Verschlüsselungsverfahren
im DVB-Standard

eingereicht am: 10. März 2004

Von: Oliver Rausch
Matrikel-Nr.: 108 000 217828

Betreut durch: Dipl.-Ing. Jan Pelzl
Kurzzusammenfassung

Inhaltsverzeichnis

1 Einführung 7
  1.1 Was heißt Digitales Fernsehen? ......................... 7
  1.2 Warum der Umstieg auf Digitales Fernsehen? .......... 8
  1.3 Entwicklung des Digitalen Fernsehens .................. 9
    1.3.1 Europa ........................................ 9
    1.3.2 USA .......................................... 10
    1.3.3 Japan und Korea ................................ 10
  1.4 Wie sieht die „Digitale Fernsehwelt“ in NRW aus? .... 11

2 Technische Aspekte 12
  2.1 Der Datencontainer .................................... 12
  2.2 Das Prinzip der Datenreduktion ......................... 13
  2.3 Der MPEG Standard .................................... 16
  2.4 Der Paketierungs- und Multiplexprozess ................ 18
  2.5 Der Digital-Decoder .................................. 20

3 Die Verschlüsselung im DVB-Standard 21
  3.1 Conditional Access .................................... 21
  3.2 Common Scrambling Algorithmus ......................... 23
Abbildungsverzeichnis

<table>
<thead>
<tr>
<th></th>
<th>Organisationsschema des Europäischen DVB-Projektes (nach [Reimers95])</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Mögliches Szenario für die Nutzung von DTVB (nach [Reimers95])</td>
<td>12</td>
</tr>
<tr>
<td>3</td>
<td>Hierarchie des MPEG-Datenformats (nach [Zoidl99])</td>
<td>18</td>
</tr>
<tr>
<td>4</td>
<td>Signalverarbeitung vom Aufnahme- zum Sendesignal</td>
<td>19</td>
</tr>
<tr>
<td>5</td>
<td>Aufbau eines Transportstrom-Paketes (nach [Mäusl03])</td>
<td>20</td>
</tr>
<tr>
<td>6</td>
<td>Das CA-System (nach [Reimers95])</td>
<td>22</td>
</tr>
<tr>
<td>7</td>
<td>Das Scramblingverfahren des CSA (nach [Reimers95])</td>
<td>23</td>
</tr>
</tbody>
</table>
Abkürzungsverzeichnis

**A/D**: Analog/Digital

**B-Picture**: Bidirektional vorhergesagtes Bild

**CA**: Conditional Access

**CAT**: Conditional Access Table

**CEC**: Commission of the European Communities

**CI**: Common Interface

**CSA**: Common Scrambling Algorithmus

**DTVB**: Digital TeleVision Broadcasting

**DVB**: Digital Video Broadcasting

**DVB-C**: Verbreitung digitaler Fernsehdaten via Kabelnetz

**DVB-S**: Ausstrahlung digitaler Fernsehdaten via Satellit

**DVB-T**: Ausstrahlung digitaler Fernsehdaten auf dem terrestrischen Wege

**EBU**: European Broadcasting Union

**ECM**: Entitlement Control Message

**EMM**: Entitlement Management Message

**EPG**: Electronic Program Guide

**ETS**: European Telecommunications Standard

**HDTV**: High Definition TeleVision

**GOP**: Group of Pictures

**I-Picture**: Intracodiertes Bild

**IEC**: International Electrotechnical Commission
IRD: Integrated Receiver Decoder

ISO: International Standards Organization

JPEG: Joint Photographic Experts Group

MPEG: Moving Pictures Expert Group

P-Picture: Einseitig vorhergesagtes Bild (Predicted Picture)

PAL: Phase Alternation Line

PAT: Program Association Table

PC: Personal Computer

PES: Paketisierter Elementarstrom

PID: Packet Identification

PMT: Program Map Table

PRNG: Pseudo Random Number Generator

QEF: Quasi Error Free

SCR: System Clock Reference

SMATV: Satellite Master Antenna TeleVision
1 Einführung

Der Begriff *Digitales Fernsehen* ist heutzutage in aller Munde. Gab es vor wenigen Jahren nur ein paar Pay TV Anbieter\(^1\), die die digitale Technik nutzten und für hohe monatliche Gebühren ein beschränktes Angebot bereitstellten, so existiert heute ein großes und wesentlich kostengünstigeres Angebot an Sendern. Auch die öffentlich-rechtlichen Sender können digital empfangen werden.

