EUROPEAN TELECOMMUNICATION STANDARD

ETS 300 174

November 1992

Source: ETSI TC-NA

Reference: DE/NA-0001*

ICS: 33.080

Key words: Coding, TV

Network Aspects (NA); Digital coding of component television signals for contribution quality applications in the range 34 - 45 Mbit/s

ETSI

European Telecommunications Standards Institute

ETSI Secretariat

Postal address: F-06921 Sophia Antipolis CEDEX - FRANCE
Office address: 650 Route des Lucioles - Sophia Antipolis - Valbonne - FRANCE
X.400: c=fr, a=atlas, p=etsi, s=secretariat - **Internet:** secretariat@etsi.fr

Tel.: +33 92 94 42 00 - Fax: +33 93 65 47 16

Copyright Notification: No part may be reproduced except as authorized by written permission. The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 1992. All rights reserved.

New presentation - see History box

Whilst every care has been taken in the preparation and publication of this document, errors in content, typographical or otherwise, may occur. If you have comments concerning its accuracy, please write to "ETSI Editing and Committee Support Dept." at the address shown on the title page.

Contents

Foreword

This European Telecommunication Standard (ETS) has been prepared by the Network Aspects (NA) Technical Committee of the European Telecommunications Standards Institute (ETSI).

The draft was agreed by a coding experts group including personnel from the European Broadcasting Union (EBU) and approved by the ETSI NA Technical Committee.

The draft was then approved under the ETSI Accelerated approval Procedure No. 3 (AP 3). However, due to technical improvements and reasons of compatibility with CCITT "CCIR Joint Study Group" - CMTT/2 work, alterations were submitted for National Voting using ETSI Vote No. 26. The nationally agreed changes are incorporated into this ETS.

The draft constitutes a common standard for the coding and transmission of television signals in the range of 34 - 45 Mbit/s, in the format specified by CCIR Recommendation 601 [1], and is in line with other relevant CCIR and CCITT Recommendations as referenced.

Annexes A, B, C and D are informative.

Blank page

1 Scope

This European Telecommunication Standard (ETS) constitutes a common standard for the coding and transmission of component television signals at bit-rates in the range of 34 - 45 Mbit/s in the format specified by CCIR Recommendation 601 [1]. The standard embraces the coding algorithm needed for digital picture coding at about 34 and 45 Mbit/s, and their interfaces with the transmission network. The video coding algorithms are based on a hybrid predictive/transform scheme incorporating arrangements for Variable word-Length Coding (VLC), synchronisation and video framing. Provision is made for the transmission of audio and teletext services to accompany the video and for the application of scrambling for conditional access.

Network adaptation is specified to both plesiochronous and synchronous digital hierarchies.

2 Normative references

This ETS incorporates, by dated or undated reference, provisions from other publications. These normative references are cited at the appropriate places in the text and the publications are listed hereafter. For dated references subsequent amendments to, or revisions of any of these publications apply to this ETS only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies.

[1] CCIR Recommendation 601: "Encoding Parameters of Digital Television for Studios".

[2] CCITT Recommendation G.751 (1988): "Digital multiplex equipments operating at the third order bit rate of 34 368 kbit/s and the fourth order bit rate of 139 264 kbit/s and using positive justification".

[3] CCITT Recommendation G.752 (1988): "Characteristics of digital multiplex equipments based on a second order bit rate of 6312 kbit/s and using positive justification".

[4] CCITT Recommendation G.707 (1988): "Synchronous digital hierarchy bit rates".

[5] CCITT Recommendation G.708 (1988): "Network node interface for the synchronous digital hierarchy".

[6] CCITT Recommendation G.709 (1988): "Synchronous multiplexing structure".

[7] CCITT Recommendation H.261 (1988): "Codec for audiovisual services at n x 384 kbit/s".

[8] CCIR Report 624: "Characteristics of television signals".

[9] EBU Tech. 3250 (1985): "Specification of the digital audio interface" (also exists as draft AES Recommendation AES 18 - 19xx).

[10] CCIR Recommendation 724: "Transmission of digital studio quality sound signals over H1 channels".

[11] ISO Standard 3309-2 (1984): "Information processing systems -- Data communication -- High-level data link control procedures -- Frame structure".

[12] CCIR Recommendation 653: "Teletext systems".

[13] EBU Technical Document 3217 (3rd edition, reissued 1986): "Specification of insertion data signal equipment for international transmissions".

[14] CCIR Recommendation 656: "Interfaces for digital component video signals in 525-line and 625-line television systems".

[15] IEC Publication 461 (1986): "Timecode and control code for video tape recorders".

[16] CCITT Recommendation V.24 (1988): "List of definitions for interchange circuits between data terminal equipment (DTE) and data circuit-terminating equipment (DCE)".

[17] CCITT Recommendation V.28 (1988): "Electrical characteristics for unbalanced double-current interchange circuits".

[18] ISO Standard 2110 (1980): "Data communication - 25-pin DTE/DCE interface connector and pin assignments".

[19] CCIR Report 1206: "Methods for picture quality assessments in relation to impairments from digital coding of television signals".

[20] BBC Research Department Report BBC RD 1986/2; Clarke, C.K.P. (1986): "Colour encoding and decoding techniques for line-locked sampled PAL and NTSC television signals".

[21] EBU Technical Statement D29-1980 (1980): "Line identification of the D_R/D_B sequence of SECAM signals".

3 Definitions, symbols and abbreviations

For the purposes of this ETS, the following definitions, symbols and abbreviations apply.

3.1 Arithmetic operators

+	Addition
-	Subtraction or negation
*	Multiplication
/	Integer division
Σ	Summation
LCM	Lowest Common Multiple
XOR	Exclusive OR binary operation (modulo-2 addition)

3.2 Relational operators

=	Equal
≠	Not equal
>	Greater than
<	Less than
≥	Greater than or equal to
≤	Less than or equal to

3.3 General abbreviations and usage

binary	A number system with base 2
hexadecimal	A number system with base 16. In written form, equivalents of the decimal numbers 10 to 15 are replaced by the letters A to F
XY hex	Values expressed in hexadecimal notation
bit	A contraction of the words "binary digit"
word	A group or sequence of bits treated together
octet	A sequence of 8 bits operated on as a data group or word
MSB	Most Significant Bit of a word or octet of bits
LSB	Least Significant Bit of a word or octet of bits
Y	Luminance signal or sample
R	Red chrominance signal
B	Blue chrominance signal
C_R	Scaled colour difference signal or sample Y-R
C_B	Scaled colour difference signal or sample Y-B
PLL	Phase Locked Loop
FEC	Forward Error Correction
ATM	Asynchronous Transfer Mode
SDH	Synchronous Digital Hierarchy
PDH	Plesiochronous Digital Hierarchy
PAL	Acronym for Phase Alternate Line - a composite analogue colour transmission system
SECAM	Acronym for Sequential Colour with Memory - a composite analogue colour transmission system
NTSC	Acronym for the National Television System Committee which developed the composite analogue colour transmission system that is used in the majority of countries using 525-line, 60 Hz scanning parameters
MAC	Acronym for Multiplexed Analogue Components. An analogue component colour transmission system. Usually prefixed with letters and/or numbers denoting the variant
FSW	Frame Synchronisation Word
VLC	Variable Length (word) Coding
CIW	Container Identification Word
CW	Control Word

ECM	Entitlement Control Message
ECW	Even Control Word
EMM	Entitlement Management Message
PRG	Pseudo-Random (sequence) Generator
IW	Initialisation Word loaded into pseudo-random sequence generators for descrambling
OCW	Odd Control Word
PPI	Phase Parity Identifier indicating which CW must be used for descrambling

Other abbreviations and specialised terminology is noted where it occurs in the document.

4 Summary specification of component tv codecs for 34 - 45 Mbit/s

Table 1

VIDEO INPUT/OUTPUT	Standard	525-line or 625-line digital video in component form. Manual or automatic selection of the video standard is at the manufacturer's discretion (see NOTE 1).
	Coding	4:2:2 level of CCIR Recommendation 601 [1].
	Interfaces	Bit-serial (10-bit, 270 Mbit/s serial interface). CCIR Recommendation 656 [14] bit-parallel interfaces shall also be provided.
SIGNAL PREPROCESS-ING	Horizontal	Full digital active line of 720 samples for luminance (Y) and 360 samples for each colour-difference (CR, CB).
	Vertical	525 line : 248 lines per field (see NOTE 2). Field 1 : lines 16 to 263 Field 2 : lines 278 to 525 625 line : 288 lines per field Field 1 : lines 23 to 310 Field 2 : lines 336 to 623
	Numerical represen-tation	Digital input samples of Y, CR and CB conform to the CCIR Recommendation 601 [1] numerical range. These samples are converted to an 8-bit 2's complement representation for the purpose of processing within the codec.
CODING	Modes	Three modes (intra-field, inter-field and motion compensated inter-frame) are used. The following three processing operations are applied either on 8x8 intra-field blocks (intra-field mode) or on differential blocks obtained by difference between the current 8x8 intra-field block and a reference block taken in the previous field (inter-field mode) or in the field with the same parity in the previous frame (inter-frame mode) (see subclause 5.1).
	DCT	Discrete Cosine Transform applied on rectangular blocks of 8 lines of 8 samples for the three components Y, CR, CB (see subclause 5.2).
	Prediction of the block	For each block processed according to inter—field mode, the reference block is determined with pixels of the previous field without motion compensation. For each block processed according to interframe mode, the reference block is taken from the position of the current block by application of a displacement vector (see subclause 5.3).
	Motion compensation	Motion compensation is applied to "macro-blocks". Each macro-block (two adjacent 8x8 blocks for Y and the two co-positioned CR and CB blocks) is assigned a single displacement vector with half-pel accuracy (see subclause 5.4).
	Quantisation	A different quantisation characteristic is used for each coefficient. Its parameters are adapted to the buffer occupancy, the type of block (luminance/chrominance), and the criticality of the block. The shape of the characteristic is nearly uniform (see Clause 6).
	Variable length coding	VLCs are used to encode the quantised DCT coefficients and motion information (see Clause 7).

(Continued)

Table 1 (concluded)

BUFFER MEMORY CAPACITY	1 572 864 bits.
VIDEO FRAMING	(See Clause 8).
VIDEO DATA ERROR PROTECTION	Reed Solomon (255, 239) interleaving factor 6 (see subclause 8.2).
SERVICE MULTIPLEX	(See Clause 10). This combines: - a video channel; - 2 048 kbit/s (or 1 544 kbit/s) audio channel(s) (NOTE 3); - 384 kbit/s teletext channel(s) (see subclause 9.3); - 128 kbit/s test-line channel (see subclause 9.4); - 8 kbit/s supervision channel (see subclause 9.2); - two 8 kbit/s conditional access channels; - two 8 kbit/s time code channels (see subclause 9.5).
NETWORK ADAPTATION	Adaptation to CCITT Recommendations G.751 [2], G.752 [3] and to SDH CCITT Recommendations G.707 [4], G.708 [5], G.709 [6] (see Clause 11 and informative Annex D).
SCRAMBLING FOR CONDITIONAL ACCESS	(See Clause 12 and informative Annex C).
NOTE 1: This codec can accommodate the transmission of PAL/SECAM/NTSC by optional decoders and encoders (see informative Annex B). NOTE 2: Only 244 lines per field are significant; lines 16, 17, 18, 19 and 278, 279, 280, 281 are encoded but not displayed. NOTE 3: Neither the coding nor the error protection of the audio channels is covered by this specification.	

5 Video coding and DCT transformation

5.1 Coding modes

Two processing modes are used, intra-field mode, and inter-field and inter-frame mode.

5.1.1 Intra-field mode

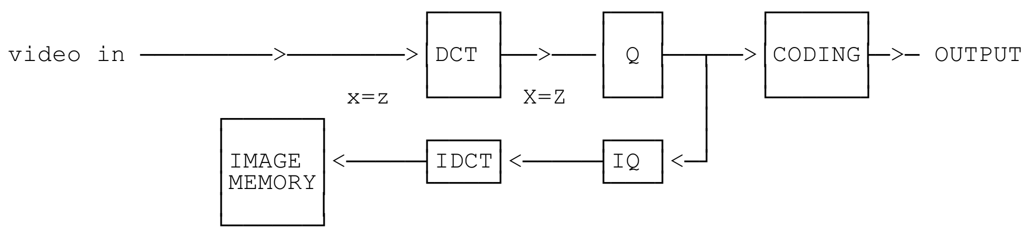


Figure 1: Intra-field mode

5.1.2 Inter-field and inter-frame mode

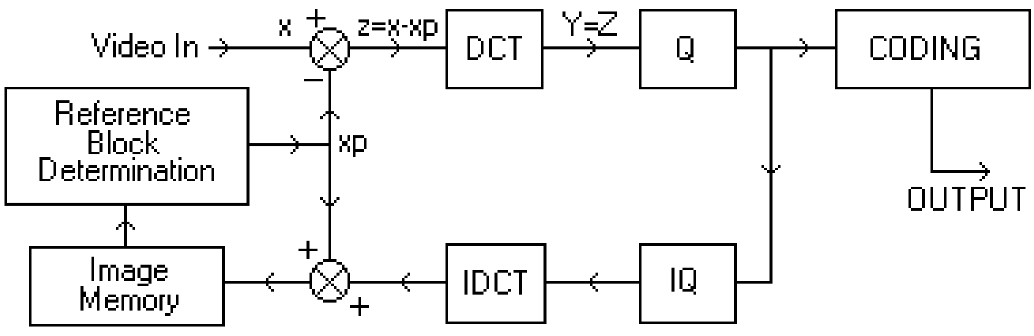


Figure 2: Inter-field and inter-frame mode

5.1.3 Definition of the different modules

DCT Discrete Cosine Transformation (for 8x8 blocks).

IDCT Inverse DCT (for 8x8 blocks).

Q Quantisation (see Clause 6).

IQ The IQ module builds a DCT-coefficients block from the corresponding transmitted information, by assigning to the coefficients the reconstruction values corresponding to the transmitted quantisation levels (see Clause 6).

Coding (See Clause 7).

Image Memory Provides storage for:

- the decoded current field. This field is used as reference for coding the next image;

- the two last previously decoded fields, which are used to determine the current reference block.

For the inter-field mode

The reference block is computed with pixels of the previous field according to the interpolation process described in subclause 5.3.

For the inter-frame mode

The reference block is taken in the field of the previous frame with the same parity as the current field. Its position is obtained from the position of the current block by a translation given by a motion vector. The specification of the motion vector is given in subclause 5.4, the exact computation of the reference block for the inter-frame mode is presented in subclause 5.3.

5.1.4 Notation

x(i,j)		8x8 pixels block.
xp(i,j)		8x8 reference block.
z(i,j)	=	x(i,j) for the intra-field mode.
	=	x(i,j) - xp(i,j) for the inter-frame or inter-field mode.
X(k,l)		The 8x8 DCT coefficients block in intra-field mode.
Y(k,l)		The 8x8 DCT coefficients block in inter-frame or inter-field mode.
Z(k,l)	=	X(k,l) for intra-field mode.
	=	Y(k,l) for inter-frame or inter-field mode.
(i,j)		Coordinates in the image domain:
		i is the line index (range: 0 to 7 from left to right);
		j is the column index (range: 0 to 7 from top to bottom).
(k,l)		Coordinates in the transform domain:
		k is the line index (range: 0 to 7);
		l is the column index (range: 0 to 7).

5.1.5 Mode choice

The chosen mode (intra-field, inter-field or inter-frame) is coded and transmitted for each processed macro-block (see subclause 8.1). No specification is given for the mode choice as it concerns only the coder side.

The inter-field and the inter-frame scheme presented in figure 2 allows the use of a priori choice (decision done before coding steps) or a posteriori choice (decision done after having coded the blocks according to both modes).

In the inter modes, the z(i,j) elements must be in the range (-128, 127); the mode decision is forced, when necessary, in order to satisfy this constraint.

To avoid the temporal propagation of transmission error effects it is recommended to use an intra-field refreshing processing. This processing concerns only the coder and is not specified.

5.2 Discrete cosine transform

For each component (Y, C_R, C_B), the discrete cosine transformation is applied to blocks composed of eight lines of eight samples. The data to be processed are, for each block, the samples of the present field, or the differences between the present field samples and those obtained from a reference block (see subclause 5.3). The direct transformation is computed according to the formula:

$$Z(k,l)=\frac{1}{4}C_k C_l \sum_{i=0}^{7} \sum_{j=0}^{7} z(i,j)\cos\frac{\pi(2i+1)k}{16}\cos\frac{\pi(2j+1)l}{16}$$

and the inverse transformation is given by:

$$Z(i,j)=\frac{1}{4}C_k C_l \sum_{k=0}^{7} \sum_{l=0}^{7} z(k,l)\cos\frac{\pi(2i+1)k}{16}\cos\frac{\pi(2j+1)l}{16}$$

with the terms as defined in subclause 5.1:

$$C_k = \frac{1}{\sqrt{2}} \text{ for } k = 0 \qquad C_l = \frac{1}{\sqrt{2}} \text{ for } l = 0$$

$$= 1 \text{ elsewhere} \qquad = 1 \text{ elsewhere}$$

Z(0,0) is called the DC coefficient: the other coefficients are AC coefficients.

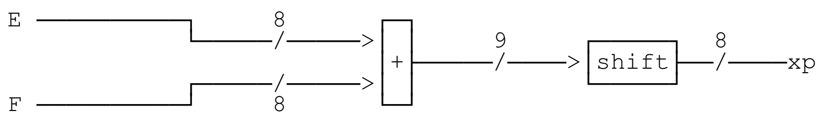
The input to the DCT is expressed as 2's complement integers of 8 bits (including sign). The output of the DCT is expressed as 12-bit 2's complement numbers, of which the integer part is 11 bits (including sign).

The accuracy of the performance of the inverse DCT computation is in accordance with that specified in CCITT Recommendation H.261 [7].

5.3 Prediction of the block

5.3.1 Inter-field mode

The reference block xp for the current block x in field N is computed with pixels of field N-1 with the following interpolation scheme:



E and F are defined below.

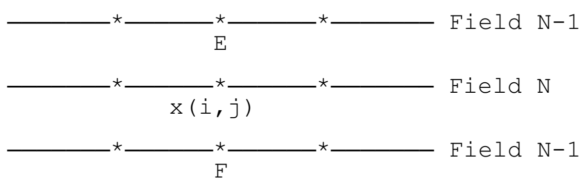


Figure 3

5.3.2 Inter-frame mode

The position of the reference block is obtained from the position of the currently processed block by a translation. For motion compensation, the translation vector (x,y) is as described in subclause 5.4.

There is no ambiguity in the definition of the reference block when the coordinates (x,y) are integer. If one of the coordinates has a non-zero fractional part, an interpolation scheme has to be used to build the reference block.

This scheme is described below for ½ pel accuracy for luminance and ¼ pel accuracy for colour difference:

A+	U.	P.	X.	+B
Q.	V.	R.	Y.	S.
C+	W.	T.	Z.	+D

A, B, C, D: reconstituted pixels of the previous frame (in the field of the same parity). Integer coordinates.

P, Q, R, S, T, U, V, W, X, Y, Z: interpolated pixels of the previous frame (in the field of the same parity).

The values assigned to interpolated pixels are:

P = [(A+B)/2]
Q = [(A+C)/2]
R = [(A+B+C+D)/4]
U = [(3A+B)/4]
V = [(3A+B+3C+D)/8]

as illustrated in figure 4.

