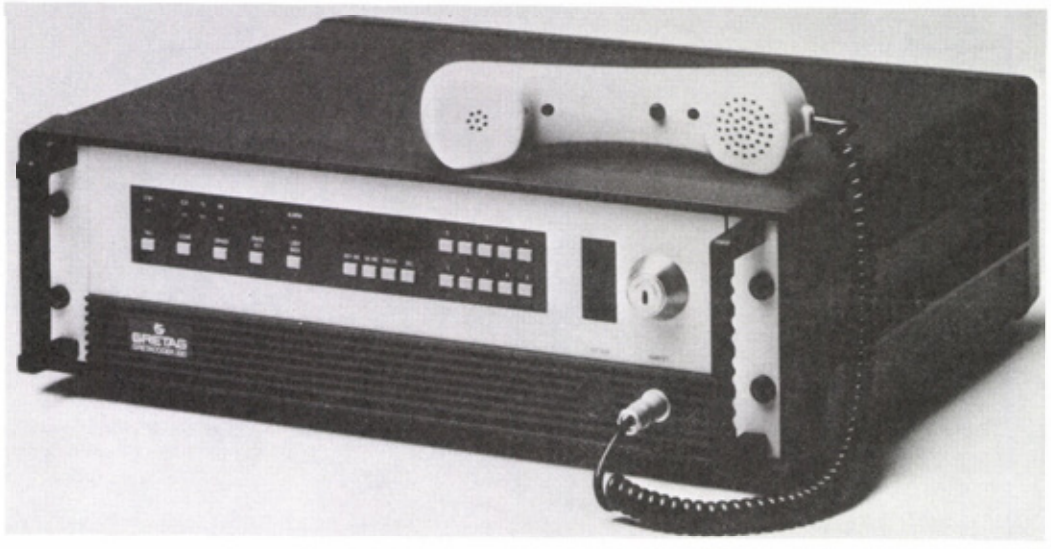


Fig. 18 Das Sprachchiffriergerät GRETACODER ®220

Das Gerät besteht aus drei Funktionseinheiten: dem LPC-Vocoder, der Chiffriereinheit und der Fernsteuereinheit (Fig. 19). Alle drei Einheiten im Innern des Gerätes sind durch ein mechanisches Schloss abgesichert. Besondere Vorkehrungen (inkl. EMV-Massnahmen) wurden getroffen, um das einwandfreie Funktionieren des Gerätes auch unter erschwerten Umweltbedingungen zu garantieren.