1.1 Was heißt Digitales Fernsehen?


Das bedeutet, dass die digitalen Datensignale (oder auch Datenpakete) durchaus auf analogem Wege zum Zuschauer gelangen können. Dies ist nötig, um die Signale in einen bestimmten Übertragungskanal einzupassen, d.h. die Datensignale werden zeitkontinuierlichen Trägerfrequenzen aufmoduliert. Durch die analoge Übertragungstechnik ist es daher auch kein Problem, sämtliche herkömmlichen Übertragungswege zu nutzen. Je nachdem, welcher Weg genutzt wird, spricht man von

- der Ausstrahlung via Satellit (*DVB-S*)
- der Einspeisung in das Kabelnetz (*DVB-C*) und von
- der Ausstrahlung auf dem terrestrischen Wege mit dem Empfang über die Hausantenne (*DVB-T*).

Im Vergleich zum herkömmlichen analogen Verfahren benötigt das Digitale Fernsehen eine deutlich geringere Übertragungskapazität und durch die Verwendung von Glasfasertechnik kann die Verbreitung von Daten über das Telefonnetz ermöglicht werden.

\(^1\)Premiere und DF 1, aus deren Fusion das heutige Premiere World entstanden ist
Theoretisch wäre es sogar möglich, ein Programm von der letzten Vermittlungsstelle zum Zuschauer über einfache Kupferleitungen zu übertragen.

1.2 Warum der Umstieg auf Digitales Fernsehen?

Außer der schon in 1.1 genannten neuen Übertragungswege gibt es noch andere Vorteile, die es rechtfertigten, trotz zahlreicher, sich bewährter Fernsehstandards, einen neuen zu entwickeln, der aufgrund des benötigten Digitalreceivers (Set-Top-Box\(^2\) oder IRD\(^3\)) noch mit Zusatzkosten für den Endkunden verbunden ist.

- Es gelingt die Übertragung von Fernsehbildern in verbesserter, d.h. verlustfreier Qualität (Zielsetzung: HDTV\(^4\)).

- Es können bis zu zehn Programme mehr auf einem Kanal übertragen werden bzw. man könnte die wenigen (analogen) breitbandigen Kanäle durch viele (digitale) schmalbandige ersetzen. Vorteilhaft dabei ist, dass der Zuschauer über eine größere Programmvielfalt verfügen kann und neue Anbieter durch höhere Kanal-Ressourcen nachrücksen können.

- Selbst mit kleinen portablen Fernsehempfängern können Bilder in guter Qualität empfangen werden. Mobilfunkgeräte der nächsten Generation sollen dies schon ermöglichen.

- Pay Per View wird ermöglicht, d.h. der Zuschauer bezahlt nur das, was er sich ansieht und zwar zu einem selbstgewählten Zeitpunkt (Video On Demand).

\(^2\)Der Name rührt daher, dass das Gerät meist auf dem Fernsehgerät steht.

\(^3\)Integrated Receiver Decoder

\(^4\)High Definition TeleVision
1.3 Entwicklung des Digitalen Fernsehens

1.3.1 Europa


Abbildung 1: Organisationsschema des Europäischen DVB-Projektes (nach [Reimers95])

Die Arbeitsgruppe „Moving Pictures Expert Group (MPEG)“\(^5\) entstand aus Mitgliedern

\(^5\) Commission of the European Communities (CEC)
\(^6\) European Broadcasting Union (UER/EBU)
der ISO-7 und IEC-8 Organisationen und hatte schon mit der Entwicklung von Standards und Verfahren für die Video- und Audiocodierung begonnen. Daher entschloss sich das Europäische DVB Projekt, diese Standards zu übernehmen, um eine international nutzbare Technik zu schaffen. Man wollte nicht noch weitere Alternativstandards entwickeln, was dem kommerziellen als auch dem Ziel der möglichst raschen Verbreitung der DVB-Technologie widersprochen hätte.

Im November 1994 wurde der European Telecommunications Standard ETS 300 421 verabschiedet. Dieser spezifiziert die Richtlinien für die Satellitenausstrahlung (DVB-S). Schon kurz darauf folgte der ETS 300 429 für DVB-C.