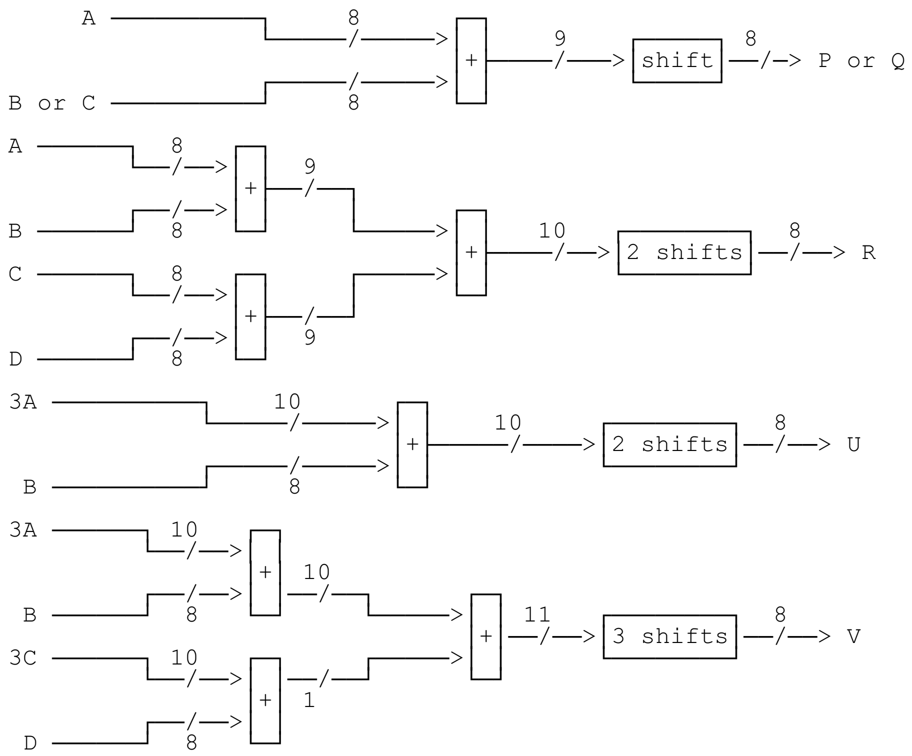


Figure 4

5.3.3 Video level outside active picture

In the definition of the reference block given in subclauses 5.3.1 and 5.3.2, the pixels outside the active picture must be set to zero, expressed in 2's complement (8 bits).

```
    0  0  0  0
 0 ┌──────────┐ 0
   │    Y     │
 0 │CB and CR │ 0
   └──────────┘
    0  0  0  0
```

Figure 5

5.4 Motion compensation

Only one motion vector is used for the blocks belonging to a macro-block. The parameters of the motion compensation are given in table 2.

Table 2

Search areas	± 14 pels and ± 7 lines
Resolution	½ pel and ½ line
Number of possible vectors	1653 (all vectors within the search area are permitted)

The method of estimation is not specified since it concerns only the coder side.

The motion vector points to the pixel in the previous frame that is used in the interframe prediction.

If the vector components are defined as:

- x increasing from left to right, from -14 to +14;
- y increasing from top to bottom, from -7 to +7;

the x component of the vector is expressed as a 6-bit 2's complement number, the integer part of which is 5 bits (including sign). The y component is expressed as a 5-bit 2's complement number, the integer part of which is 4 bits (including sign). It is coded by differential variable-length coding as described in Clause 7.

The motion vector to apply to the C_R, C_B blocks is derived from the macro-block luminance motion vector in the following way:

- the vertical coordinate is identical to that of the luminance vector;
- the horizontal coordinate is equal to half that of the luminance vector.

Chrominance samples at quarter-pixel points are obtained by interpolation as is described in subclause 5.3.

6 Quantisation of DCT coefficients

Subclauses 6.1 and 6.2 give information on the computation of parameters necessary for the operation of the inverse quantiser which is specified in subclause 6.3.

The quantiser parameters signalled to the decoder are the transmission factor and the criticality. The transmission factor is related to the buffer occupancy and it is provided at stripe level, i.e. for all the macro-blocks belonging to each group of 8 video lines.

The criticality is provided at macro-block level and allows a different quantisation precision for blocks belonging to a single stripe. The criteria for criticality selection concern only the coder side and are not specified.

6.1 AC coefficient quantisation

A different quantisation characteristic is used for each coefficient. The quantisation is achieved in two steps.

6.1.1 Computation of relative coefficients

C(k,l) = 2Z(k,l)/[S(k,l,m,f)]

where:

a) S(k,l,m,f) is the transmission threshold for (k,l) coefficients and is of the form:

S(k,l,m,f) = $2^{n(k,l,m,f)/16}$ where n(k,l,m,f) is an integer;

b) m = 0,1,2,3 according to the block criticality (criticality factor);

c) f is the transmission factor.

6.1.2 Quantisation of relative coefficients

6.1.2.1 Quantisation characteristic

Table 3 defines the quantisation levels for the nearly-linear law for luminance and chrominance information. The quantisation law is symmetric, and the characteristic is given for positive input values only.

Table 3: Nearly-linear quantiser characteristic

Input values or intervals C(k,l)	Quantiser levels	Quantised values C'(k,l)*
0	0	0
1	1	1
2	2	2
:	:	:
255	255	255
256:257	256	256
258:259	257	:
:	:	:
510:511	383	510
512:515	384	513
516:519	385	:
:	:	:
1020:1023	511	1021
1024:1031	512	1027
1032:1039	513	:
:	:	:
2040:2047	639	2043

* Outputs of the inverse quantiser

6.1.2.2 Determination of transmission threshold matrix

The S matrix for each component depends on the relative visibility matrix defined in figures 6 and 7 for both components and buffer factor f which is sent before each stripe of the DCT blocks and the criticality factor m which is sent for each macro-block.

The value of f is computed according to the buffer occupancy in order to provide a mean rate not greater than the bit-rate available for video in the transmission multiplex. Different values of f may be transmitted for luminance and chrominance components of a stripe, as shown in figure 9.

The value of m is coded with two bits per macro-block.

The modules which realise the computation of f and the choice of the value for m are only in the coder and the corresponding information is sent to the decoder.

Referring to figures 8, 9 and 10, the scalar control parameter n(k,l,m,f) for each component is obtained in the following way:

$p(k,l,m) = \mathrm{Min}\,[p_0(k,l)+Tr(m),Th(m)]$

where $p_0(k,l)$ is defined in figures 6 and 7 and where p is an integer between 0 and 52.

Tr(m) and Th(m) are parameters depending on criticality (m) and are defined in table 4.

Table 4

Criticality (m)	Translation Tr(m) [Y or C_R C_B coefficients]	Limit for Y Th(m)	Limit for C_R C_B Th(m)
0	+8	no (i.e. 44 + 8)	no (i.e. 26 + 8)
1	+2	no (i.e. 44 + 2)	no (i.e. 26 + 2)
2	0	34	16
3	0	24	9

Then n(k,l,m,f) is given by:

$$n(k,l,m,f)=\mathrm{Min}[n'(k,l,m,f),175]$$

where
$$q(k,l,m,f) = \mathrm{Min}[2p(k,l,m)-48,f] + f$$
$$n'(k,l,m,f) = \mathrm{Max}[q(k,l,m,f),0]$$

6.1.2.3 Data accuracy

Table 5

Data	Total (including sign bit)
AC - DCT coefficients Z(k,l)	12 bits
Relative coefficients C(k,l)	12 bits
Quantised coefficients	11 bits

6.1.2.4 Ranges of quantisation parameters

Table 6

Information		Range
Transmission threshold	n(k,l,m,f)	0 to 175
Transmission factor	f	0 to 175
Relative visibility	$p_0(k,l)$	0 to 44

The transmission factors are transmitted for each stripe of blocks and are each coded with 8 bits.

$p_0(k,l)$	0	1	2	3	4	5	6	7
0	0	0	2	8	12	18	22	28
1	0	6	6	10	16	18	22	34
2	0	6	10	14	18	20	24	38
3	2	6	12	16	18	20	26	40
4	6	12	14	16	20	22	28	42
5	10	14	14	18	22	24	30	42
6	14	16	16	18	22	24	34	44
7	14	18	18	20	24	30	38	44

Figure 6: Relative visibility matrix for luminance

$p_0(k,l)$	1	2	3	4	5	6	7	8
0	0	0	3	4	6	8	8	11
1	0	1	2	3	6	8	9	13
2	2	2	3	4	7	9	10	16
3	3	4	5	5	8	10	12	16
4	5	6	6	7	9	11	13	17
5	8	7	9	9	11	14	16	21
6	10	11	11	11	14	16	19	24
7	12	12	12	12	17	18	20	26

Figure 7: Relative visibility matrix for chrominance

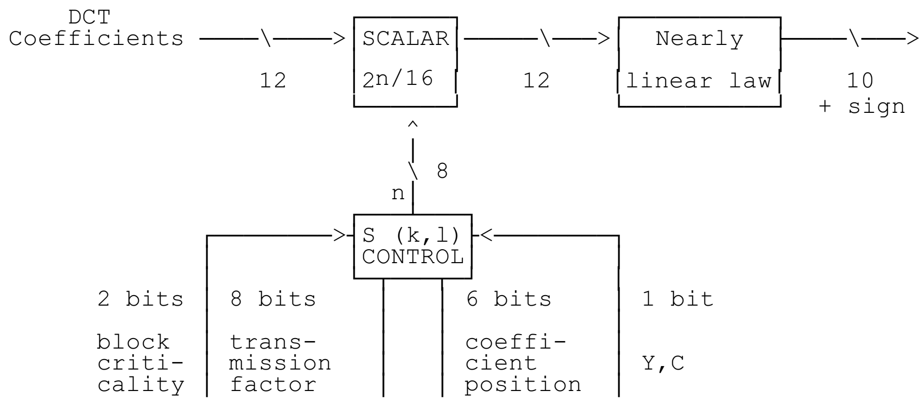


Figure 8

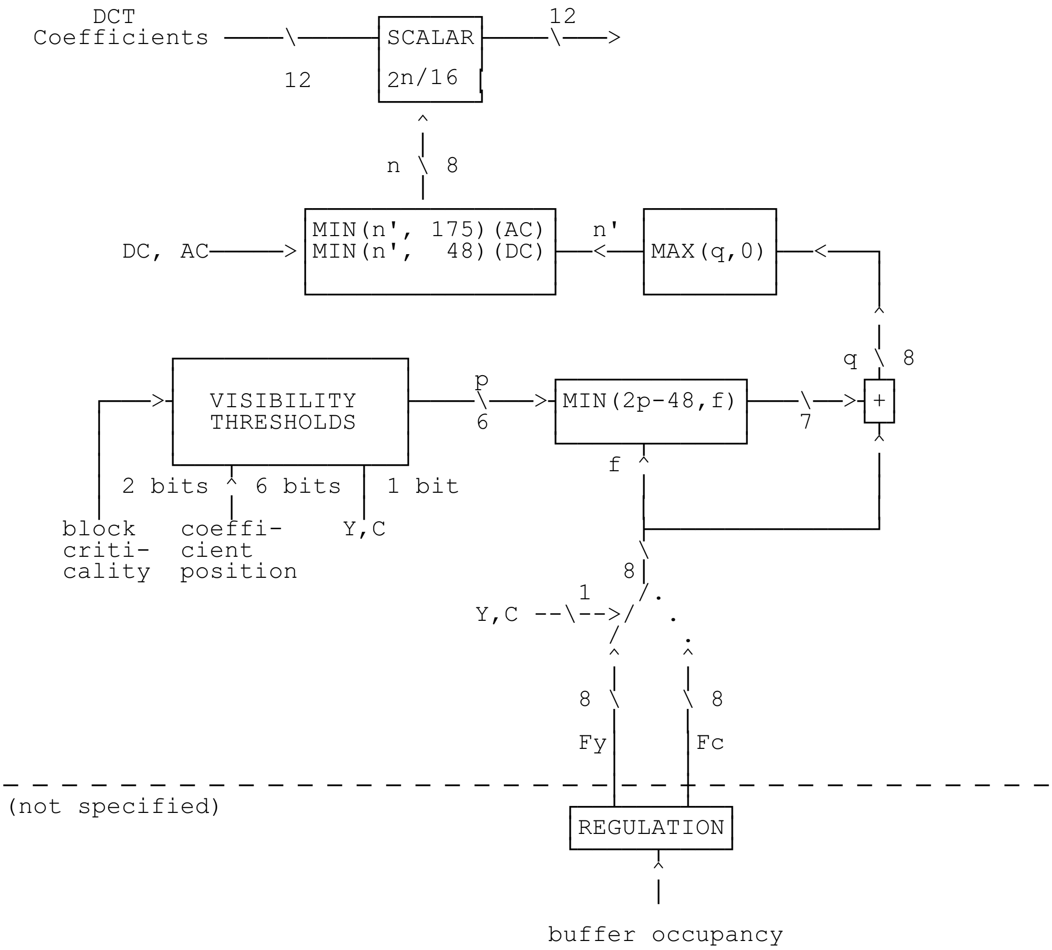


Figure 9: S (k,l) control

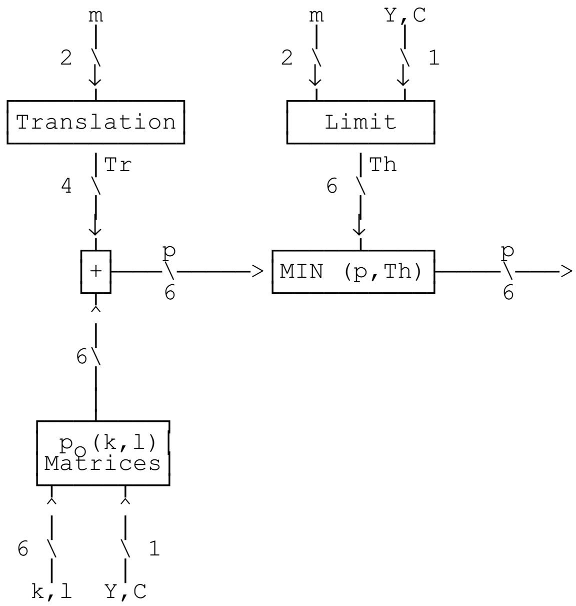


Figure 10: Computation of p(k,l,m)

6.2 DC-coefficient quantisation

The DC coefficient Z (0,0) is quantised using the same process as the AC coefficients but the scaling factor n(0,0,m,f) of the DC coefficient is limited to the range [0, 48].

6.3 Inverse quantisation

The reconstructed DCT coefficients are given by the following formula:

$Z'(k,l) = C'(k,l) * S(k,l,m,f) * ½$

where:

$S(k,l,m,f) = 2^{n(k,l,m,f)/16}$ as defined in subclause 6.1;

C'(k,l) is the quantised value corresponding to the transmitted quantiser level.

n(k,l,m,f) may be expressed as:

$n(k,l,m,f) = 16\ q + r;$

where q (quotient) and r (remainder) are integers, $0 \leq r < 16$, so that:

$Z'(k,l) = C'(k,l) * 2^{q-1} * 2^{r/16}$.

The 12 bits values for $2^{r/16}$ are given in table 7. The same set of values may be used in the quantiser.

$C'(k,l) * 2^{q-1}$ is obtained by a binary left shift of q-1 bits performed on the 12 bits value C'(k,l). Only the rightmost 12 bits of the result are significant and are used in the following multiplication.

Z'(k,l) is the result of the multiplication of $C'(k,l)2^{q-1}$ by $2^{r/16}$, truncated to 12 bits.

Table 7: Values of $2^{r/16}$

r	$2^{r/16}$	$2\ 048*2^{r/16}$
0	1,00000000000	2 048
1	1,00001011011	2 139
2	1,00010111001	2 233
3	1,00100011100	2 332
4	1,00110000011	2 435
5	1,00111101111	2 543
6	1,01001100000	2 656
7	1,01011010110	2 774
8	1,01101010000	2 896
9	1,01111010001	3 025
10	1,10001010110	3 158
11	1,10011100010	3 298
12	1,10101110100	3 444
13	1,11000001101	3 597
14	1,11010101100	3 756
15	1,11101010010	3 922

7 Variable length coding for DCT coefficients and motion vector differences

7.1 Scanning path for quantised DCT values

Non-zero DCT coefficients are quantised and VLC coded. Runs of zeros, according to the scanning path shown in figure 11 are coded as run-lengths.

0	2	6	12	20	28	36	44
1	5	11	19	27	35	43	51
3	7	13	21	29	37	45	52
4	10	18	26	34	42	50	57
8	14	22	30	38	46	53	58
9	17	25	33	41	49	56	61
15	23	31	39	47	54	59	62
16	24	32	40	48	55	60	63

scanning path for luminance

0	2	3	9	10	20	21	35
1	4	8	11	19	22	34	36
5	7	12	18	23	33	37	48
6	13	17	24	32	38	47	49
14	16	25	31	39	46	50	57
15	26	30	40	45	51	56	58
27	29	41	44	52	55	59	62
28	42	43	53	54	60	61	63

scanning path for chrominance

Figure 11

The transmission of the last run length of zeros in a block is avoided by anticipating the EOB. The decoder assumes that the last coefficients in a block are all zeros when less than 64 coefficients are decoded.

If there is one or more coefficients +1 between two runs of zeros, or between a run of zeros and the EOB, one of them is not transmitted and the decoder reinserts it.

7.2 Assignment of codewords to quantised values and run lengths

The words at the output of the variable length coder have the following structure:

$|1\ X_i| \ldots |1\ X_1|\ |0\ X_o|$, $i=0..8$, $X_i \in \{0,1\}$

$|1\ X_8| \ldots |1\ X_1|\ |1\ X_o|$, $X_i \in \{0,1\}$

where | | corresponds to a pair of bits, and where $\in$ indicates a mapping.

The first bit is the continuation bit and if this is 0 the present pair is the last one except for the word having length 18; the second bit of each pair, and both the bits of the last pair if the word length is 18, is the information bit and can assume the value 0 or 1. The length of the available words can vary from 2 to 18, as indicated in table 8, and the words having less than 18 end with a $|0\ X_0|$ pair.

Table 8

i	word length (bit)	word structure	no of words
0	2	0 X_o	2
1	4	1 $X_1$0 X_o	4
2	6	.	8
3	8	.	16
4	10	.	32
5	12	.	64
6	14	.	128
7	16	1 X_7....0 X_o	256
8	18	1 X_8....0 X_o	512
	18	1 X_8....1 X_o	512

The total number of words is 1 534. 66 of them are used to code the run length of zeros, the special words EOB_0 and EOB_1, indicating the end of each block (see subclause 8.1.4), and the word NULL (used in case of underflow).

In order to avoid underflow, the zero values can be coded using the NULL word. In this case a run-length of n zeros can be coded with n NULL words. It is permissible to mix the NULL words and run-length of zeros to obtain the desired length of n. The NULL word is considered as a normal value so a "+ 1" between two NULL words must be transmitted.

The codes 11 11 11 11 11 11 11 11 11 and 10 10 10 10 10 10 10 10 10 are reserved.

The remaining 1 466 words are available to code the quantised levels from -733 to +733.

Two assignment tables for the values of X (quantised levels) lower than 17 and greater than -17 and for the run lengths up to 28 zeros are used. In table 9 the value of luminance or chrominance coefficients assigned to codewords differ in 20 cases, thus two different assignment tables are required to specify the luminance or the chrominance coefficients. The assignments of EOB_0 and EOB_1 are fixed for all the tables.