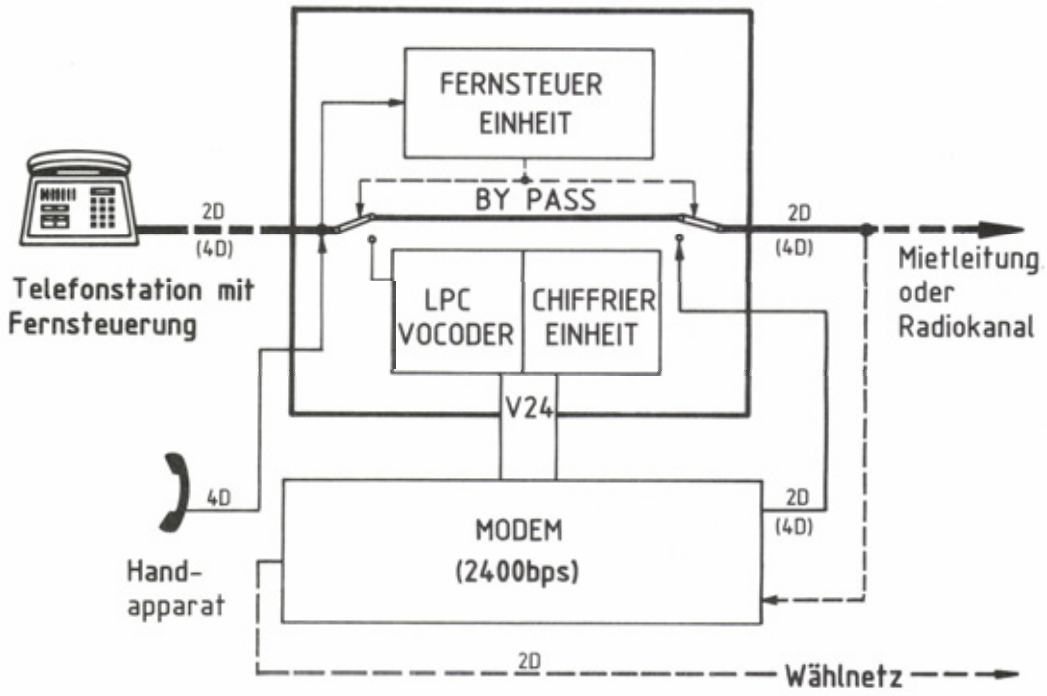


Fig. 19 Funktionsblockdiagramm des GRETACODER® 220

Für die chiffrierte Sprachübertragung benötigt der GRETACODER® 220 jeweils ein geeignetes Modem, für welches er als intelligentes Terminal gilt. Aus diesem Grunde wird der GRETACODER® 220 oft auch als Sprachchiffrierterminal bezeichnet. Die Verbindung zum Modem ist eine Standard V.24-Schnittstelle.

Fig. 20 Die Telefonstation mit Fernsteuerung

Eine mitgelieferte Telefonstation (Fig. 20) erlaubt einen normalen (nationalen oder internationalen) Verbindungsaufbau, eine ferngesteuerte Klar-/Krypto-Umschaltung und die Schlüsselwahl. Rückmeldungen des GRETACODER ® 220 bestätigen auch auf der Telefonstation, dass die Anweisungen korrekt ausgeführt worden sind oder lösen nach der Feststellung einer Fehlerfunktion eine Alarm-Anzeige aus.

Der LPC-Vocoder verwendet einen erstmalig eingesetzten Pitchdetektionsalgorithmus, ein neues Verfahren zum Stimmhaft/Stimmlos-Entscheid, eine spezielle Codierung der LPC-Parameter und eine in verschiedener Hinsicht verbesserte Sprachanalyse und -synthese. So werden z.B. wesentlich mehr Sprachsignalausschnitte (analysis frames) pro Sekunde analysiert als im LPC 10-Vocoder, um eine bessere Verfolgung des Sprachsignals während den Stimmlos/Stimmhaft-Uebergängen und bei Explosiv-Lauten zu erreichen.

Die Sprachsynthese erfolgt mit Hilfe des in Fig. 11 dargestellten und in Kapitel 3.1 besprochenen parametrischen Modells der Spracherzeugung beim Menschen. Dabei werden die folgenden LPC-Parameter verwendet: die Filterkoeffizienten k_i (Reflexionskoeffizienten), der Verstärkungsfaktor G und die Pitch-Periode P. Bei P=0 wird das rekursive Digitalfilter mit einer Pseudozufallsfolge (= stimmlos) angeregt. Das zur Sprachsynthese verwendete rekursive Digitalfilter ist ein sogenanntes 2-Multiplizierer-Kreuzglieddigitalfilter.

In der Chiffriereinheit werden die während der Analyse berechneten LPC-Parameter nach effizienter Codierung und Parallel/Serie-Wandlung Bit für Bit chiffriert. Die Bitstromchiffrierung erfolgt durch Modulo-2 Addition eines Bits des Chiffrierprogrammes zu einem Bit LPC-Parameter. Der Chiffrierprogramm-Generator ist für höchste kryptologische Sicherheit ausgelegt.

Seine kryptologischen Daten sind:

Primärschlüsselmannigfaltigkeit:	10^{48}
Sekundärschlüsselmannigfaltigkeit:	10^{1079}
Modifikationsschlüsselmannigfaltigkeit:	$4{,}4 \cdot 10^{12}$
Periode:	10^{43}
Rekursionslänge:	10^{34}

Die Primärschlüssel bestehen aus 48 Ziffern, welche von der Frontplatte aus in 8 Gruppen à 6 Ziffern eingegeben werden. 40 verschiedene Primärschlüssel können gespeichert werden. Die Sekundärschlüssel werden in einem Schlüsseleinschub von einer Schlüssel-Ladeeinheit programmiert und sind dem Benützer nicht bekannt. Beim Aufschliessen des Gerätes erfolgt eine aktive Schlüssellöschung.