1.3.2 USA


1996 beschloss die Regierung, dass bis 2006 das digitale Fernsehen das analoge vollständig ablösen soll, allerdings besaßen im Jahre 2002 nur 1% der Haushalte ein digitales Empfangsgerät, was darauf hinweist, dass sich die Umstellung verzögern wird.

1.3.3 Japan und Korea

Der asiatische Raum wartete erst einmal die weltweiten Entwicklungen ab. Durch die zahlreiche Tochterunternehmen, die Mitglieder im Europäischen DVB Projekt waren,

---

7 International Standards Organization  
8 International Electrotechnical Commission  
9 Die Grundstruktur eines Fernsehprogramms ist in den USA anders. Ein regionaler Sender kauft von einem überregionalen Anbieter ein Rahmenprogramm und vergibt seine Werbeblöcke selbst. Das bedeutet, dass die Werbekunden ihre Spots nur regional und terrestrisch ausstrahlen lassen.
hatte man jedoch stets die neuesten Entwicklungen im Blick, was letztlich dazu führte, das der japanische und koreanische Standard dem europäischen stark ähneln.

1.4 Wie sieht die „Digitale Fernsehwelt“ in NRW aus?


Im Bereich des Pay TV gibt es neben Premiere World seit November für anfänglich 500000 Haushalte weitere 56 digitale Fernsehkanäle, die vom Kabelnetzbetreiber „ish“ angeboten werden. Bis Ende 2004 sollen alle 4,2 Millionen Haushalte in NRW die Möglichkeit haben, diese Kanäle zu abonnieren [Röse03].

\(^{10}\)Es wird u.a. verlangt, dass selbst mit einfachsten, in Gebäuden montierten Empfangsantennen das volle Programm zur Verfügung steht.
2 Technische Aspekte

Abbildung 2: Mögliches Szenario für die Nutzung von DTVB (nach [Reimers95])

Abbildung 2 verdeutlicht noch einmal die verschiedenen Empfangsmöglichkeiten des digitalen Fernsehens. Wie aus der Zeichnung ersichtlich wird, ist nur das Kabelnetz rückkanalfähig. Wählt der Kunde eine andere Empfangsmöglichkeiten, muss die Set-Top-Box an das Telefonnetz angeschlossen werden, um eine Kommunikation zwischen Kunde und Programmanbieter zu gewährleisten.

Die folgenden Abschnitte beschreiben die Vorgänge von der Weiterverarbeitung des Studiosignals bis hin zur Ausgabe der Videodaten durch den Fernseher. Der Einfachheit halber gehen wir davon aus, dass das „Sendematerial“ entweder digital aufgenommen wird oder mit einem A/D-Wandler digitalisiert wird und digital vorliegt und keine weitere Verschlüsselung der Daten stattfindet.\[1\]

2.1 Der Datencontainer

Der wichtigste Begriff zum Verständnis der digitalen Fernsehtechnik ist der Begriff des Datencontainers. Auf dem Konzept des Datencontainers bauen alle drei DVB-Standards auf.\[1\] Auf die Verschlüsselung im DVB-Standard wird noch einmal speziell in Kap.3 eingegangen.
auf. In einem Datencontainer wird eine maximale Datenmenge pro Zeiteinheit quasi fehlerfrei (Quasi Error Free - QEF) übertragen. Den Datendurchsatz (MBit/s) bezeichnet man als Kapazität des Containers. [Reimers95] Die Art der Daten ist hierbei gleichgültig, wichtig sind allein die Paketierung nach den geltenden Standards sowie Zusatzinformationen, die zur Synchronisierung nötig sind.

Die Kapazität des Datencontainers hängt vom Übertragungsweg ab: Bei der Satellitenausstrahlung und im Kabelnetz liegt er bei 40 MBit/s, bei der terrestrischen Ausstrahlung bei 20 MBit/s.