Table 9: Assignment for luminance (Y) and chrominance (C) coefficients

Codeword	Y		C	Codeword	Y		C
01		1		00		-1	
11 00		2		10 01		-2	
11 01		0*1		10 00		0*2	
11 10 00		0*3		10 11 01		0*4	
11 10 01	3		0*5	10 11 00	-3		0*6
11 11 00	4		0*7	10 10 01	-4		0*8
(11 11 01 reserved, EOB_1)				(10 10 00 reserved, EOB_0)			
11 10 10 00	0*5		3	10 11 11 01	0*6		-3
11 10 10 01	0*7		4	10 11 11 00	0*8		-4
11 10 11 00		0*9		10 11 10 01		0*10	
11 10 11 01		0*11		10 11 10 00		0*12	
11 11 10 00		5		10 10 11 01		-5	
11 11 10 01	6		0*13	10 10 11 00	-6		0*14
11 11 11 00	7		0*15	10 10 10 01	-7		0*16
11 11 11 01	8		0*17	10 10 10 00	-8		0*18
11 10 10 10 00	0*13		6	10 11 11 11 01	0*14		-6
11 10 10 10 01	0*15		7	10 11 11 11 00	0*16		-7
11 10 10 11 00	0*17		8	10 11 11 10 01	0*18		-8
11 10 10 11 01		0*19		10 11 11 10 00		0*20	
11 10 11 10 00		0*21		10 11 10 11 01		0*22	
11 10 11 10 01		0*23		10 11 10 11 00		0*24	
11 10 11 11 00		0*25		10 11 10 10 01		0*26	
11 10 11 11 01		0*27		10 11 10 10 00		0*28	
11 11 10 10 00		9		10 10 11 11 01		-9	
11 11 10 10 01		10		10 10 11 11 00		-10	
11 11 10 11 00		11		10 10 11 10 01		-11	
11 11 10 11 01		12		10 10 11 10 00		-12	
11 11 11 10 00		13		10 10 10 11 01		-13	
11 11 11 10 01		14		10 10 10 11 00		-14	
11 11 11 11 00		15		10 10 10 10 01		-15	
11 11 11 11 01		16		10 10 10 10 00		-16	

In table 9, above, 0*n refers to a run-length of n zeros.

The information bits for the positive values and the corresponding negative values are complemented. The information bits for EOB_0 and EOB_1 are complemented.

The assignments for run lengths of zeros from 29 up to 63 and for the codeword NULL are shown in table 10.

There follow examples of the use of Run Lengths and End of Blocks:

EXAMPLE 1:

```
Coefficients:        -2      0 0 0    +1    +1     0 0     +2     0 0 0 0   End of Block
Codewords:   1001  11100001   01    01    1000   1100    101101     111101
Transmitted: 1001  11100001   01          1000   1100               111101
```

+1 is not transmitted because there are two +1s between two runs of zeros, and a run of 4 zeros is not transmitted because the EOB is anticipated.

EXAMPLE 2:

```
Coefficients:          -2     0 0 0 0 0 0 0 0 0     +1   End of Block
Codewords:      1001        11101100         01   111101
Transmitted:    1001        11101100              111101
```

+1 is not transmitted because it is between a run of 9 zeros and the EOB.

Table 10: Assignments for run length of zeros

Codeword	Run of zeros	Codeword	Run of zeros
11 10 10 10 10 00	0*29	10 11 11 11 11 00	0*30
11 10 10 10 10 01	0*31	10 11 11 11 11 01	0*32
11 10 10 10 11 00	0*33	10 11 11 11 10 00	0*34
11 10 10 10 11 01	0*35	10 11 11 11 10 01	0*36
11 10 10 11 10 00	0*37	10 11 11 10 11 00	0*38
11 10 10 11 10 01	0*39	10 11 11 10 11 01	0*40
11 10 10 11 11 00	0*41	10 11 11 10 10 00	0*42
11 10 10 11 11 01	0*43	10 11 11 10 10 01	0*44
11 10 11 10 10 00	0*45	10 11 10 11 11 00	0*46
11 10 11 10 10 01	0*47	10 11 10 11 11 01	0*48
11 10 11 10 11 00	0*49	10 11 10 11 10 00	0*50
11 10 11 10 11 01	0*51	10 11 10 11 10 01	0*52
11 10 11 11 10 00	0*53	10 11 10 10 11 00	0*54
11 10 11 11 10 01	0*55	10 11 10 10 11 01	0*56
11 10 11 11 11 00	0*57	10 11 10 10 10 00	0*58
11 10 11 11 11 01	0*59	10 11 10 10 10 01	0*60
11 11 10 10 10 00	0*61	10 10 11 11 11 00	0*62
11 11 10 10 10 01	0*63	10 10 11 11 11 01	Null

The assignments for values of quantised levels X are made in two's-complement using the following rules:

Range of x	Rules
-733 ... -479	Add +1501, then generate 9 info bits, set continuation bit of last pair to 1 (see EXAMPLE 3).
-478 ... - 17	Add -34, then generate up to 9 info bits, not considering all the leading bits equal to 1 (see EXAMPLE 4).
- 16 ... + 16	Use table 9 for assignment.
+ 17 ... +478	Add +33, then generate up to 9 info bits, not considering all the leading bits equal to 0 (see EXAMPLE 5).
+479 ... +733	Add +34, then generate 9 info bits, set continuation bit of last pair to 1 (see EXAMPLE 6).

EXAMPLE 3: from -733 to -479
X=-733 > -733+1501 = 768 = $(001\ 100000000)_2$ =
(|1 1|1 0|1 0|1 0|1 0|1 0|1 0|1 0|1 0|)vlc
(X_8 X_7 X_6 X_5 X_4 X_3 X_2 X_1 X_0)vlc

X=-479 > -479+1501 = 1022 = $(001\ 111111110)_2$ =
(|1 1|1 1|1 1|1 1|1 1|1 1|1 1|1 1|1 0|)vlc
(X_8 X_7 X_6 X_5 X_4 X_3 X_2 X_1 X_0)vlc

EXAMPLE 4: from -478 to -17
X=-478 > -478-34 = -512 = $(111\ 000000000)_2$ =
(|1 0|1 0|1 0|1 0|1 0|1 0|1 0|1 0|0 0|)vlc
(X_8 X_7 X_6 X_5 X_4 X_3 X_2 X_1 X_0)vlc

X=-403 > -403-34 = -437 = $(111\ 001001011)_2$ =
(|1 0|1 0|1 1|1 0|1 0|1 1|1 0|1 1|0 1|)vlc
(X_8 X_7 X_6 X_5 X_4 X_3 X_2 X_1 X_0)vlc

X=-23 > -23-34 = -57 = $(111111\ 000111)_2$ =
(|1 0|1 0|1 0|1 1|1 1|0 1|)vlc
(X_5 X_4 X_3 X_2 X_1 X_0)vlc

EXAMPLE 5: from +17 to +478
X=23 > 23+33 = 56 = $(000000\ 111000)_2$ =
(|1 1|1 1|1 1|1 0|1 0|0 0|)vlc
(X_5 X_4 X_3 X_2 X_1 X_0)vlc

X=403 > 403+33 = 436 = $(000\ 110110100)_2$ =
(|1 1|1 1|1 0|1 1|1 1|1 0|1 1|1 0|0 0|)vlc
(X_8 X_7 X_6 X_5 X_4 X_3 X_2 X_1 X_0)vlc

X=478 > 478+33 = 511 = $(000\ 111111111)_2$ =
(|1 1|1 1|1 1|1 1|1 1|1 1|1 1|1 1|0 1|)vlc
(X_8 X_7 X_6 X_5 X_4 X_3 X_2 X_1 X_0)vlc

EXAMPLE 6: from +479 to +733
X=479 > 479+34 = 513 = $(001\ 000000001)_2$ =
(|1 0|1 0|1 0|1 0|1 0|1 0|1 0|1 0|1 1|)vlc
(X_8 X_7 X_6 X_5 X_4 X_3 X_2 X_1 X_0)vlc

X=733 > 733+34 = 767 = $(001\ 011111111)_2$ =
(|1 0|1 1|1 1|1 1|1 1|1 1|1 1|1 1|1 1|)vlc
(X_8 X_7 X_6 X_5 X_4 X_3 X_2 X_1 X_0)vlc

7.3 Coding of the motion vectors

Predictive encoding of the motion vectors is performed along a stripe of blocks. The components of the prediction error on the horizontal (MV_x) and vertical (MV_y) directions are VLC coded according to table 11. The prediction for the motion vector of a macro-block is the motion vector of the previous macro-block of the stripe. The prediction for the first macro-block of a stripe and for a macro-block following an intra-field or inter-field encoded macro-block is 0 for both coordinates of the motion vector.

The motion vector differences MV_x and MV_y are only sent:

- if the macro-block is inter frame encoded; and

- if the motion vector difference (MV_x , MV_y) is different from (0,0).

The corresponding macro-blocks are identified by MI = "10".

Table 11: Codewords for the motion vector differences

Codeword	MV_x or MV_y	Codeword	MV_x or MV_y
01	0	00	−0,5
11 00	+0,5	10 01	−1
11 01	+1	10 00	−1,5
11 10 00	+1,5	10 11 01	−2
11 10 01	+2	10 11 00	−2,5
11 11 00	+2,5	10 10 01	−3
(11 11 01 reserved, EOB_0)		(10 10 01	reserved, EOB_0)
11 10 10 00	+3	10 11 11 01	−3,5
11 10 10 01	+3,5	10 11 11 00	−4
11 10 11 00	+4	10 11 10 01	−4,5
11 10 11 01	+4,5	10 11 10 00	−5
11 11 10 00	+5	10 10 11 01	−5,5
11 11 10 01	+5,5	10 10 11 00	−6
11 11 11 00	+6	10 10 10 01	−6,5
11 11 11 01	+6,5	10 10 10 00	−7
11 10 10 10 00	+7	10 11 11 11 01	−7,5
11 10 10 10 01	+7,5	10 11 11 11 00	−8
11 10 10 11 00	+8	10 11 11 10 01	−8,5
11 10 10 11 01	+8,5	10 11 11 10 00	−9
11 10 11 10 00	+9	10 11 10 11 01	−9,5
11 10 11 10 01	+9,5	10 11 10 11 00	−10
11 10 11 11 00	+10	10 11 10 10 01	−10,5
11 10 11 11 01	+10,5	10 11 10 10 00	−11
11 11 10 10 00	+11	10 10 11 11 01	−11,5
11 11 10 10 01	+11,5	10 10 11 11 00	−12
11 11 10 11 00	+12	10 11 10 01	−12,5
11 11 10 11 01	+12,5	10 10 11 10 00	−13
11 11 11 10 00	+13	10 10 10 11 01	−13,5
11 11 11 10 01	+13,5	10 10 10 11 00	−14
11 11 11 11 00	+14	10 10 10 10 01	−14,5
11 11 11 11 01	+14,5	10 10 10 10 00	−15
11 10 10 10 10 00	+15	10 11 11 11 11 01	−15,5
11 10 10 10 10 01	+15,5	10 11 11 11 11 00	−16
11 10 10 10 11 00	+16	10 11 11 11 10 01	−16,5
11 10 10 10 11 01	+16,5	10 11 11 11 10 00	−17
11 10 10 11 10 00	+17	10 11 11 10 11 01	−17,5
11 10 10 11 10 01	+17,5	10 11 11 10 11 00	−18
11 10 10 11 11 00	+18	10 11 11 10 10 01	−18,5
11 10 10 11 11 01	+18,5	10 11 11 10 10 00	−19
11 10 11 10 10 00	+19	10 11 10 11 11 01	−19,5
11 10 11 10 10 01	+19,5	10 11 10 11 11 00	−20
11 10 11 10 11 00	+20	10 11 10 11 10 01	−20,5
11 10 11 10 11 01	+20,5	10 11 10 11 10 00	−21
11 10 11 11 10 00	+21	10 11 10 10 11 01	−21,5
11 10 11 11 10 01	+21,5	10 11 10 10 11 00	−22
11 10 11 11 11 00	+22	10 11 10 10 10 01	−22,5
11 10 11 11 11 01	+22,5	10 11 10 10 10 00	−23
11 11 10 10 10 00	+23	10 10 11 11 11 01	NULL
11 11 10 10 10 01	+23,5	10 10 11 11 11 00	−23,5
11 11 10 10 11 00	+24	10 10 11 11 10 01	−24
11 11 10 10 11 01	+24,5	10 10 11 11 10 00	−24,5
11 11 10 11 10 00	+25	10 10 11 10 11 01	−25
11 11 10 11 10 01	+25,5	10 10 11 10 11 00	−25,5
11 11 10 11 11 00	+26	10 10 11 10 10 01	−26
11 11 10 11 11 01	+26,5	10 10 11 10 10 00	−26,5
11 11 11 10 10 00	+27	10 10 10 11 11 01	−27
11 11 11 10 10 01	+27,5	10 10 10 11 11 00	−27,5
11 11 11 10 11 00	+28	10 10 10 11 10 01	−28

8 Video framing and forward error correction

8.1 Video framing

A single stream is produced for Variable Length Coded (VLC) and Fixed Length Coded (FLC) data. All data are transmitted MSB first.

8.1.1 General structure

Even fields are organized as follows:

FSW 00 FCP BOF

FSW 01 FCP BOF

FSW 10 FCP BOF

SSW SN_0 BO_0 TFY_0 TFC_0 $(MI_j\ CT_j\ VLC_j)_0$ $[STUFF]CRC_0$

:

SSW SN_i BO_i TFY_i TFC_i $(MI_j\ CT_j\ VLC_j)_i$ $[STUFF]CRC_i$

:

SSW SN_{m-1} BO_{m-1} TFY_{m-1} TFC_{m-1} $(MI_j\ CT_j\ VLC_j)_{m-1}$ $[STUFF]CRC_{m-1}$

m = 36 for a 50 Hz system
m = 31 for a 60 Hz system
i varies from 0 to m-1 for each stripe and j varies from 1 to 45 (position of the macro-block in the stripe).
VLC_j are VLC data for the jth macro-block, and have the form:

$$[MV_x, MV_y]\ \ VLC_{y1}\ \ EOB\ \ VLC_{cb}\ \ EOB\ \ VLC_{y2}\ \ EOB\ \ VLC_{cr}\ \ EOB$$

Odd fields are organized in a similar manner where i varies from m to 2m-1.

8.1.2 Detailed content

FSW	Field Synchronisation Word (47"1" + "0") (see NOTE 1)	48 bits
	00 01 10 — Are used to identify the threefold repetition of FSW, FCD and BOF	2 bits
FCP	Field Coding Parameters (see subclause 8.1.3)	30 bits
BOF	Buffer Occupancy Field (measured at the beginning of the active field just before the first FSW is inserted into the buffer) (see NOTE 2)	16 bits
SSW	Stripe Synchronisation Word ("0" + 46"1" + "0")	48 bits

BO	Buffer Occupancy (indicates the buffer occupancy at the coder just before the SSW of the current stripe is inserted into the buffer) (see NOTE 2)	16 bits
SN_i	Stripe Number for the ith stripe range is from 0 to 71 {50 Hz system}: 0 to 35 {even field} 36 to 71 {odd field} the MSB is set to "0" range is from 0 to 61 {60 Hz system}: 0 to 30 {even field} 31 to 61 {odd field} the two MSB's are set to "0"	8 bits
TFY_i	Transmission Factor for luminance in the ith stripe (from 0 to 175)	8 bits
TFC_i	Transmission Factor for chrominance in the ith stripe (from 0 to 175)	8 bits
CRC_i	Cyclic Redundancy Code for the ith stripe (to be applied to all bits of the encoded stripe excluding SSW. The generator polynomial is $1 + x^2 + x^{15} + x^{16}$	16 bits
MI_j	Mode Identification 00 intra-field mode 01 inter-field mode 10 inter-frame mode with motion compensation [motion vector difference ≠ (0,0)] 11 inter-frame mode with motion compensation [motion vector difference = (0,0)]	2 bits
CT_j	Criticality (from 0 to 3)	2 bits
MV_x	VLC codeword associated with the motion prediction error in the horizontal direction (see table 11 and NOTE 4)	variable
MV_y	VLC codeword associated with the motion prediction error in the vertical direction (see table 11 and NOTE 4)	variable
VLC_y1	VLC words for first Y block in the macro-block	variable
VLC_{cb}	VLC words for C_B block in the macro-block	variable
VLC_{y2}	VLC words for second Y block in the macro-block	variable
VLC_{cr}	VLC words for C_R block in the macro-block	variable
[STUFF]	Stuffing bits (see NOTE 3)	2, 4, 6, 8, 10, 12 or 14 bits
EOB	End-Of-Block code (see subclause 8.1.4) (EOB_0 = "10 10 00" EOB_1 = "11 11 01")	6 bits

NOTE 1: The stream of video data is organised in 16-bit words. In order to ensure easy synchronisation, FSW and SSW are aligned at the beginning of these words.

NOTE 2: Minimum coder buffer occupancy equals 128 kbit. Maximum coder buffer occupancy is 1 572,864 kbit minus 128 kbit. The buffer occupancy at the coder is measured in bits, and is 21 bits long. The empty condition is equal to "zero" and only the 16 most significant bits are transmitted.

NOTE 3: In order to ensure that the number of coded bits corresponding to a stripe is an integer multiple of 16 bits, stuffing bits are inserted between the last coded macro-block of the stripe and the CRC, if needed. As the number of coded bits is even, the possible configurations for the stuffing bits are: (00)*n where n = 1, 2, 3, 4, 5, 6 or 7 and (00)*n means n times repetition.

NOTE 4: MV_x and MV_y are transmitted only when mode MI_j=10.

8.1.3 Definition of the data for phase information and status in the video multiplex

Field Coding Parameters (FCP)

MSB	r	VF	AR	r	ST	VA	FS	SL	BA	SCP	LSB
	2	3	1	3	1	1	3	1	7	8	

r reserved bits, set to "0", ignored by the receiver.
VF Video Format
000 = 4:2:2, 001 = PAL, 010 = NTSC
011 = SECAM, 100 = MAC.
AR Aspect Ratio
0 = 4:3
1 = 16:9.
ST System Type
0 = 50 Hz, 1 = 60 Hz.
VA V-Axis switch (PAL)
VA = 1 for positive phase on the first line of each field.
FS

Field Sequence	Frame	Field
000	1	1
001	1	2
010	2	3
011	2	4
.	.	.
.	.	.
.	.	.
111	4	8

SL Subcarrier/Line frequency relationship
0 = correct.
BA Burst Amplitude (for PAL and NTSC only).
The amplitude of the subcarrier burst is quantised as a CCIR Recommendation 601 luminance signal, with the MSB omitted.
SCP Subcarrier Phase (for PAL and NTSC only).
Phase of the reference subcarrier at the field-synchronisation datum respectively field start as defined in CCIR Report 624-3 [8], MSB first.

Scale: 0 = ([360°/256] * 0)
1 = ([360°/256] * 1)
... = ...
255 = ([360°/256] * 255)

8.1.4 Generation of the EOB sequence

Two VLC words are assigned to the End-Of-Block event: EOB_0 and EOB_1. At the coder a pseudo random sequence is generated, the repetition of which is equal to the number of blocks (180) in a video stripe of blocks. The pseudo random generator is reset at the beginning of each stripe. At the end of each block, the pseudo random generator steps forward one bit and the output of the generator, 0 or 1 determines which of the two EOB words, EOB_0 and EOB_1 is inserted as delimiter of the block.

The pseudo-random generator is based on the following polynomial:

$$g(x) = 1 + x^5 + x^9$$

and corresponds to the feedback shown in figure 12.

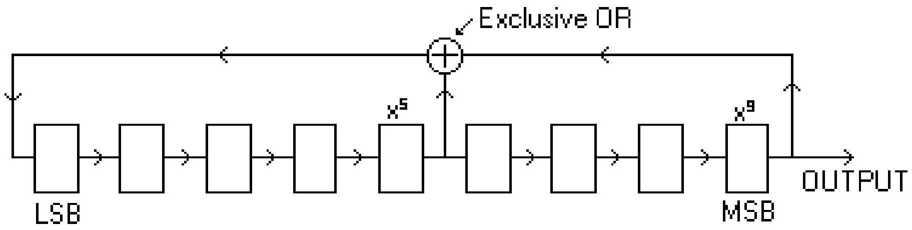


Figure 12

EOB_0 and EOB_1 correspond respectively to one "0" and "1" at the output of the pseudo random generator.

The initial value of the shift register at the beginning of each stripe is:

```
LSB —> 100111000.
```

With the configuration, the initial value at the beginning of a stripe may also be obtained by simply inverting the LSB of the contents of the shift register at the end of the previous stripe.