Der Modifikationsschlüssel wird fehlergesichert und multiplexiert mit den chiffrierten LPC-Parametern und der Synch-Sequenz übertragen. Aus ihm werden, in Abhängigkeit der geheimen Primär- und Sekundärschlüssel, laufend neue Arbeitsschlüssel generiert.

Die robuste Synchronisation trägt dem Einsatz zur chiffrierten Sprachübertragung über Kurzwellenkanäle Rechnung. Das Gerät synchronisiert auch bei einer Bitfehlerrate von einigen Prozenten.

Eine schnelle Initialsynchronisation (< 100 ms), gefolgt von einer kontinuierlichen Synchronisation (sie wird alle 450 ms aufdatiert), ermöglichen einen schnellen Wechselverkehr (Halbduplex-Betrieb) und einen Späteintritt in weniger als einer Sekunde, sowie eine schnelle und automatische Erholung des Systems nach Fadings, Kanalstörungen oder Unterbrüchen.

Die Einsatzarten des GRETACODER ® 220 sind zahlreich: Wählnetz, Kurzwellenkanal, Hotline, Vollduplex-/Halbduplex-Betrieb, mit oder ohne Klarbypass, mit oder ohne Fernsteuerung, usw. Die gewählte Einsatzart ist mit Hilfe des hinter der (abgeschlossenen) Frontplatte angebrachten Set-up-Schalters leicht einzustellen.

Die Betriebssicherheit ist wie folgt sichergestellt: Die Tasten auf der Frontplatte sind für Unbefugte inaktiv. Das Gerät verlangt die Eingabe eines Identifikationscodes und akzeptiert keine Anweisungen, bis dieser korrekt eingegeben ist.

Ein schneller GO/NOGO-Test und ein ausführlicher Selbsttest (BITE) erlauben eine rasche Lokalisierung eines fehlerbehafteten Bauteils. Eine entsprechende Meldung wird auf dem Display angezeigt.

7. LITERATURVERZEICHNIS

/1/ Jayant N.S., McDermott B.J., Christensen S.W. and Quinn A.M.: A Comparison of Four Methods for Analog Speech Privacy. IEEE Trans.Commun., COM-29, (Januar 1981), S. 18-23.

/2/ Jayant N.S.: Analog Scramblers for Speech Privacy, Computers & Security I, North-Holland, (1982), S. 275-289.

/3/ Jayant N.S., McDermott B.J., Christensen S.W. and Quinn A.M.: Analog Scramblers for Speech Based on Sequential Permutations in Time and Frequency. B.S.T.J. 62, (Januar 1983), S. 25-46.

/4/ Cox R.V. and Tribolet J.M.: Analog Voice Privacy Systems Using TFSP Scrambling: Full Duplex and Half Duplex. B.S.T.J. 62, (Januar 1983), S. 47-61.

/5/ Delgado J.C. and Tribolet J.M.: Analog Full-Duplex Speech Scrambling Systems. IEEE Journal on Selected Areas in Commun., SAC-2, (Mai 1984), S. 456-459.

/6/ Speech and Facsimile Scrambling and Decoding. Aegean Park Press (1981).

/7/ Rabiner L.R. and Schafer R.W.: Digital Processing of Speech Signals. Englewood Cliffs, Prentice-Hall, Inc. (1978).

/8/ Flanagan J.L. et al.: Speech Coding. IEEE Trans. on Commun., COM-17, (April 1979), S. 710-737.

/9/ Crochiere R.E.: On the Design of Sub-band Coders for Low-Bit-Rate Speech Communication. B.S.T.J., 56, (Mai-Juni 1977), S. 747-770.