2.2 Das Prinzip der Datenreduktion

Die oben beschriebene Begrenzung der Datencontainergröße weist die Notwendigkeit der Datenreduktion auf: Ein vollständig digitalisiertes Fernsehbild benötigt eine Datenrate von 216 MBit/s bzw. 166 MBit/s, wenn die Austastlücken „ausgepuffert“ und somit vernachlässigt werden. Es ist also nicht einmal möglich ein Fernsehprogramm in einem Datencontainer zu übertragen, sofern es nicht gelingt, den erforderlichen Datenstrom zu reduzieren. Ähnlich verhält es sich bei dem Audiostream: Ein vollständig digitalisiertes Audiosignal in CD-Qualität benötigt 1,4 MBit/s, eine Menge, die zwar in den Container passen, aber unverhältnismäßig viel Kapazität beanspruchen würde.

Als einfache Beispielrechnung wird hier ein TV-Bild mit 256 Graustufen angenommen. Deutschland verwendet bei der TV-Übertragung das PAL12-Verfahren, welches 576 sichtbare Zeilen mit jeweils 720 Bildpunkten (Pixel) sendet. Pro Sekunde werden 25 Vollbilder oder 50 Halbbilder im Interlace-Modus13 gesendet. Da in diesem Beispiel nur Graustufen übertragen werden, reichen für die Beschreibung eines Pixels mit 8 Bit aus. Es ergibt sich folgende Berechnung der nötigen Datenrate:

\[
\text{576 Zeilen} \times \text{720 Pixel} \div \text{Zeile} \times 25 \text{ Hertz} \times \frac{8}{\text{Pixel}} = 82.944.000 \text{Bit/s} \approx 80 \text{ MBit/s}
\]

Offensichtlich würde die vorgesehene Kapazität eines Datencontainers nicht einmal für ein in Graustufen digitalisiertes Bild ausreichen. Wenn man nun ein Farbsignal haben wollte, bräuchte man zur Beschreibung eines Pixels 24 Bit14, also die dreifache Datenrate.

12 „Phase Alternation Line“, analoges Farbfernsehsystem
13 Zeilensprung, diese Technik wird verwendet, um Flimmern zu vermeiden
14 Jedes Pixel kann in die Farbkomponenten Rot, Grün und Blau unterteilt werden. Diese können wiederum je 256 Intensitäten annehmen, d. h. jedes Pixel besteht aus 8+8+8=24 Bit.
Es muss also ein Verfahren verwendet werden, welches die erforderlichen Datenraten ohne wahrnehmbare Qualitätsverluste in Bild und Ton reduziert. Die Motion Picture Expert Group begann mit der Entwicklung eines Standardverfahrens und stellte im November den MPEG-2 Standard (siehe dazu 2.3) fertig.

Die Datenreduktion wird auf zwei verschiedene Arten erreicht:

**Redundanzreduktion:** Bereits bekannte Informationen werden weggelassen.

**Irrelevanzreduktion:** Es werden Informationen weggelassen, die für das menschliche Auge und Ohr nicht wahrnehmbar sind.


Bei der Irrelevanzreduktion werden die Schwächen des menschlichen audiovisuellen Systems genutzt.

Das Auge besitzt zum Beispiel folgende für die Datenreduktion nützliche Eigenschaften:

- Große, sich lokal nur langsam ändernde Strukturen besitzen eine niedrige Ortsfrequenz, feine Strukturen eine hohe. Der Mensch kann eine Struktur nur bis zu einer bestimmten Ortsfrequenz auflösen, d.h. man braucht Strukturen nur bis zu einem bestimmten Grenzwert zu digitalisieren, da alle weiteren Informationen ohnehin nicht mehr genutzt werden können. Es ist sogar möglich, dass man noch größer auflösen kann, je näher man an diesen Grenzwert kommt, da solche Kodier-Fehler bei hohen Ortsfrequenzen nicht mehr wahrgenommen werden [Zoidl99].

- In der Natur kommen vornehmlich vertikale und horizontale Strukturen vor, welche vom menschlichen Gehirn bevorzugt wahrgenommen werden. Bei der Datenreduktion wird der *Oblique-Effekt* ausgenutzt, eine Schwäche des menschlichen
Gehirns bei Erkennung von diagonalen Strukturen. Durch diese können die diagonalen Strukturen bei der Bilddigitalisierung grüber aufgelöst werden [Zoidl99].