The successive states of the pseudo random generator are:

State 1	100111000 (beginning of a stripe)
State 2	110011100
State 3	111001110
.	.
.	.
.	.
State 180	001110001 (end of stripe)
Following state	000111000
	v
State 1	100111000 (beginning of the following stripe)

8.2 Forward error protection and correction

The transmission signal is protected from transmission errors by a RS (Reed Solomon) (255,239) code which is used to correct 8 octet errors and has 2 octet interleaving.

The generator polynomial of the RS code is given by:

$$\Pi_{i=0}^{15} (x+\alpha^{i})$$

where α is a root of the binary primitive polynomial $x^8 + x^4 + x^3 + x^2 + 1$.

A data octet (d_7, d_6, ..., d_1, d_0) is identified with the element $d_7\alpha^7 + d_6\alpha^6 + ... + d_1\alpha + d_0$ in Galois Field (GF) (256), the finite field with 256 elements.

The redundancy of the forward error coding is 6,69 %.

The data stream is interleaved in a two-stage operation, as follows.

First stage.

the data stream at the output of the video encoder is arranged in a matrix of 16 rows of 239 columns. Each column corresponds to one 16-bit word of video data. The first column is reserved and ignored by the decoder.

The RS (255,239) code is computed on each of the 2 rows of octets and the 16 octet error control group is added to the corresponding row. The write sequence is performed from column 1 to column 238 with the sequence shown in figure 13.

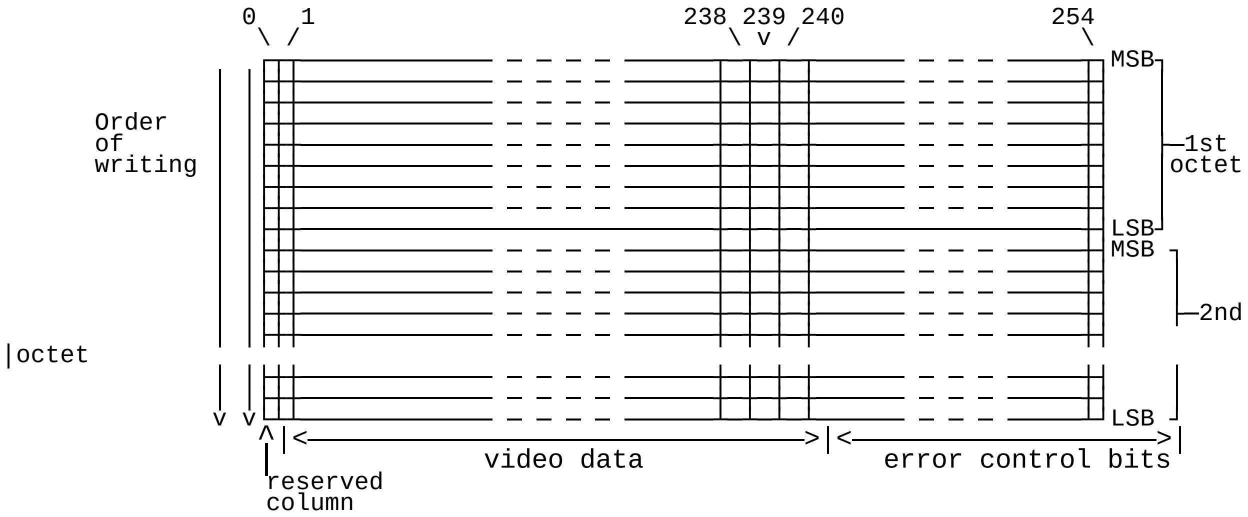


Figure 13

Second stage .

Three successive blocks formed in the first stage are interlaced column by column to form the superblock shown in figure 14. Numbers refer to the sequence of video-data octets passed from the video-framing layer to the first stage of error protection. Transmission is performed reading octets column by column.

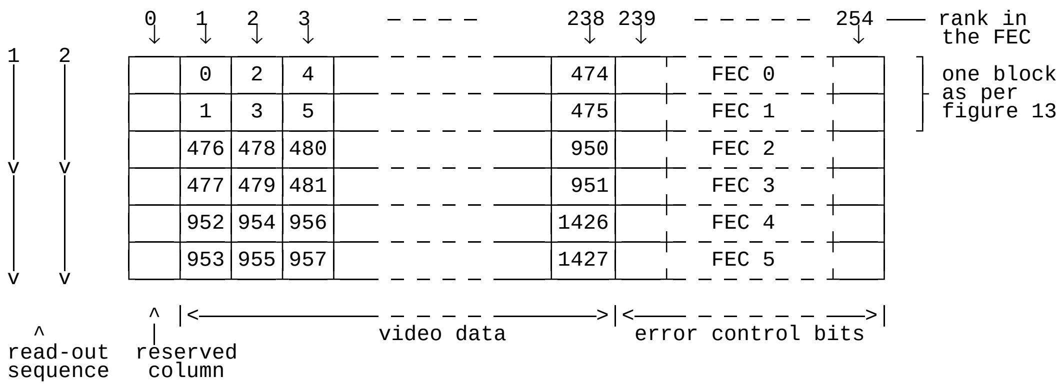


Figure 14

9 Additional services

9.1 Audio

A maximum of two separate channels is provided for the transport of audio services through the codec. These appear in the multiplex as octets A and A', where A is the primary and A' is the supplementary audio data channel. By varying the frequency of occurrence of A and A' octets in the multiplex, channel rates of 2 048 kbit/s or 1 544 kbit/s can be accommodated either singly, or as a pair. Any data capacity not used for audio is reutilised for video data. The A and A' channels can be used synchronously or asynchronously, and are intended for use with appropriate audio codecs having their own data protection mechanisms.

9.2 Supervision channel

9.2.1 Overview

The supervision channel is intended to carry information related to the operation of the encoder and to the management of the transmission.

Part of this information is directly related to the codec and is specified in this subclause. Other information may be defined at a later stage.

The requirement that various types of messages are serially inserted in the channel necessitates a protocol which will accommodate potentially long user-messages yet which guarantees a sufficiently short transmission time for urgent service messages such as alarms.

To this effect, the organisation of the supervision channel complies with the rules developed for the formatting of user data in the AES/EBU digital audio interface (see EBU Tech. 3250 [9]).

For transmission of necessary fundamental codec messages only that part of the format described below need be implemented. The parameters introduced to maintain full compatibility with the complete format are noted between braces { }.

The definition of the supervision channel comprises the following sections:

- message definition;
- packet structure;
- frame structure;
- channel management;
- extension rules.

9.2.2 Message definition

9.2.2.1 Alarms (mandatory, address FE hex, priority 3)

Alarms indication message. The alarm condition is logic "zero". It is comprised of:

Octet 0: Alarms related to the encoder itself:

- bit 0 (LSB) power supply fault;
- bit 1 time-base error in the multiplexer;
- bit 2 fault in the video processing chain;
- bit 3 fault in the audio processing chain;
- bit 4-7 reserved (set to logic "one");

Octet 1: Alarms related to the video input:

- bit 0 (LSB) no input signal (analogue interface) junction fault (digital interface);
- bit 1 time-base error;
- bit 2 out-of-spec input signal (the encoder cannot work properly);
- bit 3 out-of spec input signal (the encoder can still work, possibly with reduced quality);
- bit 4-7 reserved (set to logic "one");

Octet 2: Alarms related to the auxiliary signals in the video field blanking interval:

- bit 0-7 reserved (set to logic "one");

Octet 3: Alarms related to the audio input(s):

- bit 0 (LSB) junction fault (digital interface only);
- bit 1 time-base error;
- bit 2 out-of-spec input signal (the encoder cannot work properly);
- bit 3 out-of-spec input signal (the encoder can still work, possibly with reduced quality e.g. saturation of analogue inputs);
- bit 4-7 reserved (set to logic "one").

9.2.2.2 Multiplex structure (mandatory, address FD hex, priority 2)

This message provides information related to the multiplex structure for use by network supervision equipment, if necessary.

Octet 0: Copy of the 8-bit word carried by bit m_2 in octet J4 of the multiplex. LSB corresponds to the bit carried in frame 0, MSB to the bit carried in frame 7.

Octet 1: Copy of bits carried through bit m3.

Octet 2: Copy of bits carried through bit m4.

Octet 3: Video format, as specified in the FCP field of the videomux:

- bit 0 (LSB) system type;
- bit 1 aspect ratio;
- bit 2-4 video format;
- bit 5-7 reserved (set to logic "one").

Octet 4: Sound encoding method:

- 00 not specified;
- 01 according to CCIR Recommendation 724 [10];
- others reserved (set to logic "one").

9.2.2.3 Source identification (optional, address FC hex, priority 2)

User-defined alphanumeric string of up to 15 ASCII characters. MSB is set to "0". Non-printing control characters (codes 01 hex to 1F hex and 7F hex) are not permitted.

9.2.2.4 Destination identification (optional, address FB hex, priority 2)

User-defined alphanumeric string of up to 15 ASCII characters. MSB is set to "0". Non-printing control characters (codes 01 hex to 1F hex and 7F hex) are not permitted.

9.2.2.5 Identification of the encoder (optional, address FA hex, priority 2)

User-defined alphanumeric string of up to 15 ASCII characters. It may be used to distinguish each of the coders on the network. MSB is set to "0". Non-printing control characters (codes 01 hex to 1F hex and 7F hex) are not permitted.

9.2.2.6 Other messages

The present list of messages may be extended, provided that they comply with the requirements of the extended system. In particular, messages longer than 15 octets will be segmented in order to limit the length of packets.

9.2.2.7 Header

Each message is preceded by the following header octet:

bit 0-3 message length in octets, excluding the header (LSB is bit 0);

bit 4 set to "0" {"1" indicates the encoding of lengths above 15 octets};

bit 5-7 3-bit continuity index of messages sent with a given address. Not incremented in case of repetition of the previous message.

9.2.3 Packet structure

Messages preceded by the header described above {and segmented if necessary, in the case of the extended mode} are inserted in packets.

A packet consists of:

- an address octet identifies the nature of the message. This address is specified in subclause 9.2.2 for the messages already defined (in the case of an extended system, an address extension octet may be added);
- a control octet: structured as follows:
  - bits 0 and 1: priority index {used to manage resource sharing when needed}. See subclause 9.2.2 for the messages already defined;
  - bits 2 to 4: continuity index referring to packets sent with a given address. Not incremented in case of repetition of the previous message. For single segment messages, this index may be equal to the message repetition index;
  - bit 5: "0" {used for software address extension};
  - bit 6 and 7: b6="0",b7="1" {used to link segmented messages};
- the message {or message segment}.

9.2.4 Frame structure

The packets defined above (19 octets maximum) are transmitted within High-Level Data Link Control (HDLC) frames (see ISO Standard 3309-2 [11]) on the 8 kHz supervision channel provided by bit S of the container.

An HDLC frame comprises:

- a beginning flag: "01111110";
- a packet;
- a 16-bit error-detecting CRC (FCS: Frame Check Sequence);
- an ending flag, identical to the beginning one.

To avoid the imitation of flags by data, HDLC defines a method of suppressing long strings of ones in the data or CRC areas.

All messages received incorrectly will be ignored according to the HDLC rules. Furthermore, messages sent to addresses which are not recognised by the receiver should also be ignored.

9.2.5 Channel management

HDLC frames are organised in blocks starting every 800 ± 1 bits (10 Hz repetition rate).

Each block starts with the transmission of the alarm message (address FE hex), followed by other HDLC frames in any order. The "idle" mode should be avoided between transmission of successive HDLC frames.

When all frames to be transmitted in a block have been sent, the channel is filled with "ones" ("idle" mode) until the start of the new block.

This procedure is compatible with the extended system and allows, if needed, downstream insertion of other data.

To prevent channel saturation, it is recommended that the encoder should send messages defined with priority 2 every two or three blocks and with an approximately even distribution over successive blocks.

9.2.6 Extension rules

Extension to the transmission of other messages, if necessary, will be based on the protocol under study in AES for the transmission of user data across the professional digital audio interface.

However, it should be recognised that the reduced bit-rate available will have implications on the real-time performance of the system and on the definition of priority levels.

Address field 00 to 7F hex is allocated for user-defined applications. All undefined addresses in the field 80 hex to FF hex are reserved.

9.3 Transmission frame for teletext and other digital data inserted during field blanking intervals

This subclause concerns the use of a 384 kbit/s channel to carry teletext and other signals found in the Vertical Blanking Interval (VBI) of a television signal. Teletext is normally present only for distribution but this may not be true in the future, or where "teletext" coding is used to enable data to be transmitted during contribution, e.g. ancillary data carried in the 4:2:2 interface (see table 1).

9.3.1 Introduction

The frame is optimised for the transmission of the various teletext systems described in CCIR Recommendation 653 [12], but it may also be used for other forms of messages. Up to 4 096 messages may be defined, among which teletext messages form a particular class.

Each message comprises a type identifier, a length indicator and the data field itself.

Each frame has a fixed length and consists of a synchronisation word, a frame status, a 46-octet field carrying one (possibly 2) message(s) and protection bits.

When the allocated transmission bit-rate exceeds the required data bit-rate, dummy data fields are transmitted. Thus, there is no need to justify the frames in the transmission multiplex.

9.3.2 Frame structure

The frame is composed of the following information (see figure 15). In all fields MSB are sent first:

- a 10-bit synchronisation word 010011011X (see NOTE 1);
- a 4-bit frame header including:
  - . a system type identifier:
    0: 625/50;
    1: 525/60;
  - . a reserved bit fixed to 0;
  - . a frame status 2 bits, see subclause 9.3.3;
- a 24-bit message header including:
  - . a 12-bit message type-identifier;
  - . a field identifier (see NOTE 2):
    0: first field;
    1: second field;
    2: third field;
    3: fourth field;
  - . a 6-bit message length indicator;
  - . a 4-bit interleaved parity word: BIP-4 (even parity computed over the frame header and the message header);
- depending on the frame status, either:
  - . a 43-octet data field for a single message;

  or,

  - . a 20-octet data field for a first message;
  - . a second message header (the BIP-4 applies also to the frame header);
  - . a second 20-octet data field for a second message;
- an 18-bit error protecting code, BCH (390, 372), computed over the full frame, synchronisation word excepted (see NOTE 3).

NOTE 1: X alternates between "0" and "1". The beginning of the synchronization word coincides with the start of a new octet in the container (see subclause 10.2).

NOTE 2: Field numbering is in accordance with CCIR Report 624-3 [8]. The code corresponds to the field number from which the current data unit is extracted.

NOTE 3: The code is a shortened BCH (511,493) with the generator polynomial $g(x)=(x^9+x^4+1)(x^9+x^6+x^4+x^3+1)$.

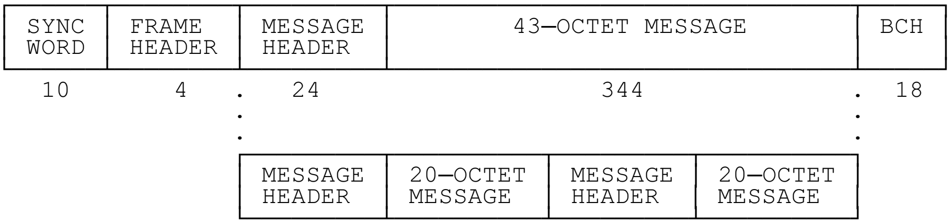


Figure 15: Frame structure

9.3.3 Data field allocation

Messages of length 43 octets or less are inserted in the appropriate data field. If the message length is less then the data field capacity, the last remaining octets are set to zero. The length indicator is in the range 1 to 43 (or 1 to 20).

Single data field frames are indicated by a status equal to 0.

Double data field frames are indicated by a status equal to 1.

If messages longer than 43 octets are to be transmitted, they are split into 43-octet segments. These segments are sent in successive frames bearing the same message type-identifier. The length indicator of the last segment describes the number of useful octets in this segment. The length indicator of other segments starts from 48 and is increased by one from frame to frame (63 is updated to 48).

The frame status is encoded as follows:

0: frame with a single 43-octet data field (message of length up to 43 octets);

1: frame with two 20-octet data fields;

2: frames of a segmented message, except the last one;

3: last frame of a segmented message.

Unused data fields are marked with a message type-identifier equal to zero. Data field is set to all zeros.

9.3.4 Teletext messages

Teletext messages are formed by the complete data unit specified for the system. For system B teletext in 525/60 systems, a dummy octet, set to zero, is added at the end of the data unit. The message length is therefore as shown in table 12.

Table 12

Teletext System	Message Length (625/50)	Message Length (525/60)
A	38	
B	43	36
C	34	34
D		35

The message type-identifier is in the form 1111000XXXXX. The 5 LSBs form a Line Identifier (LI) which indicates the line number (see NOTE) as shown in table 13.

Table 13

(LI)		625/50		(LI)		525/60	
0	=	line	1/314	0	=	line	1/264
1	=	line	2/315	1	=	line	2/265
2	=	line	3/316	2	=	line	3/266
.				.			
.				.			
.				.			
20	=	line	21/334	20	=	line	21/284
21	=	line	22/335	21	=	line	260/523
22	=	line	311/624	22	=	line	261/524
23	=	line	312/625	23	=	line	262/525
24	=	line	313	24	=	line	263
25 to 31		unused		25 to 31		unused	

NOTE: Line numbering is in accordance with CCIR Report 624-3 [8]. The code corresponds to the line number from which the current data unit is extracted.

9.3.5 EBU Tech 3217 data

These biphase coded data, EBU Technical Document 3217 (3rd editiion 1986) [13], are not decoded. The sampling frequency is thus equal to twice the nominal data frequency (5 MHz). The message type-identifier is 111100011111 (F1F hex).

9.4 Transmission format of test lines in a 128 kbit/s channel

9.4.1 Introduction

In intervals of 5 fields a testline is digitised according to the sampling structure defined in subclause 9.4.2. The data are given to a transmission buffer and then transmitted in a format (described in subclause 9.4.3) by a channel with a bit-rate of 128 kbit/s.

If 3 testlines per field are in use, they are sampled sequentially. Thus the lines have to be repeated 15 times when reinserting them at the decoder.

In order to keep the phase consistency for the subcarrier in composite lines, the test lines have to be reinserted in the fields with the same field number (1 to 8 for PAL). This means that 8 times the number of testlines used per field have to be stored.

9.4.2 Sampling of the testlines

Testline sampling is in accordance with CCIR Recommendation 601 [1] luminance sampling with the following differences:

10 bit scale used, with range 0 ... 1023;

black corresponds to 288 (32 + 256);

100 % white corresponds to 726.

This sampling structure permits values below black level (composite signals) with double resolution. It corresponds to CCIR Recommendation 601 [1] with 9 bits resolution, scale extension and scale shift by 256.

9.4.3 Format

The transmission of a testline starts after sampling of a testline and has the following format:

00	S	R	FS	L	E	D1	D2		Dn	00

↑ Field start, modulo 5 fields

S Synchronisation word {32 "1" + "00010010"}. The beginning of the synchronisation word coincides with the start of a new octet in the container (see subclause 10.2).

R Reserved bits, 3 bits (normally = 0).

FS Field status, 3 bits.

0	0	0	field one
0	0	1	field two
.	.	.	.
.	.	.	.
.	.	.	.
1	1	1	field eight

L Line identifier, 5 bits. Same assignment as for teletext (see table 13).

E Error protection, 5 bits.
R, FS and L are protected by an extended Hamming code (16,11)
{(15,11) code + even parity} generated with the polynomial $x^4 + x + 1$ + even parity bit.

Dn Data word + parity, 12 bits.
d0 = MSB
d9 = LSB
d10 = Reserve (e.g. higher resolution) else = 0
p = Parity bit, even parity over d0, d1, d2, d3, d4.

Pairs of consecutive words are interleaved as follows (' denotes the second sample):

d0	d'0	d5	d'5	followed by
d1	d'1	d6	d'6	followed by
d2	d'2	d7	d'7	followed by
d3	d'3	d8	d'8	followed by
d4	d'4	d9	d'9	followed by
p	p'	d10	d'10	

- the first sample, D1, corresponds with the first sample of the digital line (resp. after the active video timing reference code) defined in CCIR Recommendation 656 [14];

- the number, n, of data words is 864 for the 625 lines system and 858 for the 525 lines system, respectively;

- the number of remaining octets until the data of the next testline depends on the system type and should be filled with octets of zeros.