/10/ Zellinski R. and Noll P.: Adaptive Transform Coding for Speech Signals. IEEE Trans. on Acoustics, Speech and Signal Processing, ASSP-25, (August 1977), S. 299-309.

/11/ Un C.K. and Lee H.S.: A Study of the Comparative Performance of Adaptive Delta Modulation Systems. IEEE Trans. on Commun., COM-28, (Januar 1980), S. 96-101.

/12/ Schafer R.W. and Rabiner L.R.: Parametric Representation of Speech, in Speech Recognition. Academic Press, Inc., (1975).

/13/ Markel J.D. and Gray A.H. Jr.: Linear Prediction of Speech. Springer-Verlag, (1976).

/14/ Sambur M.R.: Speech Algorithm Advances Promise Toll-Quality Medium-Band Digitized Speech. Speech Technology, (Sept. - Oct. 1982), S. 22-31.

/15/ Schroeder M.R.: Linear Predictive Coding of Speech Signals: Review and Current Directions. IEEE Communications Magazine, 23, (August 1985), S. 54-61.

/16/ Tremain T.E.: The Government Standard Linear Predictive Coding Algorithm: LPC-10. Speech Technology, (April 1982), S. 40-49.

/17/ GarnerJ., McChesney T. and Glancy M.: Advanced Narrowband Digital Voice Terminal. Signal, (November 1982), S. 7-18.

/18/ Horvath S.: LPC-Vocoder, Entwicklungsstand und Perspektiven. Sammlung der Kolloquiumsvorträge "Krieg im Aether", Folge XVII, (Juni 1978), S. 5/1-5/16.

/19/ Copperi M. and Serneo D.: 9,6 kb/s Piecewise LPC Residual Excited Coder Using Multiple-Stage Vector Quantization. Proc. of IEEE Int. Conf. on Acoustics, Speech and Signal Processing, (1984), S. 10.5/1 -10.5/4.

/20/ Sluyter R.J., Bosscha G.J. and Schmitz M.P.I.: A 9,6 kbit/s Speech Coder for Mobile Radio Applications, in Links for the Future. North Holland, (1984), S. 1159-1162.

/21/ Atal B.S. and Remde J.R.: A New Model of LPC Excitation for Producing Natural-Sounding Speech at Low Bit Rates. Proc. IEEE Int. Conf. On Acoustics, Speech and Signal Processing, (1982), S. 614-617.

/22/ Parker A., Alexander S.T. and Trussell R.J.: Low Bit Rate Speech Enhancement Using a New Method of Multiple Impulse Excitation. Proc. IEEE Int. Conf. on Acoustics, Speech and Signal Processing, (1984), S. 1.5/1 - 1.5/4.

/23/ Berouti M., Garten H., Kabal P. and Mermelstein P.: Efficient Computation and Encoding of Multipulse Excitation for LPC. Proc. IEEE Int. Conf. on Acoustics, Speech and Signal Processing (1984), S. 10.1/1 - 10.1/4.

/24/ Becker H.J. and Piper F.C.: Secure Speech Communications. Academic Press, (1985).

/25/ Denning D.E.R.: Cryptography and Data Security. Addison-Wesley Publishing Company, (1983).

/26/ Staffelbach O.: Datensicherung bei der Uebermittlung und in Netzen. Elektroniker, Nr. 10/1985, S. 55-61.

/27/ Rueppel R.A.: New Approaches to Stream Ciphers. Diss. ETH No. 7714, (1984).

/28/ Orceyre M.J. and Heller R.M.: An Approach to Secure Voice Communication Based on the Data Encryption Standard. IEEE Communications Magazine, (November 1978), S. 41-50.

/29/ Till R.: Adaptive Sprecherecho-Kompensation in Modems für die Duplex-Datenübertragung im Fernsprechernetz. Frequenz, 37 (1983), S. 145-154.

/30/ Hellen P.A.T.: Military Secure Speech Using HF. Electronics & Power, (März 1985), S. 232-238.

/31/ Van Uffelen J.P. and Deconche A.: Transmission de données série à grand débit sur canal HF. NATO Conference Proceedings No. 363, S. 39/1 - 39/8.