- Der Mensch erkennt Objekte nicht anhand seiner Flächen, sondern anhand seiner Umrandungen. Der Mach-Effekt hebt die Objektkanten stärker als in der Realität hervor. Dadurch kann man die Flächen vernachlässigen, da sie für die Wahrnehmung noch weniger an Wert besitzen. Dies ist allerdings ein signalverfälschender Effekt [Zoidl99]!

- Bei bewegten Bildern darf die Auflösung schlechter sein, als bei stehenden Bildern, das gleiche gilt für stehende und sich bewegende Objekte in einem Bild. Dies erkennt man schnell an einem kleinen Beispiel: Je schneller ein Auto an einem vorbeifährt, desto schwieriger ist es, sich das Kennzeichen zu merken [Zoidl99].

Aber auch durch Eigenschaften des menschlichen Ohres kann die Datenrate reduziert werden, ohne dass Qualitätsverluste wahrgenommen werden können. Die Empfindlichkeit des Ohres hängt von der Frequenz des Tones ab. Am empfindlichsten ist das Ohr im Bereich von 1kHz bis 5kHz, wobei Töne unter 30Hz und über 15kHz kaum noch wahrgenommen werden. Die hier genannten Grenzen gelten nicht für alle Altersklassen, beispielsweise hört der Säugling noch weitaus höherfrequente Töne, jedoch stellen sie allgemeine Richtwerte für Erwachsene dar. Zu dem Frequenzbereich, in dem ein wahrnehmbarer Ton liegen muss, existiert ebenfalls eine Lautstärkeschwelle. Forschungen haben ergeben, dass bei dem menschlichen Ohr sogenannte Maskierungseffekte auftreten (vgl. [Mäusl03]). Bei lauten Tönen einer bestimmten Frequenz werden leisere Töne einer nahen Frequenz maskiert, d.h. der Hörer nimmt diese Töne nicht wahr. Tritt beispielsweise ein 1kHz-Ton mit einer Lautstärke von 80dB auf, kann ein 2kHz-Ton, der leiser als 40dB ist, nicht mehr wahrgenommen werden [Zoidl99].

Je höher die Frequenz des starken Signals, desto breiter ist das maskierte Frequenzband. Maskierungseffekte treten allerdings nicht nur im Frequenz- sondern auch im Zeitbereich auf: Laute, impulsartige Geräusche (z.B. ein Knall) überlören nicht nur leisere Töne kurz nach dem Auftreten, sondern auch kurz davor [Mäusl03, Zoidl99].

Es liegt nahe, Töne die maskiert werden oder die aufgrund ihrer Lautstärke oder ihres Frequenzganges ohnehin nicht wahrnehmbar sind, bei der Digitalisierung herauszufiltern um die Datenrate zu reduzieren.

Wichtig ist, dass bei der Irrelevanzreduktion Informationsverluste und Signalverfälschungen stattfinden, die aber entweder gar nicht oder als nicht störend wahrgenommen werden.
2.3 Der MPEG Standard

Der MPEG Standard ist ein asymmetrisches Kodierverfahren, d.h. die Kodierung ist wesentlich aufwendiger als die Dekodierung. Daher eignet er sich besonders zur Speicherung oder Übertragung auf Geräte mit geringeren Leistungs- oder Speicherkapazitäten. Auch wenn ein heutiger PC ein MPEG 2-Video problemlos und flüssig abspielt, muss erwähnt werden, dass dies vor ein paar Jahren ohne zusätzliche Hardware noch nicht möglich war.

Der MPEG Code sollte prinzipiell alle Möglichkeiten der Digitalisierung bieten und erst durch Reduktion von unnötigen Daten und Parametern auf bestimmte Medien spezialisiert werden. Er legt keine Kompressionsalgorithmen fest, sondern lediglich das Dateiformat, das den Datenstrom beschreibt [Zoidl99].

Es soll keine Kompatibilitätsprobleme oder Einschränkungen für den Benutzer geben, daher wurde festgelegt dass trotz unterschiedlichster Komprimierungsverfahren u. a. immer folgende Funktionen zur Verfügung stehen müssen [Zoidl99]:

- schnelles Vor- und Rückschauen
- wahlfreier Zugriff innerhalb des digitalen Videos
- Fehlertoleranz
- Formatflexibilität

Zwei wesentliche Bestandteile von MPEG sind die Bewegungskompensation (Motion oder Moving Compensation) und die Interframe Compression.