9.5 Transmission of 80-bit serial time code in a dedicated 8 kHz channel

The time code, which is defined in IEC Publication 461 [15] is first demodulated and then justified in successive transmission frames of 9-bit length.

Each frame contains 2 or 3 bits of time code data, the justification indication and error correction redundancy. It is constituted as follows (d0 transmitted first):

- d0 = 1st time code data bit;

- d1 = 2nd time code data bit;

- d2 = 3rd time code data bit (or justification bit);

- ij = justification indication ("1" if d2 is used);
- p0 = exclusive OR of (d0, d1, ij);
- p1 = exclusive OR of (d1, d2, ij);
- p2 = exclusive OR of (d0, d1, d2) complemented;
- p3 = exclusive OR of (d0, d2, ij);
- ij' = repetition of ij.

NOTE 1: p0 - p3 are complemented and form a Hamming extended code protecting d0, d1, d2 and ij. In case of double error detection, ij' may be used instead of ij.

NOTE 2: In case of sync loss on reception, all code words received are detected in error.

NOTE 3: The precise timing between time code and video components may be guaranteed in the decoder by controlling the time of emission of the time code sync word.

10 Service multiplex

10.1 Introduction

The service multiplex is based on a set of two compatible TV containers, organised according to a octet-oriented 8 kHz structure.

It permits multiplexing of:

- a video channel;
- zero, one or two channels for audio (1 544 kbit/s or 2 048 kbit/s) (see NOTES 1, 2, 3 and 7 of subclause 10.2.3);
- zero, one or two 384 kbit/s channels for teletext/auxiliary applications (see NOTES 6 and 7 of subclause 10.2.3);
- a 128 kbit/s channel for testlines (see NOTE 7 of subclause 10.2.3);
- an 8 kbit/s channel for supervision;
- two 8 kbit/s channels for conditional access;
- two 8 kbit/s channels for time codes.

The structure is arranged in 6 rows (see figure 16) giving 384 kbit/s per column. The multiplex structure is indicated by a special channel and gives the flexibility needed to allocate the above channels. Changes in capacity are made in steps of a number of columns (n x 384 kbit/s).

For error monitoring a bit-interleaved parity check is provided. An appropriate pointer permits the synchronisation of the FEC block.

The service multiplex does not provide error correction for the channels. Therefore for random bit-errors the contributory channels will have the same bit error ratios as that of the received data stream.

10.2 TV container

10.2.1 General structure

Data are transmitted row after row.

1)			1	2				14	15				26	27				39	40				51	52				64	65				76	77			88
2)			1	2				18	19				34	35				50	51				66	67				83	84				99	100			114
	P	L	A	A'	V	V	...	A	A'	V	V	...	A	A'	V	V	...	T	T'	V	V	...	A	A'	V	V	...	A	A'	V	V	...	A	A'	V	V	...
			J1	J'1	V	V	...	A	A'	V	V	...	A	A'	V	V	...	T	T'	V	V	...	A	A'	V	V	...	A	A'	V	V	...	A	A'	V	V	...
			J2	J'2	V	V	...	A	A'	V	V	...	A	A'	V	V	...	T	T'	V	V	...	A	A'	V	V	...	A	A'	V	V	...	A	A'	V	V	...
			A	A'	V	V	...	A	A'	V	V	...	A	A'	V	V	...	T	T'	V	V	...	A	A'	V	V	...	A	A'	V	V	...	A	A'	V	V	...
			J3	J'3	V	V	...	A	A'	V	V	...	A	A'	V	V	...	T	T'	V	V	...	A	A'	V	V	...	A	A'	V	V	...	A	A'	V	V	...
			J4	J'4	V	V	...	A	A'	V	V	...	A	A'	V	V	...	T	T'	V	V	...	A	A'	V	V	...	A	A'	V	V	...	A	A'	V	V	...

1) 34 Mbit/s column allocation
2) 45 Mbit/s column allocation

Figure 16: Container structure (125 μs)

The container defined for 34 Mbit/s (530 octets in length) is compatible with five SDH TU-2 containers concatenated (TU2-5c), a SDH VC-3 container and fits into the 34 368 kbit/s CCITT Recommendation G.751 [2] transmission frame.

The container defined for 45 Mbit/s (686 octets) is compatible with a SDH VC-3 container, seven SDH TU-2 containers concatenated and fits into the 44 736 kbit/s CCITT Recommendation G.752 [3] transmission frame.

Interworking between 34 and 45 Mbit/s levels is possible by mapping of one container in the other as described in subclause 10.2.4.

10.2.2 Column allocation

Octets J, which indicate the use of other columns, are always transmitted in column 1.

Columns 14, 26, 51, 64 and 76 (18, 34, 66, 83 and 99 at 45 Mbit/s) are used to carry channel A (2 048 kbit/s or 1 544 kbit/s if column 76 (99) is not used).

Column 39 (50) is used for channel T.

Columns 2, 15, 27, 52, 65 and 77 (2, 19, 35, 67, 84 and 100) are used to carry a second channel A' (2 048 kbit/s or 1 544 kbit/s if column 77 (100) is not used). Column 2 is active only when channel A' is active, otherwise it carries video data.

Column 40 (51) is used for a second channel T'.

All other columns (but never column 1), plus columns for A, A', T and T' if not in use, are allocated to video data.

10.2.3 Definitions

V Octet for video data. The first octet in the container belongs to FEC 0 of a superblock (see subclause 8.2).

P Bit Interleaved Parity (BIP) code using even parity (BIP-8, as defined for SDH); the P refers to the previous container, excluding its P. It is computed after scrambling, if applied.

L [l_1, l_2, l_3, ... l_8] Pointer for FEC block synchronisation. L indicates the rank of the first V octet of a container within FEC 0 of a superblock (see figure 14). l_1 = MSB.

L=0 when the first V octet of the container corresponds to the first octet of the FEC 0, L = 254 for the last octet of FEC 0.
L indicates the position of the first two video octets carried at the beginning of the container within the two interleaved error correction blocks (2 x 255 octets). l_1= MSB.

L=0 when the first two video octets of the container correspond to the first column of the FEC block, L = 254 for the last column.

A, A' Octets for 2 048 kbit/s or 1 544 kbit/s channels (synchronous or asynchronous mode, see NOTES 1, 2 and 3). Channel A is the primary audio channel.

T, T' Octets for teletext/auxiliary applications. Channel T is the primary channel for data formatted according to 9.3. T' is the primary channel for data not formatted according to subclause 9.3.

J, J' Octets containing justification, video clock recovery and frame usage bits, as follows (transmitted from left to right):

J1	aj	vj	ca1	r	b_0	b_1	b_2	b_3
J2	aj	vj	ca2	vitc	b_4	b_5	b_6	b_7
J3	aj*	vj	s	ltc	b_0	b_1	b_2	b_3
J4	m_1	m_2	m_3	m_4	b_4	b_5	b_6	b_7
J'1	a'j	r	r	r	r	r	r	r
J'2	a'j	r	r	r	r	r	r	r
J'3	a'j*	r	r	r	r	r	r	r
J'4	r	r	r	r	r	r	r	r

ca1 Channel for the key management of the conditional access system.

ca2 Synchronisation channel for the conditional access system.

s Bit for 8 kbit/s supervision channel.

ltc Channel for the 80 bits longitudinal time code (see subclause 9.5).

vitc Reserved for transmission of vertical insertion time code.

b_0-b_7 Bits for testline transmission of 128 kbit/s organised in octets (b_0 is the MSB).

m_1 Bit sequence defining a multiframe of length 8 (see table 14).

m_2,m_3 Channel defining the frame usage in a bit-serial (see table 14).

& m_4 Format (see table 14).

aj, aj* Positive/negative justification bits for channel A. The justification is made on two successive 8 kHz frames.

- aj* in the first frame (even frame) and bits aj in both frames transmit the justification indication, repeated 5 times.

- aj* in the second frame (odd frame) is available for positive justification of channel A. For negative justification, the first bit of the next A octet has to be used. Positive justification is indicated by aj/aj* = 1.

a'j, a'j* Same definition as aj, aj* for A' channel.

vj Bit for video clock transmission (pos./neg.) {repeated three times - see NOTE 4}.

r bits reserved for future applications.

Table 14

FRAME NUMBER	PARITY	m_1	FRAME USAGE DEFINED BY: m_2	m_3	m_4
0	even	1	"1" if T channel in use	"1" if T' channel in use	Scrambling update flag (see subclause 12.7.3)
1	odd	1	"1" if A channel in use	"1" if A' channel in use	Scrambling operation mode (see subclause 12.7.3)
2	even	1	"1" if A channel is synchronous (see NOTE 2)	"1" if A' channel is synchronous (see NOTE 2)	Scrambling operation mode (see subclause 12.7.3)
3	odd	0	"1" if A channel is 1544 kbit/s (see NOTE 3)	"1" if A channel is 1544 kbit/s (see NOTE 3)	Reserved
4	even	1	"0" if T channel is formatted as in subclause 9.3 "1" if T channel is used for auxiliary purposes	"0" if T' channel is formatted as in subclause 9.3 "1" if T' channel is used for auxiliary purposes	Reserved
5	odd	0	000* = single video channel, 34 Mbit/s	Reserved	Reserved
6	even	0	001 = single video channel, 45 Mbit/s	Reserved	Reserved
7	odd	0	others reserved	Reserved	Reserved

***)** Frame 5 carries the MSB

NOTE 1: If channel A or A' is used to transmit 1 544 kbit/s, the last column is left for video data. The two A or A' octets in column 1 are unused with the exception of the first bit in the first octet.

NOTE 2: A synchronous mode is provided for A and/or A' channels. The first A or A' octet in the container frame corresponds to time-slot 0 of the 2 048 kbit/s frame or to the framing bit of the 1 544 kbit/s frame.

NOTE 3: If both A and A' channels are in use, they must have the same nominal bit-rates.

NOTE 4: The 13,5 MHz clock used for video sampling in the encoder is compared to a network-related 8 kHz reference. A 13,5 MHz clock is used to drive a counter which is reset at the end of each 8 kHz clock period; the count reached before resetting can be either 1 687 or 1 688.

Each frame of the transmission multiplex carries a video clock recovery bit, repeated 3 times for error protection, and defined as follows:

- "0" if 1 687 clock pulses;
- "1" if 1 688 clock pulses.

The original 8 kHz reference is reconstructed in the decoder by division of the local 13,5 MHz clock and compared with a local 8 kHz network-related reference. The phase difference is used to adjust the frequency of the local oscillator.

The generation of the block sequence should be controlled by the encoder in such a way that, in the absence of jitter at the input of the encoder, the phase jitter requirement defined by CCIR Recommendation 601 [1] is met when the PLL in the decoder has a bandwidth of 3 Hz or less. The use of dithering or of an equivalent technique is necessary.

The system should be able to tolerate an error on the video clock sampling frequency of up to 10^{-5}.

NOTE 5: In order to permit the proper compensation of any difference in sound or vision delay resulting from different implementations of encoders or decoders, the delays needed to synchronise sound and vision components should be divided equally between both ends.

For each end, the sound and vision delay should be zero ± 1 ms.

The sound delay is defined as the average delay between the input of a sound signal to the sound encoder and the time of transmission of the corresponding data bits in the container.

The vision delay is defined as the delay between the time of reception by the encoder of the first pixel of the first active line and the time of transmission of the FSW, when the BOF sent in the FSW corresponds to 50 % of the specified buffer capacity.

Sound and vision delays should include any delay associated with a possible pre-processing of sound or vision components (e.g. filtering).

NOTE 6: The format for teletext use is defined in subclause 9.3. The same format may also be used for transmission of auxiliary data.

Alternatively, the channels formed by the T' and T octets may be used as transparent 384 kbit/s channels. The data format is not specified for this application.

NOTE 7: As a consequence of the framing structure, the burst error length is normally limited to 8 bits for the 2 048 kbit/s, 1 544 kbit/s and 384 kbit/s channels (i.e. audio, teletext/auxiliary) and to 4 bits for the 128 kbit/s channel (testlines). The appropriate error protection, which is to be provided by these tributaries, should take due account of these characteristics.

10.2.4 34 and 45 Mbit/s interworking

For interworking between 34 and 45 Mbit/s networks, the following procedure is recommended:

Encoding is performed at the bit-rate defined by the 530-octet container. This container is carried on 34 Mbit/s-based networks by means of the corresponding network adaptation layers.

For transmission on 45 Mbit/s-based networks, this container is mapped into the 686-octet container, carried by the corresponding network adaption layer.

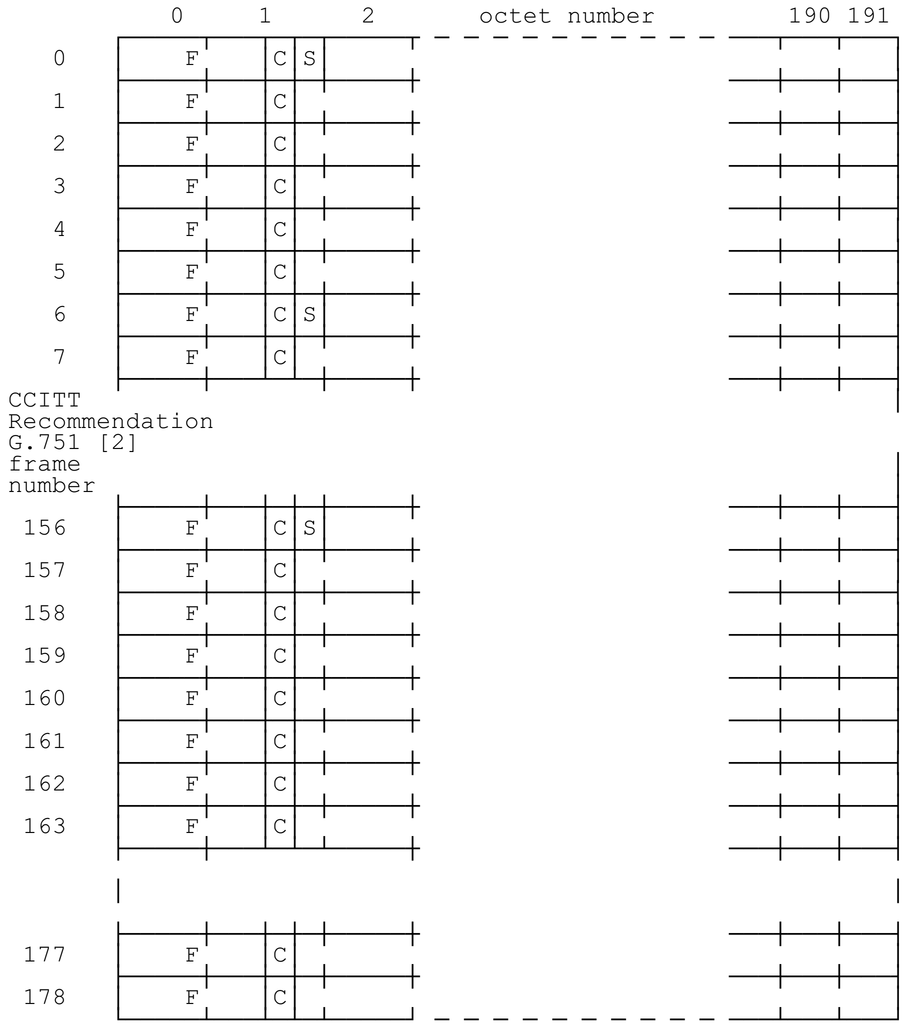
The mapping of the 530-octet container in the 686-octet one is achieved by filling each field in the 686-octet container with the corresponding data in the 530-octet container followed by the necessary stuffing octets, set to "all ones", in columns 14 to 17, 30 to 33, 47 to 49, 62 to 65, 79 to 82, 95 to 98 and 112 to 114.

11 Network adaptation

11.1 Network adaptation to 34 368 kbit/s CCITT Recommendation G.751 frame

If the framing structure of CCITT Recommendation G.751 [2] is used for transmission, the TV container is first mapped into blocks of 532 octets comprising two reserved octets followed by 530 octets of data. These blocks are then mapped into a CCITT Recommendation G.751 [2] frame by using a multiframe structure. As is shown in figure 17 the same multiframe structure may also be used for mapping ATM or Distributed Queue Dual Bus (DQDB) cells.

Payload capacity: 34 048 kbit/s.
Block length: 532 octets.
Multiframe: 179 G.751 frames carrying 64 blocks; the first bit after the 2 stuffing bits in frame 0 is the first bit of one block of 532 octets.



F (12 bits) = frame alignment (10 bits) plus alarm bit and national bit.
C (2 bits) = chain code.
S (2 bits) = stuffing bits (every 6th frame, from frame 0 to frame 156).

Figure 17: Structure of the 8 ms multiframe (179 CCITT Recommendation G.751 [2] frames)

Two C bits are assigned to every frame. These bits are obtained from a pseudo-random generator based on the polynomial:

$$g(x) = 1 + x^5 + x^9$$

and corresponds to the feedback shown in figure 18:

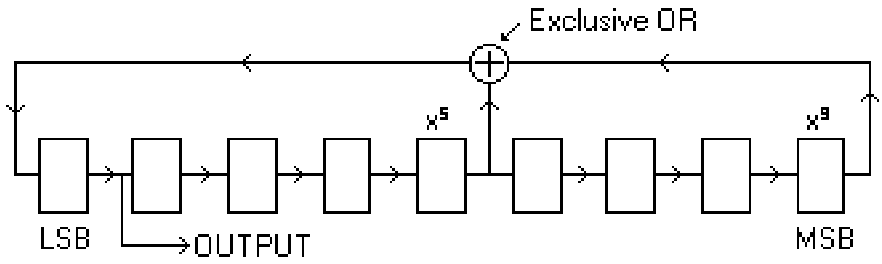


Figure 18

The initial value at the beginning of the first frame is:

```
LSB —> 01111101
```

and is updated twice every frame.

With this configuration, the initial value at the beginning of the first frame may also be obtained by simply inverting the LSB of the contents of the shift register at the end of the last frame.

The successive states of the pseudo-random generator are:

```
                          LSB      MSB
                          |        |                         First     Second
State 0                   001111101                              \     /
                                      ]- Frame 0      transmitted bits 0,0
State 1                   000111110
State 2                   100011111
                                      ]- Frame 1      transmitted bits 1,0
State 3                   010001111
State 4                   101000111
                                      ]-  Frame 2     transmitted bits 1,1
State 5                   110100011
.               ...         ...           ...
.               ...         ...           ...
State 354                 111010110
                                      ]-  Frame 177   transmitted bits 1,1
State 355                 111101011
State 356                 111110101
                                      ]-  Frame 178   transmitted bits 1,0
State 357                 011111010
Following state           101111101
                          ↓
State 0                   001111101
                                      ]- Frame 0      transmitted bits 0,0
State 1                   000111110
```

11.2 Network adaptation of 686 octet containers to 44 736 kbit/s CCITT Recommendation G.752 frame

If the framing structure of CCITT Recommendation G.752 [3] is used for transmission, the appropriate 125 µs information block is mapped into this frame by using a multiframe structure. In this case, the block is equivalent to the TV container for 45 Mbit/s.

Payload capacity:	43 904 kbit/s.
Block length:	686 octets.
Multiframe:	699 G.752 frames, carrying 595 blocks; the first bit after the 6 'K' bits in the first frame of the multiframe is the first bit of one TV container.

bit number

0				85		170		255		340		425		510		595	
X	L	K		F_1		C		F_0		C		F_0		C		F_1	
X				F_1		C		F_0		C		F_0		C		F_1	
P				F_1		C		F_0		C		F_0		C		F_1	
P	R	R		F_1		C		F_0		C		F_0		C		F_1	
M_0				F_1		C		F_0		C		F_0		C		F_1	
M_1				F_1		C		F_0		C		F_0		C		F_1	
M_0	S			F_1		C		F_0		C		F_0		C		F_1	

Figure 19: Structure of one CCITT Recommendation G.752 [3] frame

This frame is repeated 699 times to make up one multiframe.

Structure of the 9,398 kHz (CCITT Recommendation G.752 [3]) frame

L	(10 bit) CCITT Recommendation G.752 [3] frame number (MSB first) starting from 0 and extending to 698.
K	(6 bit) indicates the frames where S is a stuffing octet according to the 14+ J*15 law with J having values between 0 and 45: K = 111111 for frames 14, 29, 45, etc.; K = 000000 for all other frames.
S	(8 bit) video stuffing octet.
R	(16 bit) reserved.
X*	Service function bit (repeated once).
C*	Control channel.
P*	Parity bit for the preceding multiframe (repeated once).
F_0*, F_1*	Subframe alignment bits.
M_0*, M_1*	Frame alignment bits.

* defined or present in CCITT Recommendation G.752 [3].

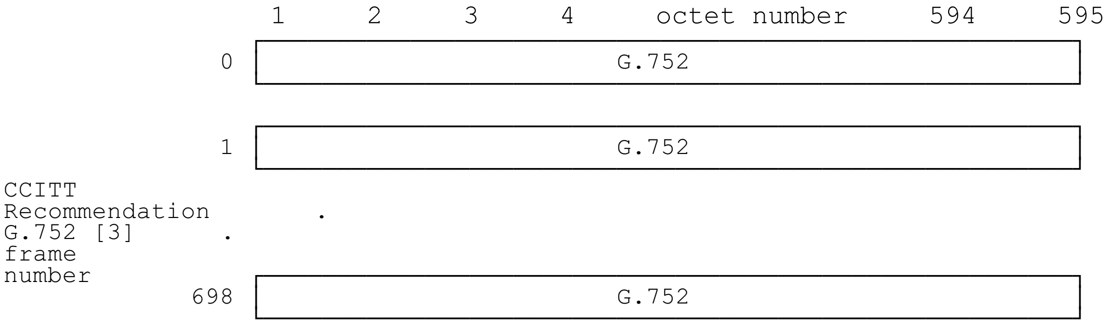


Figure 20: Structure of the 74,375 ms multiframe

11.3 Network adaptation to SDH

The 8 kHz structure of the television container is particularly convenient for mapping into SDH VC3 or VC2-5c containers. A proposed mapping for VC2-5c is given in informative Annex D.

12 Scrambling for conditional access of transmitted data

12.1 General description of the access control system

Figures 21 and 22 provide the functional block diagram of an encoder and a decoder with an access control system for one channel. The source information may be any one of the programme components (video, audio, or teletext) or all components together, considered as a unique service. Only the audio, teletext and video octets (V,A,A',T,T') may be scrambled. The auxiliary channels such as the supervision channel are not scrambled.

The main features of the scrambling system are:

- scrambling is done at the level of the service multiplex. Therefore, it is applied to audio, teletext and video after forward error correction;

  NOTE: Calculation of bit interleave parity is done after scrambling as specified in Clause 10.

- scrambling is achieved by means of an "Exclusive Or" operation between information octets (A,T,V) and sequential octets produced by a Pseudo-Random Generator (PRG). Octets P, L, J1, J2, J3, J4, J'1, J'2, J'3, J'4 are never scrambled;

- the scrambling sequence generator is a pseudo-random generator with a very long cycle time. Its output is made unpredictable by the use of a Control Word (CW) and a cyclic 16-bit Container Identification Word (CIW). A combination of these words initialises the PRG at the beginning of each container, every 125 µs;

- the length of the cyclic sequence giving the CIW is 65534. CW's are changed at the beginning of each new CIW sequence i.e. every 8,2 s (125 µs * 65534);

- the cryptograms are sent in Entitlement Control Messages (ECM) containing 2 encrypted control words (the current CW and the next CW) and also data concerning the administration of the control word. To allow faster locking for receivers connected during an 8,2 s period, cryptograms of CW's may be transmitted more frequently. ECMs are sent through the 8 kbit/s channel carried in bit CA1;

- the descrambling system must be synchronised between the source and the receiver. The scrambled source component, the CIW generator and the synchronising signal are derived from the multiplex structure. For instance, the validity period of a new control word begins when the CIW equals a specific value.

Moreover, the service operator can choose to send the signal scrambled or in the clear.

If scrambled, the service operator can use either a local control word which is constant and stored in the receiver or a regenerated control word transmitted in the ECM.

When the different programme components are scrambled individually, separate PRGs are used with different CWs. PRGs, which are not used to scramble (and unscramble) an octet at a given time are inhibited (no clock pulse and ignored output). Because of the delay needed for PRG initialisation, the last 11 octets of the container are left unscrambled.

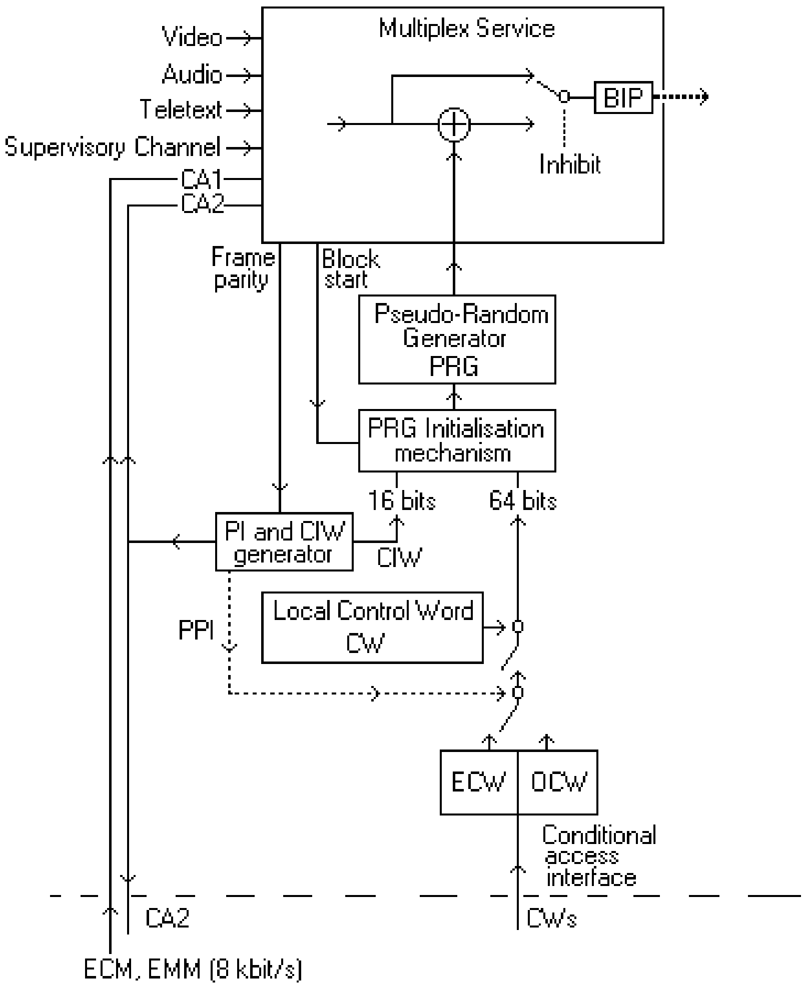


Figure 21: Scheme of the encoder

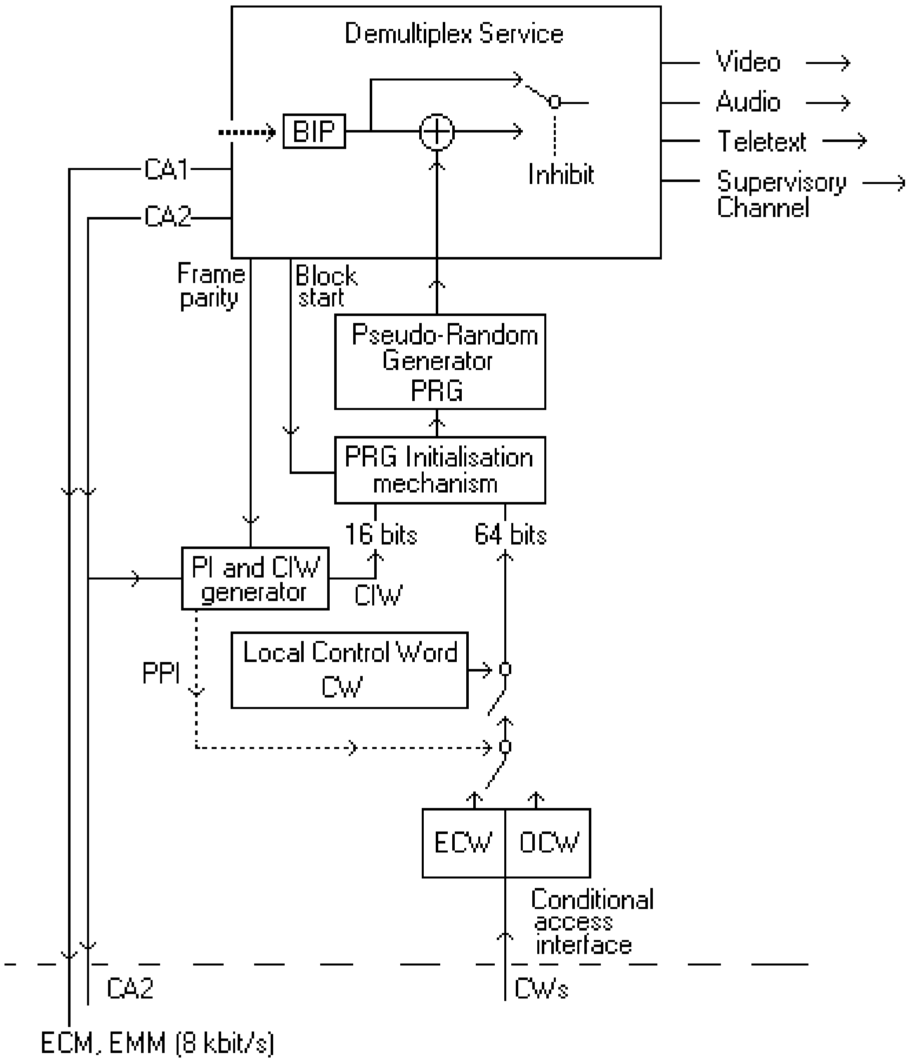


Figure 22: Scheme of the decoder

12.2 The pseudo-random generator

12.2.1 Introduction

The Pseudo-Random Generator (PRG) described in this ETS can be considered as being defined, at each step, by three variables:

- the internal state: X_n
- the input register: I_n
- the output register: O_n

The relations between these variables are:

$O_n = f(X_n)$ and $X_{n+1} = g(X_n, I_n)$.

The functions f and g are described later.

The PRG is based on four irreducible polynomials: Q, R, S, T. Two are defined over the Galois Field GF(31) and the other two over the Galois Field GF(127) as follows:

Polynomial Q $X^5 = 15X^2 + 30$ over GF(31) (the order of the roots of Q is $(31^5 - 1) / 15$).

Polynomial R $X^7 = X + 15$ over GF(31) (the order of the roots of R is $(31^7 - 1) / 3$).

Polynomial S $X^5 = 2X^2 + 125$ over GF(127) (the order of the roots of S is $(127^5 - 1) /9$).

Polynomial T $X^7 = 2X + 125$ over GF(127) (the order of the roots of T is $(127^7 - 1) /9$).

The PRG is synchronised on a container basis (125 µs). The PRG is initialised at the beginning of each container with a 64-bit Control Word (CW) sent by the conditional access system, and a 16-bit Container Identifier Word (CIW).

12.2.2 Description

(see figure 23)

The internal state X_n of the PRG is made up of the following registers:

- 5 registers of 5 bits: Q0, Q1, Q2, Q3, Q4;
- 7 registers of 5 bits: R0, R1, R2, R3, R4, R5, R6;
- 5 registers of 7 bits: S0, S1, S2, S3, S4;
- 7 registers of 7 bits: T0, T1, T2, T3, T4 ,T5, T6.

Hence, the size of the internal state is 144 bits.

Four start up registers QI, RI, SI, TI are loaded with a selection of the 8 bits of the input register:

if I_n = i7, i6, i5, i4, i3, i2, i1, i0 (8 bits) (i7 is the MSB)

then QI = i3, i2, i1, i0, i7 (5 bits)

RI = i0, i7, i6, i5, i4 (5 bits)

SI = i6, i5, i4, i3, i2, i1, i0 (7 bits)

TI = i7, i6, i5, i4, i3, i2, i1 (7 bits)

The evolution of the PRG, after n cycles of the clock is described by the following function g:

$$X_{n+1} = g\ (I_n, X_n)$$

$$\text{if } X_n = \left[\begin{array}{l} Q0,\ Q1,\ Q2,\ Q3,\ Q4 \\ R0,\ R1,\ R2,\ R3,\ R4,\ R5,\ R6 \\ \\ S0,\ S1,\ S2,\ S3,\ S4 \\ T0,\ T1,\ T2,\ T3,\ T4\ ,T5,\ T6 \end{array} \right.$$

$$\text{then } X_{n+1} = \left[\begin{array}{l} Q1,\ Q2,\ Q3\ \ (XOR)\ \ QI,\ Q4,\ \ (16\ \overline{Q2} + \overline{Q0})\ mod\ 31^* \\ R1,\ R2\ \ (XOR)\ \ RI,\ R3,\ R4,\ R5,\ R6,\ (R1 + 16\ R0)\ mod\ 31^* \\ \\ S1,\ S2,\ S3\ \ (XOR)\ \ SI,\ S4,\ (2\ S2 + 2\ \overline{SO})\ mod\ 127^* \\ T1,\ T2\ \ (XOR)\ \ TI,\ T3,\ T4,\ T5\ ,T6,\ (2\ T1 + 2\ TO)\ mod\ 127^* \end{array} \right.$$

Where (XOR) signifies EXCLUSIVE OR:

NOTE: X mod N* means that N is subtracted from X when X is greater than N (i.e. the result belongs to the interval [0, N]).

The output function f: $O_n = f\ (X_n)$ is computed thus:

If O_n = o(7), o(6), o(5), o(4), o(3), o(2), o(1), o(0) (8 bits, where o(7) is the MSB)

$$\begin{array}{l} o(0) = [S3(2).T5(0) + Q1(0).\overline{T5(0)}]\ \ (XOR)\ \ [T3(2).Q3(1) + R3(1).\overline{Q3(1)}] \\ o(1) = [S3(3).T5(1) + Q1(1).\overline{T5(1)}]\ \ (XOR)\ \ [T3(3).Q3(2) + R3(2).\overline{Q3(2)}] \\ o(2) = [S3(4).T5(2) + Q1(2).\overline{T5(2)}]\ \ (XOR)\ \ [T3(4).Q3(3) + R3(3).\overline{Q3(3)}] \\ o(3) = [S3(5).T5(3) + Q1(3).\overline{T5(3)}]\ \ (XOR)\ \ [T3(5).Q3(4) + R3(4).\overline{Q3(4)}] \\ o(4) = [Q2(1).R5(0) + S2(3).\overline{R5(0)}]\ \ (XOR)\ \ [R1(1).S1(0) + T1(3).\overline{S1(0)}] \\ o(5) = [Q2(2).R5(1) + S2(4).\overline{R5(1)}]\ \ (XOR)\ \ [R1(2).S1(1) + T1(4).\overline{S1(1)}] \\ o(6) = [Q2(3).R5(2) + S2(5).\overline{R5(2)}]\ \ (XOR)\ \ [R1(3).S1(2) + T1(5).\overline{S1(2)}] \\ o(7) = [Q2(4).R5(3) + S2(6).\overline{R5(3)}]\ \ (XOR)\ \ [R1(4).S1(3) + T1(6).\overline{S1(3)}] \end{array}$$

Where (XOR) signifies EXCLUSIVE OR.

Bit o(7) processes the first transmitted bit of an encrypted octet; bit o(0) processes the last transmitted bit.

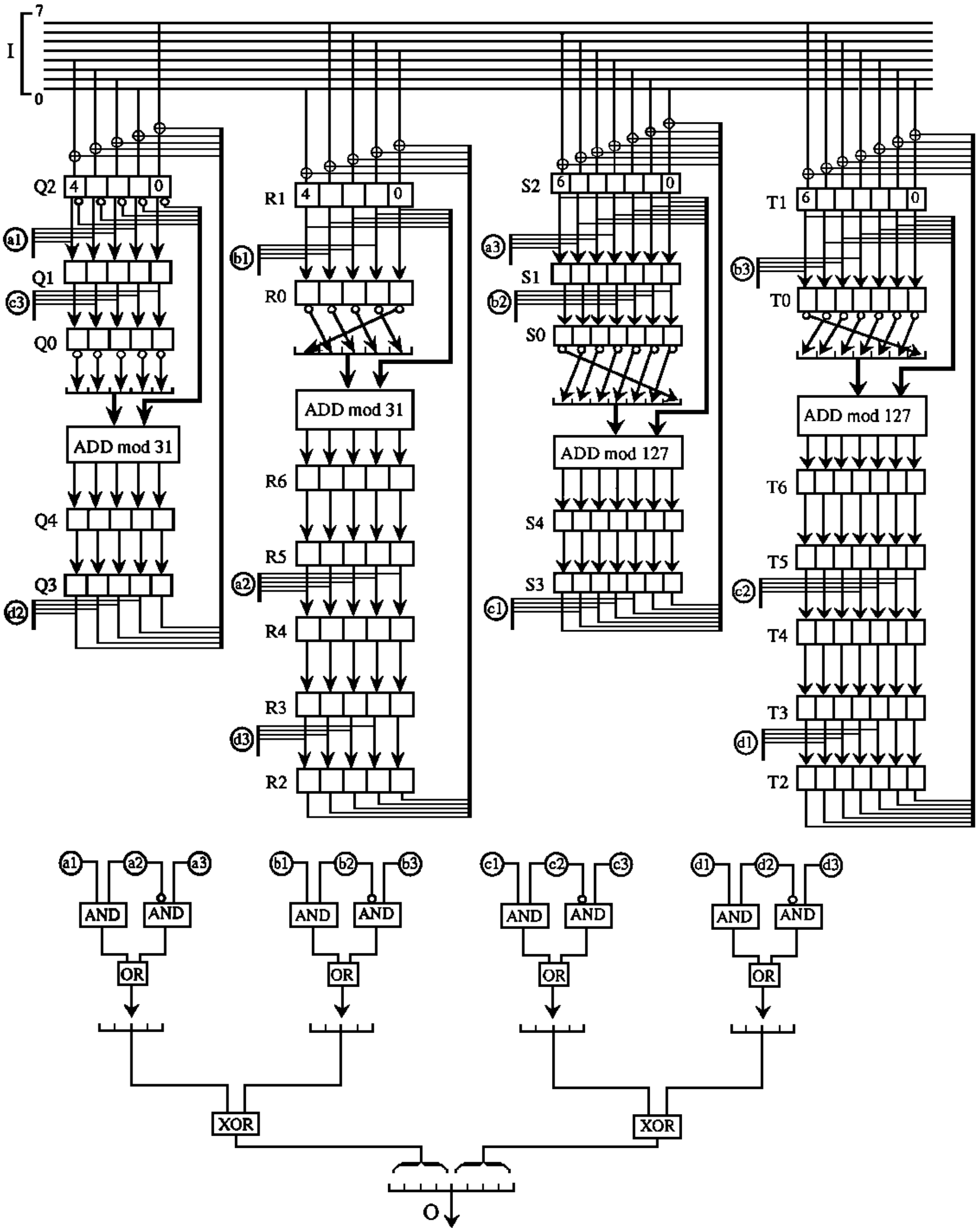


Figure 23: Pseudo-random generator

12.3 PRG initialisation parameters

12.3.1 CIW generator

The Container Identification Word (CIW) is a 16-bit word generated at the coder side and regenerated at the decoder side by means of a 15-bit chain-code and a frame parity bit as LSB. The input of the shift register associated with the chain-code is sent in the CA2 channel of the container: it allows the synchronisation of the sequences in the coder and in the decoder. This information is sent every two containers (odd frames as defined by bit m_1). A Phase Parity Identifier (PPI) is sent in the same bit of the container during even frames.