Bei der Bewegungskompensation werden Bewegungen von Makroblooken der Größe 16x16 Pixel in Form von Bewegungsvektoren beschrieben. Dies bedeutet, dass die Kodiersoftware natürlich keine Objekte erkennen kann, dennoch erkennt sie Bewegungen (eben dieser Makroblocke, welche z.B. Teile eines fahrenden Autos sein können) und beschreibt deren Richtung. Dabei entstehen selbstverständlich Fehler (prediction errors), da beispielsweise keine genauen Bewegungsvektoren für die Faltenbildung eines Kleidungsstückes vorhergesagt werden können. Diese können aber mit speziellen Verfahren minimiert werden [Zoidl99, Mäusl03].

Die Interframe Compression nutzt die Ähnlichkeit von aufeinanderfolgenden Bildern. MPEG unterteilt in drei verschiedene Bildarten, die in einer Gruppe von Teilbildern
(GOP)\textsuperscript{15} vorkommen können. Eine solche Gruppe kann diese Bildarten in fast beliebiger Reihenfolge und Mengen enthalten. Diese Einschränkungen werden im folgenden noch genannt.

Die verschiedenen Bildtypen sind:

**Intracodierten Bildern (I-Pictures):** Dieses ist ein sogenanntes Schlüsselbild und wird prinzipiell als einfaches JPEG\textsuperscript{16}-Bild komprimiert. Diese Bilder besitzen keine Beziehungen und ermöglichen beispielsweise erst das Vor- und Zurückspulen. Es ist das erste Bild, das der Zuschauer beim Einschalten sieht. Damit er beim Umschalten zwischen den Programmen nicht so lange warten muss, werden im MPEG-Strom gewöhnlich zwei I-Pictures pro Sekunde gesendet, d.h. jedes zwölftes Bild einer GOP ist ein intracodiertes Bild. Da ein solches Bild fast alle Informationen enthält, ist die Kompressionsrate vergleichsweise gering: ca. 1:1,7 [Zoidl99, Mäusl03].

**Einseitig vorhergesagtes Bild (Predicted Picture, P-Picture):** In einem P-Bild ist eine Referenz zu einem vorherigen I- oder P-Bild codiert. Es beschreibt lediglich die Änderungen zu diesen mittels Bewegungsvektoren, referenziert aber auch immer auf die vorherigen Bilder. Kompressionsrate: ca. 1:20 [Zoidl99].

**Bidirektionall vorhergesagtes Bild (B-Picture):** Diese Bilder benötigen Referenzen auf das vorliegende und nachfolgende Bild, allerdings ist hier die Kompressionsrate maximal: ca. 1:50 [Zoidl99].

Zu erwähnen ist, dass die Reihenfolge der im MPEG-Strom gesendeten Bilder nicht unbedingt identisch mit der realen zeitlichen Reihenfolge sein muss. Abbildung 3 veranschaulicht die hierarchische Gliederung eines MPEG-Stromes. Als Farbsystem bietet sich bei der Kompression anstelle des RGB\textsuperscript{17} das YC\textsubscript{r}C\textsubscript{b}-Farbsystem an. Dieses System unterteilt einen Pixel in in drei Komponenten: Die Luminanz (Helligkeit)\textsubscript{Y} und die rote (\textsubscript{Cr}) und blaue (\textsubscript{Cb}) Chrominanz, welche die Lage des Pixels auf dem Farbkreis wiedergeben. Normalerweise bräuchte man für die Beschreibung jeder einzelnen Komponente 8 Bit, was zu keiner Datenersparsnis gegenüber dem RGB-Farbsystem führen würde. Da das menschliche Auge auf Helligkeitsunterschiede jedoch

\textsuperscript{15} Group of Pictures
\textsuperscript{16} Joint Photographic Experts Group, eine Expertengruppe, die ein Verfahren zur Kompression von Einzelbildern entwickelte
\textsuperscript{17} Rot-Grün-Blau oder Red-Green-Blue, ein System, welches 24Bit zur Beschreibung eines Pixels benötigt und in der herkömmlichen Fernsehtechnik benutzt wird
Abbildung 3: Hierarchie des MPEG-Datenformats (nach [Zoidl99])

wesentlich empfindlicher reagiert als auf Farbunterschiede, reicht es, die beiden Chrominanzen mit halber Auflösung zu übertragen [Zoidl99].

Durch die genannten Komprimierungsverfahren kann aus einem 166MBit/s Videosignal (Standard-Studiosignal) ein Signal mit einer mittlere Datenrate von 4,25MBit/s erzeugt werden [Mäusl03].

Als Beispiel kann hier die Sendung „Tagesschau“ dienen: Ein sich kaum bewegender Nachrichtensprecher vor einem sich nur selten verändernden Hintergrund kann zu einer Kompressionsrate von 96% führen.

Der MPEG-Standard definiert außerdem noch den Multiplex von Video-, Audio- und Datenstrom in einem einzigen Datenstrom, wie im folgenden erläutert wird.

2.4 Der Paketierungs- und Multiplexprozess

Am Ende des Komprimierungsprozesses (Encoding) entstehen zwei unpaketierte Elementarströme. Diese werden gemäß des MPEG-Standards paketisiert. Das Ergebnis wird

Der komplette Ablauf vom Aufnahme- zum Sendesignal wird noch einmal in Abbildung 4 veranschaulicht.

Abbildung 4: Signalverarbeitung vom Aufnahme- zum Sendesignal


\(^{18}\)engl. Video Packetized Elementary Stream und Audio Packetized Elementary Stream

\(^{19}\)„Electronic Program Guide“

\(^{20}\)Decoding Time Stamp (DTS)

\(^{21}\)Presentation Time Stamp (PTS)
Ein Transportstrompaket hat eine feste Länge von 188 Byte, von denen 4 Byte für den Header vorgesehen sind (vgl. Abbildung 5).

<table>
<thead>
<tr>
<th>Header 4 Byte</th>
<th>Adaption Field (u.a. Program Clock Reference)</th>
<th>Payload (Nutzlast)</th>
</tr>
</thead>
</table>

Abbildung 5: Aufbau eines Transportstrom-Paketes (nach [Mäusl03])

Der Header besteht u.a. aus einem für die Synchronisation wichtigen SYNC-Byte22, welches den Paketanfang anzeigt, und der Packet Identification (PID). Über diese werden die Daten den jeweiligen Programmen und Signalen zugeordnet. Pakete mit der PID 0 sind für die Program Association Table (PAT) vorgesehen, welche die Zusammensetzung des Programm-Multiplexes und die PIDs für die Program Map Tables (PMT) der einzelnen Programme enthält. Die PMTs wiederum beinhalten die Liste der zu ihrem Programm gehörenden PIDs. Ist auch nur ein Programm aus dem Bouquet verschlüsselt, wird eine Conditional Access Table (CAT) gebildet, welche die Art der Verschlüsselung und die Berechtigungsbedingungen beschreibt. Für die CAT ist die PID 01 vorgesehen [Mäusl03].

### 2.5 Der Digital-Decoder

Der Decoder empfängt den Sende-MPEG-2-Transportstrom, er muss sich aber noch vermittels der SYNC-Bytes mit der Senderseite synchronisieren. Danach werden alle Pakete mit der PID 0 herausgefiltert um die PAT aufzubauen. Ist dies geschehen, kann der Zuschauer das gewünschte Programm auswählen. Über die passende PMT werden die richtigen Pakete herausgefiltert, sowie der System Clock synchronisiert.

Danach startet die Video- und Audiodekodierung und die Umwandlung des YC/Ch- in das RGB-Signal. Es erfolgt die Ausgabe am Fernsehgerät. Der Synchronisierungsprozess beansprucht eine gewisse Zeit, außerdem muss erst auf ein I-Bild (siehe 2.3) gewartet werden, bis die Bildinformationen wiedergegeben werden können. Daher dauert das Umschalten zwischen den Programmen beim digitalen Fernsehen länger als beim analogen.