The chosen pseudo-random sequence is based on the polynomial $g(x) = 1 + x^{14} + x^{15}$. Which is generated using a shift register with the feedback loop shown in figure 24.

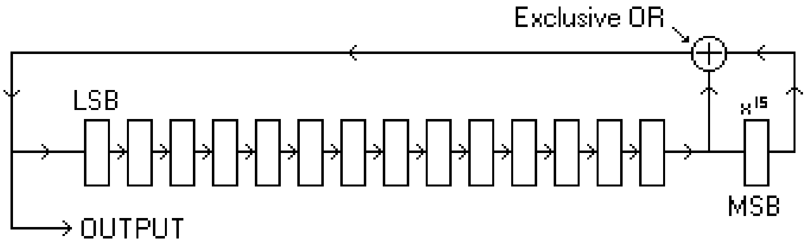


Figure 24

The shift register steps forward one bit at the end of every odd container, and the input of the shift register is sent to the decoder for synchronisation purposes. The CIW is constructed using:

- the contents of the shift register (15 MSBs of CIW);

- the parity of the current frame (LSB of CIW) ("0" for even frames, "1" for odd frames).

The period is $2*(2^{15} - 1)$ = 65 534 containers (8,2 s).

The CIW defines blocks of 8,2 s which delimit the period of validity of successive CWs. The first container in a block is identified by a parity bit and all bits of the shift register equal to "0" except for the LSB of the chain code which is set to "1" (CIW= 0000 0000 0000 0010). The Phase Parity Identifier (PPI) is inverted from block to block and is used to identify the CW related to the current block and the one related to the next block. The PRG for the first container of a block is initialised at the end of the previous block with the CW related to that block, as shown in figure 25.

```
        Start of a new 8,2 s block ——>|
                                      |  ┌——— PPI bit
                  Chain—code bits     |  |     Chain—code bits
     _ _ _  ______________________   |  |   __________________  _ _
                  |       |       |   |  |  |       |       |
                  v       v       v   |  v  v       v       v
          0       0       0          1       1       1       1
       ---+---+---+---+---+---+---+---+---+---+---+---+---+---
                                        ^
        Even block (PPI=0)            |   |  Odd block  (PPI=1)
        ECW refers to current block   |   |  OCW        refers to current
block
        OCW refers to next block          |  ECW        refers to next block
                                      |   |
                                          └── Application of the new CW
                                      |
```

Figure 25: Block-change mechanism

12.3.2 Control word

The control word may be a local control word for testing or for low security services. The method to introduce and/or change the local control word is left to the manufacturer. For normal usage, the control word is generated at the source by the sender, and sent enciphered to the receiver. The control word changes every 65 534 containers but its cryptogram may be transmitted every second.

12.3.3 Synchronisation

Synchronisation is used to prepare and load a new Initialisation Word (IW) in the PRG. This word results from the concatenation of the container identification word CIW , followed by the control word CW and a repetition of the CIW.

Synchronisation happens:

- every 125 µs (at each container), corresponding to a CIW change;

- every 8,2 s (every 65 534 containers), corresponding to a CW change.

Two CWs are used, one each for odd 8,2 s blocks (OCW), and for even 8,2 s blocks (ECW). This mechanism is necessary to prepare the next CW before a new synchronisation command and also to allow a new receiver to obtain the current CW.

Synchronisation makes use of:

- the CIW;

- OCW and ECW;

- the Phase Parity Identifier (PPI) to define the parity of the 8,2 s block and therefore which CW is active.

The synchronisation of the PRG should be performed during the last video octets of each container, which are left unscrambled. The CW and CIW defined during a container are therefore used to define the initialisation word of the PRG for the next container.

12.4 Performance of the PRG

12.4.1 Periodicity of sequences

The PRG can produce (2^{16} * 2^{64}) distinct sequences of octets because of its initialisation method. The highest periodicity of these sequences can be deducted from the behaviour of the polynomials Q, R, S and T.

Therefore, the PRG, which is a combination of the four polynomials Q, R, S and T, can generate sequences of octets which have a periodicity equal to the least common multiple of Tq, Tr, Ts and Tt:

LCM (Tq, Tr, Ts, Tt) = $1.36 * 10^{37}$.

12.4.2 Degenerations

Degenerations occur when one of the groups of registers (Qi, Ri, Si or Ti) remains in the same state. This happens only if all the registers of this group are loaded with 0 or 31 (for Q and R) or with 0 or 127 (for S and T). If only one group of registers is degenerated, we say that we have a single degeneration. If all the groups of registers are degenerated, we call it a fourfold (or complete) degeneration.

Among the 225 possible states of the registers Q0 to Q4 after the initialisation process, we can reference:

- 25 states with the registers loaded with 0 or 31;

- 325 - 25 states shared out among 15 sequences.

The same arguments can apply to the polynomials R, S and T.

It is now possible to enumerate all the degenerated states of the PRG:

- number of states leading to a complete degeneration:

  $2^5 * 2^7 * 2^5 * 2^7 = 2^{24}$;

- number of states leading to a threefold degeneration: around 2^{66}

  $(2^5 * 2^7 * 2^5 * (128^7 - 128) + 2^5 * 2^7 * (128^5 - 128) * 2^7 + 2^5 * (32^7 - 32) * 2^5 * 2^7 + (32^5 - 32) * 2^7 * 2^5 * 2^7)$;

- number of states leading to a double degeneration: around 2^{95};

- number of states leading to a single degeneration: around 2^{124};

- no degeneration: around $2^{144} - 2^{124}$.

12.5 Generating scrambling sequences with the PRG

Figure 26 describes how the PRG is initialised before scrambling a container. This initialisation requires 13 cycles.

For each session, the PRG works as follows:

1) reset the internal state of the PRG ... $X_0 = 0$;

2) initialisation of the PRG by loading the input register with the start-up octets (during this phase, the output is inhibited). Most significant octets are sent first for all words;

3) generation of the scrambling octets delivered by the output register (during this phase, the input register is loaded with the octet 0). The first scrambling octet is obtained when the last initialisation octet has been clocked into the PRG.

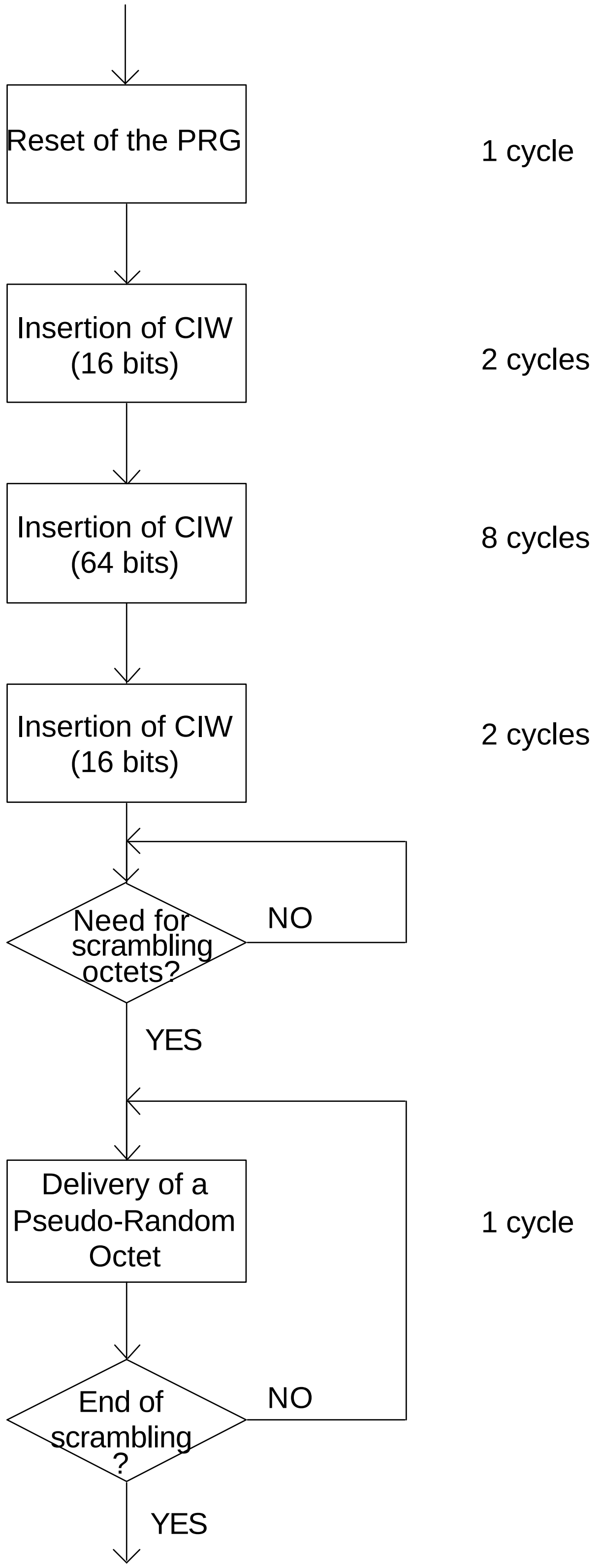


Figure 26

12.6 Conditional access system

Decoders with access control need a security module called the Access Control System (ACS) which may be buried in the decoder, or be detachable. If so, it is connected via an external codec-ACS interface, specified in subclause 12.7. The ACS itself, which embodies (amongst other things) the way of producing the Control Words (CWs), is not defined in this specification. Informative Annex C contains additional information as an example.

12.7 Interface between codec and access control system

12.7.1 Interface signals

The interface comprises the following signals:

- **transmitted data (encoder only).**

Sends ACS data to the encoder for insertion in the CA1 channel of the multiplex;

- **received data (decoder only).**

Sends to the ACS the data extracted by the decoder from the CA1 channel;

- **control words and configuration messages.**

Transmits even and odd control words produced by the ACS to the pseudo-random generator of the encoder or decoder in HDLC frames (defined in subclause 12.7.4). Configuration messages are also sent on this line to indicate the scrambling mode (encoder only);

- **status.**

In an encoder, the data sent in the CA2 channel is sent to the ACS . In a decoder, the line is set to logical level "0". This may be used by the ACS to distinguish encoders from decoders;

- **clock.**

An 8 kHz reference at container repetition rate used to control data exchange on the serial lines defined above. The cyclic ratio should be about 50 %. New data shall appear on the transition from logical "1" to logical "0". Data shall be sampled on the transition from logical "0" to logical "1".

NOTE: Appropriate latches should be provided on the transmission lines to meet the above timing requirements. No specific phase relationship between the clock and the container is specified since the transmission delay between the encoder/decoder and the ACS is not critical.

12.7.2 Electrical and physical interface

This interface derives from CCITT Recommendation V.24 [16]. The electrical interface should conform to CCITT Recommendation V.28 [17]. The connector is the 25-pin connector specified in ISO Standard 2110 [18]. The socket is female on the encoder or decoder, assumed to be a DCE, and male on the ACS, considered as a DTE.

The pin allocation is as follows:

pin	circuit	direction
1	protective ground	
2	transmitted data	ACS to encoder
3	received data	decoder to ACS
7	signal ground	
14	control words	ACS to encoder/decoder
15	clock	encoder/decoder to ACS
16	Status	encoder/decoder to ACS

12.7.3 Encryption modes

Four modes of operation are permitted:

mode 0: no scrambling;

mode 1: all components are scrambled together by a single PRG. The control word is fixed ("local control word");

mode 2: components are scrambled by a single PRG. The control word, changed every block, is provided through the ACS. The ACS indicates also which of the components are subjected to scrambling;

mode 3: components are scrambled by more than one PRG. In this optional mode, control words are provided for every block by the ACS with indication of the relevant components.

If present, control words received from the ACS and relating to blocks sent in mode 0 or 1 are not used by the encoder or the decoder.

The mode of operation is described by bit m_4 of octet J4 according to table 15.

Table 15

m4 in frame 1	m4 in frame 2	Mode
0	0	0
0	1	1
1	0	2
1	1	3

Changes between these modes are effective only at the boundary between two successive 8,2 s blocks. Such changes are announced by bit m_4 in frame 0 used as an update flag:

Between 0,5 s and 1 s before the end of the current block, bit m_4 in frame 0 is set to "1". Bits m_4 in the following frames describe the configuration to be introduced for the next block.

Within 0,5 s after the beginning of the new block, bit m_4 in frame 0 should be reset to "0".

The timing of bits m_4 is controlled by the encoder. Changes in modes should be received from the ACS at least 2 s before the beginning of a new block.

12.7.4 Format of the CWs and configuration messages

CWs and messages are sent in HDLC frames. They include:

- a start flag;

- an address octet, identifying the type of packet transmitted. Possible values are:

  · "00" the corresponding message is:
    * the mode number if the ACS is connected to an encoder;
    * FF hex if the ACS is connected to a decoder;

  · "01" for packets carrying odd control word OCW;

  · "02" for packets carrying even control word ECW;

  · "03" for packets carrying both even and odd control words;

· "04" for packets transmitting a temporary alternative local control word;

· "05" for packets loading a new internal local control word;

· "06" for packets corresponding to "no CW available" (i.e. the access to the corresponding component is not authorised);

"07" for packets identifying unscrambled components;

other packet types are reserved for future use;

- a control octet with:

  · bits 0 to 5: Indication of the multiplex components concerned with the current packet:

  bit 0 set to "1" if T component is concerned;
  bit 1 set to "1" if A component is concerned;
  bit 2 set to "1" if T' component is concerned;
  bit 3 set to "1" if A' component is concerned;
  bit 4 set to "1" if V component is concerned;
  bit 5 reserved for future use;

  in modes 0 and 1, bits 0 to 4 should be ignored by the decoder. They should all be set to "0" in mode 0 and to "1" in mode 1;

  · bits 6 and 7: continuity index of messages sent with a given address (not incremented if the same message is repeated);

- the configuration message, which consists of:

  - 0 octets if the address octet = "06" or "07";
  - 1 octet containing the mode number if the address octet = "00" (b0 = LSB of mode, b1 = MSB of mode, b2 to b7 are reserved);
  - 8 octets for a new local control word;
  - 8 octets if ECW or OCW are transmitted separately;
  - 16 octets if ECW and OCW are transmitted together (ECW first);

- 2 CRC octets, as specified by the HDLC format;

- an end flag.

For each transmitted octet, bit 0 is the least significant bit and is sent first according to HDLC specification. However, octets are sent most significant first.

After the end flag, the HDLC line returns to the "idle" mode. Successive frames must be separated by a minimum guard time of 50 ms and a maximum time-out of 1 s. This minimum activity may be obtained by transmission of packets with address "00".

Manufacturers may decide on the most appropriate ways of storing local control words in the codecs, and of using the remote CW loading messages (addresses "04" and "05").

Annex A (informative): Recommended features

A.1 Introduction

In order that a codec should fully satisfy the intended levels of picture quality, error performance and operational convenience, the attention of manufacturers is drawn to the importance of careful design of the following system elements. These elements are not completely defined by this specification because some of their parameters do not influence the video transmission format and can remain as manufacturer options. The choice of these parameters may, however, have a significant impact on overall codec performance.

Users wishing to establish the subjective performance of a codec may employ the methods recommended by the CCIR (see CCIR Report 1206 [19]), while methods are currently under development for the verification of a codec's design with the options discussed below. Such verification methods may operate by comparison of the output of the codec under test with a standard codec which is known to exercise fully the options below. Alternatively, the comparison test may be made on separate encoders or decoders by incorporating them in a codec pair with a standard decoder or encoder respectively.

A.2 Mode choice

(See subclause 5.1)

Subject to the requirement for a refresh strategy, the coder should take full advantage of the increase in coding efficiency offered by the motion-compensated interframe and the interfield modes.

A.3 Refresh strategy

(See subclause 5.1)

Intrafield refreshing is necessary to limit error propagation and recovery time, but attention is also drawn to the effect on coding efficiency of an increase in the proportion of intrafield blocks.

A.4 Motion estimation

(See subclause 5.4)

The use of motion estimation to the full range and accuracy allowed by the specification is recommended.

A.5 Truncation or rounding of coefficients

(See Clause 6)

Attention is drawn to the fact that coding quality may be affected by the manner in which the quantity C(k, l) is converted to an integer prior to quantisation.

A.6 Buffer regulation

(See Clause 6)

The method of calculating the transmission factor in terms of buffer occupancy should be such that the full capability of the buffer to absorb variations in bit-rate should be exploited for critical picture material.

Depending on the implementation of the encoder, the stripes may be processed at different speeds with possible influences on the exact signification of the BO information sent in each stripe.

The precise synchronisation of the decoder should rely on the information sent in the BOF field which should normally lead to timing information consistent from field to field.

It is however recommended that decoders should accept fluctuations of this information as long as they correspond to less than 5 000 bits.

A.7 Criticality

(See Clause 6)

The codec should take full advantage of the criticality parameter defined in the specification.

A.8 Error concealment

(See subclauses 8.1 and 8.2)

The CRC and the RS code provide information about uncorrected errors that may be used to control a concealment strategy in the decoder, giving improved performance at high bit-error rates.

A.9 Transmission of PAL signals

The PAL signal is decoded to Y C_R C_B for transmission through the codec. It is recommended that this decoding is both complementary and of as high a quality as possible to minimise cross-effects which would spoil the performance of the codec. However, if the signal is to remain in component form at the receiving end, rather than being converted back to PAL, the ideal coding algorithm may not be complementary.

Annex B (informative): Transmission of composite signals using the component tv codec

B.1 Introduction

The bit-rate reduction algorithms used in the 34 Mbit/s codec have been carefully optimised for component video signals sampled according to CCIR Recommendation 601 [1], that is, orthogonally at 13,5 MHz. However, there will for many years be a requirement to use these codecs to transmit composite (PAL, SECAM, NTSC) signals. Clearly, the composite TV signal must be decoded to a form as close as possible, in both structure and content, to a CCIR Recommendation 601 [1] signal. PAL and NTSC decoders produced for general applications are unlikely to meet this requirement.

Initially, composite signals will usually be presented in analogue form, having been transmitted on analogue sections of a mixed network, although in future it is possible that composite signals will appear in digital form.

B.2 PAL and NTSC

Closest similarity to a CCIR Recommendation 601 [1] signal can be achieved by sampling the analogue composite signal at 13,5 MHz and decoding digitally to components using techniques described in BBC Research Department Report BBC RD 1986/2 [20]. This approach has the advantage that the signals transmitted on a network are of the same form irrespective of whether the source was component or composite.

Digital decoding of PAL or NTSC consists of three processes:

- generation of a sampled subcarrier signal;
- separation of luminance and chrominance by filtering;
- demodulation of the chrominance signal.

B.2.1 Complementary decoding

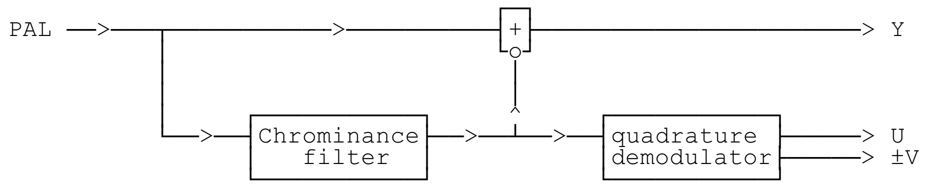


Figure B.1

Many different filters have been proposed for separating chrominance and luminance in the decoder. An important concept is that of a complementary decoder in which the chrominance signal defined by the separation filter is subtracted from the composite signal to give luminance.

Because of the subtractor, the luminance signal contains no information defined as chrominance and vice versa: no information is lost and none is transmitted in both luminance and colour-difference channels. This does not mean that a perfect separation of chrominance and luminance has been achieved: the amount of crosstalk in the decoded signals depends on how good the chrominance filter is at separating real chrominance from luminance. In the simplest case the chrominance filter would be a high-pass or band pass filter - but depending on the application it may be much more complex, including line or field delays or a PAL modifier.