22Das SYNC-Byte hat die fest definierte Bitfolge 01000111 (hex 47).
3 Die Verschlüsselung im DVB-Standard

Digitales Fernsehen weist für Pay TV Anbieter wesentliche Vorteile gegenüber dem analogen Fernsehen auf. Bei der analogen Technik werden vor der Übertragung des Fernsehbildes lediglich die Bildzeilen vertauscht, die Audiosignale bleiben unverschlüsselt. Der analoge Decoder prüft dann anhand der Smartcard, die Pay TV Abonnenten bekommen, ob der Benutzer das jeweilige Programm sehen darf. Ist er berechtigt, werden die Bildzeilen wieder an der richtigen Stelle wiedergegeben. Diese Verschlüsselungsmethode ist sehr unsicher, da un autorisierte Nutzer die Programme zumindest hören können, was bei Sportereignissen, wie z. B. Bundesliga-Spieltagen, vielen reicht. Zudem sind PCs mittlerweile so schnell, dass sie durch Vergleich der Farbverläufe der einzelnen Zeilen diese oftmals richtig anordnen können. Bei Fußball- oder Tennisspielen gelingt das aufgrund der sehr ähnlichen Bildzeilen zwar nicht so gut, Spielfilme sind allerdings sehr leicht zu entschlüsseln. Im Folgenden wird nun die digitale Version des Pay TV beschrieben.

3.1 Conditional Access

Das Conditional Access (CA)- System\textsuperscript{23} ist für die Unterteilung der Benutzer in mehrere Gruppen mit unterschiedlichen Berechtigungen verantwortlich. Häufig abonniert der Kunde nicht ein Programm, sondern ein ganzes Programmpaket, beispielsweise ein Sport- oder ein Spielfilm-Paket. Damit ein Kunde wirklich nur die Sendung sehen kann, für die er auch bezahlt hat, wurde ein CA-System entwickelt, dessen Aufbau man in Abbildung 6 sehen kann.


\textsuperscript{23}Conditional Access $\equiv$ bedingter Zugriff

\textsuperscript{24}Kontrollwörter $\equiv$ Control Words
Auf der Empfängerseite werden die den Kunden betreffenden EMMs auf einer Smartcard abgespeichert. Zusammen mit dem auf dieser Karte gespeicherten Kundenschlüssel können die empfangenen ECMs entschlüsselt werden, sofern der Benutzer dazu autorisiert ist. Die Kontrollwörter aus der ECM ermöglichen es nun, die verschlüsselten Programm­pakete zu entschlüsseln (descrambling) und über den Fernseher wiederzugeben.

Der Vorteil bei der Verschlüsselung des digitalen Fernsehens besteht darin, dass man jede Art von Daten verschlüsseln kann. Ein nicht-autorisierter Nutzer kann also weder Bild noch Ton wahrnehmen.


Abbildung 6: Das CA-System (nach [Reimers95])
3.2 Common Scrambling Algorithmus

Der Common Scrambling Algorithmus wurde von dem Europäischen DVB-Projekt entwickelt, um eine große Kompatibilität zwischen verschiedenen Digital-Decodern zu gewährleisten. Dadurch, dass alle Pay TV Anbieter denselben Algorithmus zur Verschlüsselung ihres Programm-Bouquets nutzen, wird es dem Kunden ermöglicht, den Anbieter zu wechseln, ohne sich eine neue Set-Top-Box kaufen zu müssen.


Nachdem aber im Jahr 2000 Patentschriften über den CSA verbreitet wurden, erschien kurz darauf die Software FreeDec, welche den gesamten CSA beinhaltete. Kurz darauf geschah das, was die Entwickler durch die oben genannte Bedingung haben verhindern wollen: Die Software wurde disassembled und der CSA analysiert.

Das Prinzip des CSA wird in Abbildung 7 veranschaulicht. Die einzelnen Transportstrom-

Die Kontrollwörter werden vom Anbieter dreimal pro Sekunde gesendet, damit das Umschalten zwischen den Programmen nicht unnötig verzögert wird. Alle zehn Sekunden werden die Control Words gewechselt, daher gab es bisher noch keine erfolgreichen Angriffe auf den CSA. Die bisherigen Möglichkeiten, unautorisiert Pay TV zu empfangen, basierten alle auf Fehlern in der anbieterspezifischen Verwaltung der EMMs und ECMs, d. h. man manipulierte die Smart Card so, dass man die Gruppenzugehörigkeit verändern konnte\textsuperscript{26}.

\textsuperscript{25}Pseudo Random Number Generator (PRNG)

\textsuperscript{26}Beispiel Premiere World: Die Gruppe „Händler“ durfte alle Programme entschlüsseln, sogar sämtliche Startzeiten des Video On Demand-Systems
Literatur