The action of any complementary PAL decoder, no matter how complex the chrominance filter, can be reversed by a simple PAL decoder consisting of a quadrature modulator and an adder, provided the following conditions are met:

- the frequency and phase of the recoding subcarrier must be the same as those of the decoding subcarrier;
- the sense of the V-axis switch must be the same in the recoder as in the decoder;
- the decoded signals must not be subjected to any irreversible processing before recoding.

Methods for transmission of subcarrier phase and V-axis switch are defined in subclause 8.1.3.

B.2.2 Choice of decoding technique

Cross-effects (cross-colour and cross-luminance) in the decoded signals may degrade the performance of the bit-rate reduction processing. Cross-luminance is the worst problem because the moving subcarrier pattern may interfere with the action of the motion compensation circuitry. So the decoder must be of high quality, implying a fairly complex chrominance separation filter.

A complementary decoder will be more appropriate if the objective is to reconstitute the PAL or NTSC signal perfectly at the output of the decoder. Work reported to the EBU has shown that with sampling at 13,5 MHz it is possible to reconstruct PAL signals at the output of the codec with negligible degradation when a high-quality complementary decoder is used at the codec input.

A non-complementary decoder may be more appropriate if the primary objective is to ensure that all signals can be treated after transmission as true component signals (of course signals on such a network will often have to be recoded to PAL). In this case it will still be important to ensure that no information is repeated in luminance and colour-difference signals, since this could give rise to overload on recoding. A modification to the complementary technique could be used where the separated chrominance and luminance signals are subjected to further non-complementary processing specifically to reduce the most objectionable forms of cross-colour and cross-luminance. The implication is that some information will be lost and so it will be important to ensure that the loss is not cumulative if the filters are cascaded.

B.3 SECAM

Decoding of SECAM signals involves the following steps:

- separation of luminance and chrominance;
- demodulation of the chrominance signal; and
- correction of the demodulation delays.

The attention of manufacturers is drawn to the necessity to preserve as much as possible of the chrominance bandwidth and on the need to compensate for the delay in the chrominance path which is due to the necessary vertical processing.

EBU Technical Statement D29-1980 [21] requires that all equipment dealing with SECAM signals be designed for the line-identification system only (so-called SECAM-H).

Furthermore, from an operational point of view, it should be noted that international television contribution networks often mix PAL and SECAM modes of operation, which is permitted with present analogue links. Manufacturers should therefore consider the possibility of offering equipment that will recognise both forms of signals and automatically switch the appropriate decoder/recoder. This feature is of particular importance at the encoder side.

Annex C (informative): Access control management

C.1 Introduction

Decoders with access control need a security module called the Access Control System (ACS) which is connected to the rest of the decoder via a decoder-ACS interface.

The Control Word (CW) is sent, encrypted by a session key, in Entitlement Checking Messages (ECM). Data relevant to the conditional access mode are also present in the ECM. The content of the ECM is protected against falsification by a signing procedure. The Session Key (SK) is secret information stored in the ACS security module. If the authorisation parameters (called "entitlements") received by the decoder are accepted by the ACS, the session key can be used to decrypt the CW.

The entitlements are updated periodically. The session key is common to all users and can be changed under exceptional circumstances. Both entitlements and session keys may be sent to the users using over-addressing methods in Entitlement Management Messages (EMM).

The session keys are sent encrypted with a Distribution Key (DK) specific to the programme supplier. The content of the EMM is protected using a signing procedure as for the ECM.

The ECM and EMM messages are sent in the data multiplex. The entitlement management messages are, in most cases, addressed to individual customers (EMM-U), common to specific groups of customers (EMM-S) or even to the entire audience (EMM-C). They are then identified by a customer address which is a unique address for a message to a particular customer or a shared address for a message to a group of customers. In this case, only those EMM packets which have a correct customer address (unique, shared or collective) cross the decoder-ACS interface. The result of this is that the ACS submits its customer addresses to the decoder's EMM receiving circuit before selection can be implemented.

C.2 Message format

Figure C.1 illustrates the transmission format for ECM and EMM:

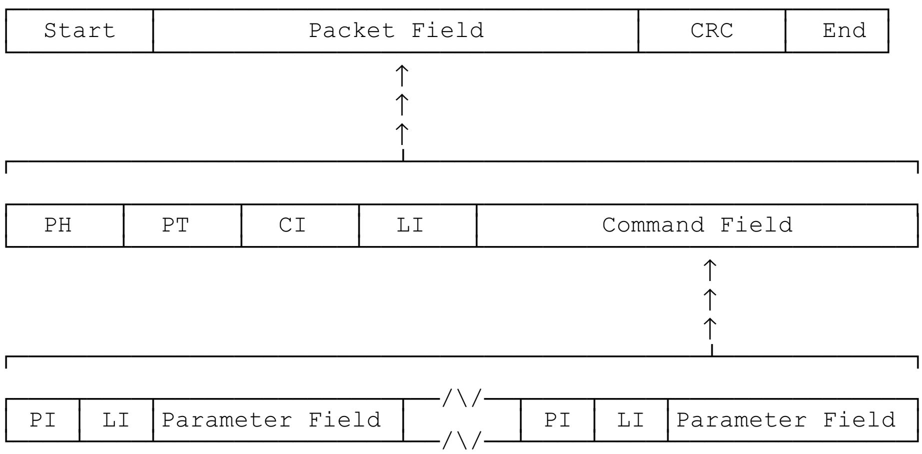


Figure C.1: ECM format

ECM and EMM are inserted in a transport layer defining the strategy for error transmission.

The first two fields, PH and PT, are common to all packets. The Packet Header (PH) contains a field identifying the component concerned with this packet and a 2-bit continuity Index (I) associating packets to the same message. The first packet of a message always has a zero continuity index (I=0), while the subsequent packets have continuity index values in the range [1,3], the value of I being incremented by 1 in modulo 3 sequence each time a packet belonging to the same message is sent (see figure C.2). This index is useful if the size of packets is limited by the transport level.

MSB	Component Identifying Field (6)	I (2)	LSB

Figure C.2: Packet Header (PH)

The Component Identifying Field (CIF) is a bit-field, each bit being associated with a component to indicate if the following message concerns this component

The "Packet Type" (PT) field takes the value 00 hex for ECM packets and the values XX hex, XX hex, XX hex, for EMM-U, EMM-S and EMM-C.

After the PT field, packets contain a message field.

Messages are structured as commands. The beginning of each message is introduced by a 1-octet Command Identifier (CI).

This is followed by a Command Length Indicator (CLI) (1 octet) specifying the length of the ECM message parameter field (from 0 to 255 octets).

Within the message parameter field of the command, each parameter comprises:

- a Parameter Identifier (PI) (1 octet);
- a parameter Length Indicator (LI) (1 octet) specifying the length of the data field associated with the parameter;
- the parameter data field.

The parameters can be combined into a Group Parameter (PG). The length of the group parameter field is also specified by a group Parameter Length Identifier (PLI), (1 octet).

Within a command field, the codes associated with the PG and with isolated PI parameters (not combined within a PG) must be transmitted in ascending order. Similarly, PI parameters which fall within a PG are also transmitted in ascending order.

All messages containing an unrecognised CI field will be ignored. Unrecognised PI fields will be ignored (as will the associated data field), but this will not cause the entire message to be rejected.

The parameter data fields contain an integer number of octets. The most significant octet is the octet containing the Most Significant Bit (MSB). The least significant octet is the octet containing the Least Significant Bit (LSB). The octets of a parameter data field are transmitted most significant octet first and least significant octet last.

All message octets from and including the CI code are transmitted least significant bit first and most significant bit last.

NOTE: PH Packet Header: this contains the continuity index I (2 bits) and the field describing the data channels concerned with access control messages.

PT Packet Type (2 bits).

CI Command Identifier (8 bits): this specifies the format of the parameter field and the type of crypto-algorithm.

CLI Length Indicator for the data field associated with CI (8 bits).

PI Parameter Identifier (8 bits).

LI Length Indicator for the data field associated with PI (8 bits).

C.3 Control words transfer using ECM

In subclause C.3.2, the length and contents defined for the parameter field correspond to the particular implementation given as an example. For other implementations, the length of the defined parameter fields may be extended or shortened provided those parts of the data field currently specified continue to be used. Further parameters may also be introduced provided that they comply with the following rules:

- the PPID parameter must be present in all ECM;

- the HASH parameter must be present in all ECM.

The cryptogram SK(CW) is sent in an entitlement control message (ECM), which is transmitted in the signalling component (J octets of the multiplex). The message also contains data concerning the administration of the control word.

C.3.1 Description of Entitlement Control Messages (ECM)

C.3.1.1 Command Identifier (CI)

The CI identifier comprises 8 bits. It describes the format being used for the parameter field and the type of cryptographic algorithm used for decryption. It is included in all ECM messages and is located in the message synchronising packet.

It contains (see figure C.3):

- T (1 bit) is the toggle bit. This is maintained in the same state as long as the OCW/ECW pair of the ECM message remains unchanged. When the contents of the ECM control words change, the toggle bit changes state. The toggle bit is attached to a given crypto-algorithm type; therefore if ECMs corresponding to two different types of crypto-algorithm are sent, the corresponding toggle bits are kept separate;

- F is the format bit indicating that the following parameter field is either in fixed format without PI LI structure, (F=0), or in variable format with PI LI structure, (F=1). ECMs are in variable format;

- type of crypto-algorithm (6 bits).

MSB	Type of crypto-algorithm (6)	F (2)	T (1)	LSB

Figure C.3: Command Identifier (CI)

C.3.1.2 Command Length Indicator (CLI)

The CLI parameter comprises 8 bits. It indicates the number of octets in the ECM message parameter field. It is always included in an ECM message and follows the CI parameter.

C.3.1.3 Parameter Identifier (PI)

The ECM messages convey all the information specifying the conditions of access to a programme. The same programme can thus be received by customers assigned different entitlements.

Control words are generated by the transmission point and sent encrypted in the ECM messages.

All the parameters listed below are optional within a given ECM message; only those parameters needed to describe the conditions of access to the programme are included.

C.3.1.4 List of parameters available in ECM messages

The list below describes the PI parameters available (values expressed in hexadecimal notation).

PI = 90 hex	Programmer Provider Identifier (PPID) representing the operator generating the ECM. This is used to point to the operation (or management) key of the programme provider.
PI = E1 hex	Broadcast Date (CDATE) + programme theme/level (THEME/LEVEL); included when the broadcast programme is accessible in subscription per theme/level.
PI = E2 hex	Broadcast Date (CDATE) + programme class (LINK); included when the programme is accessible in subscription per link.
PI = E3 hex	Programme Number (PNUMB); included when the programme is accessible in pre-booked pay-per-view per programme.
PI = E4 hex	Programme Number (PNUMB) and programme cost (PPV/P); included when the programme is accessible in impulse pay-per-view per programme.
PI = E5 hex	Programme Number (PNUMB) and cost per time unit of the programme (PP/T); included when the programme is accessible in impulse pay-per-view per time.
PI = E8 hex	Even Control Word cryptogram (ECW); this is used, in conjunction with OCW, in the phase preceding change of key or access criteria. In this case, a PG parameter is also required.
PI = E9 hex	Odd Control Word cryptogram (OCW).
PI = EA hex	Odd and Even Control Word cryptograms (ECW/OCW).
PI = F0 hex	Signature (HASH); guarantees the integrity of all sensitive, clear or encrypted data contained in the ECM parameter field. The ECM cannot be analysed and executed by the security processor unless it finds a match between the transmitted signature and the internally generated result of its own message signature computation. It therefore entails a cryptographic redundancy of the sensitive parameters of the ECM, which ensures that no component of the message has been modified.

The PG parameter, encoded 80 hex, is used when several signatures are required in an ECM message. It frames the parameters concerned. It is used, in particular, when the access configuration is changed in controlled access mode. This occurs if the programme is accessible under certain access conditions during period T (about 8,2 s) and under different conditions during period T+1.

This list of parameters allows five access control modes:

- subscription per level and theme with a validity period. The subscription is valid between two dates. The subscription is also characterised by a level, specifying the highest level of services which can be accessed by a customer (each service has a level reference) and a theme specifying the theme of the services which can be accessed (each service also has a theme reference);

- subscription per link, in which users have access to the service during a period defined by a starting date and an ending date. The subscription is also characterised by a list of classes of services; for each class, the list indicates whether the user is authorised or not (the service is referenced by a class);

- "pre-booked pay-per-view", in which users have access to one or more service items or set of services defined by an initial service number and by a total number of services (set length);

- "pay-per-view per service", in which users get a credit. This credit is debited for the cost of the service when it is accessed. Each service is referenced by its service number and its cost. This method is efficient for impulse pay-per-view; it allows a feed-back on the actual service bought by users;

- "pay-per-view per time", in which users get a credit. This credit is debited on a time basis. Each service is there referenced by its service number and its cost. This mode allows a feedback on the actual service bought by the users.

C.3.1.5 Programme Provider Identifier (PPID)

PI = 90 hex.
LI = 03 hex.
value = programme provider identifier (see figure C.4).
name = PPID.

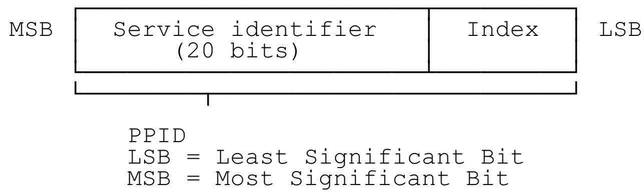


Figure C.4: Programme Provider Identifier (PPID)

This parameter identifies the programme provider generating the ECM. This parameter must be included in the ECM message and points to the key used to encrypt the control words and sign the message. The Least Significant Bits (LSBs) of PPID specify the index of the key. This index is used to modify the value of a key and to distinguish the key in current use from the future key to be used. This index can also be used to define two keys for each programme provider (an operation key reserved for computing control words and a management key for entering entitlements as well as computing control words). The MSB of the index is used to distinguish a management key from an operation key.

C.3.1.6 Broadcast date CDATE + Theme/Level THEME/LEVEL

PI = E1 hex.
LI = 04 hex.
value = broadcast date + theme + level.
name = DATE + THEME/LEVEL.

This parameter is included when a programme is accessible in subscription per theme/level. The first field, CDATE, describes the current date of transmission of the programme covered by subscription. This date is expressed in the form year/month/day. The date is described on two octets; its contents are illustrated in figure C.5.

MSB	Year (7)	Month (4)	Day (5)	LSB

CDATE

00 hex ≤ Year ≤ 7F hex.
01 hex ≤ Month ≤ 0C hex.
01 hex ≤ Day ≤ 1F hex.

Figure C.5: CDATE parameter

This date is relative to the reference year 1980. For example, January 15, 1988 is encoded (in hexadecimal notation):

CDATE	=	102F hex.
Year	=	0001000 (1980 + 8).
Month	=	0001 (January = month No. 1).
Day	=	01111 (15).

The security processor checks that the current date CDATE falls within one of the validity ranges for the subscription entitlements stored.

The second field comprises 16 bits. The eight most significant bits specify the theme of the programme. The eight least significant bits specify the level of the programme. The security processor checks that, for the current date, it has a subscription with the same theme and a level LE greater than or equal to the level of the programme. If this is not the case, access is barred.

The conditions for accessing a programme in subscription per theme/level are therefore:

THEME=TH and LEVEL ≤ LE with TH and LE mandatorily valid on the current date, therefore BD ≤ CDATE ≤ FD.

There are a number of special cases associated with the theme:

- if THEME = FF hex (in the ECM message) the security processor disregards this field and, no matter what the TH value entered in the component, the check on this field will be positive;

- if TH = FF hex (entitlement entered in the security processor), no matter what the THEME parameter transmitted in the ECM message, this field will be disregarded and the verification will be positive.

The Theme/Level parameter is described in figure C.6:

MSB	CDATE (16)	THEME (8)	LEVEL (8)	LSB

Figure C.6: CDATE + THEME/LEVEL parameter

C.3.1.7 Broadcast date CDATE + Programme class LINK

PI	=	E2 hex.
LI	=	03 hex.
value	=	broadcast date + programme class.
name	=	CDATE + LINK.

This parameter is included when a programme is accessible in subscription per link. The first field, CDATE, is as described in glossary. The second parameter field, LINK (8 bits), specifies the class of the programme and points to a bit in the list of customer classes (CUSTWD) sent in the EMM messages (cf. glossary). Each of the bits in the list of classes indicates whether the customer is entitled (bit at 1) or not (bit at 0) to the class concerned. The LINK value specifies the location of the bit in the list of classes; for example, LINK = 0 refers to bit 0, LINK = 1 refers to bit 1, etc. If the LINK value is greater than the CUSTWD length, access is completely barred. Access will be authorised only if the validity period which covers CUSTWD includes CDATE and the bit corresponding to LINK is set to 1 (see figure C.7).

MSB	CDATE (16)	LINK (8)	LSB

Figure C.7: Programme class parameter CDATE + LINK

C.3.1.8 Programme Number (PNUMB)

PI = E3 hex.
LI = 03 hex.
value = programme number.
name = PNUMB.

This parameter is included when a programme is accessible in pre-booked pay-per-view. It describes the programme number PNUMB (3 octets).

In pre-booked pay-per-view mode, access to the programme is allowed only if the programme number is one of the series of programmes stored in the security processor, as follows:

INUMB ≤ PNUMB ≤ FNUMB.

The format of this parameter is given in figure C.8.

MSB	PNUMB (24)	LSB

Figure C.8: PNUMB parameter

C.3.1.9 Programme Number (PNUMB) and Programme cost (PPV/P)

PI = E4 hex.
LI = 05 hex.
value = programme number + programme cost.
name = PNUMB + PPV/P.

This parameter is included when a programme is accessible in impulse pay-per-view per programme. It describes the programme number PNUMB (3 octets) and the cost of the programme PPV/P (2 octets).

In impulse pay-per-view per programme, if the programme has not already been purchased, it will not be accessible unless the cost of the programme is less than or equal to the remaining credit plus the authorised overdraft. Next, the programme number is entered into the security processor and the remaining credit is reduced by the cost of the programme. If the programme has already been acquired, the programme can be accessed.

The structure of this parameter is illustrated in figure C.9.

MSB	Programme number (24) PNUMB	Programme cost (16) PPV/P	LSB

Figure C.9: PNUMB + PPV/P parameter

C.3.1.10 Programme Number (PNUMB) + Cost per time unit PPV/T

PI = E5 hex.
LI = 05 hex.
value = programme number + cost per time unit.
name = PNUMB + PPV/T.

This parameter is included when a programme is accessible in impulse per-pay-view per time. It describes the programme number PNUMB (3 octets) and the cost per time unit PPV/T (2 octets). The 16 bits of PPV/T (see figure C.10) represent the cost of computing control words, expressed in fractions of units.

In pay-per-view per time, access is granted for a given period provided the remaining credit plus the authorised overdraft is greater than or equal to the total cost of the time unit. The remaining credit is then reduced by this cost.

The customer is asked to confirm purchase in order to open any new counter (new PNUMB) or when the counter value exceeds a maximum cost, COUTMAX, locally defined and stored by the customer. In addition, the PIN code will be needed if the impulse pay-per-view lock is set. The customer can stop a purchase in PPV/T mode at any time.

MSB	Programme number (24) PNUMB	Cost per time unit (16) PPV/T	LSB

Figure C.10: Cost per time unit parameter PNUMB + PPV/T

C.3.1.11 Even Control Word cryptogram (ECW)

PI = E8 hex.
LI = 08 hex.
value = even control word cryptogram.
name = ECW.

This parameter describes the cryptogram of the even control word ECW (see figure C.11) which is in use when the PPI is set to 0. The control word cryptogram is obtained from the encryption of the control word by the operation key indicated by PPID.

It can be used (in conjunction with OCW) in place of ECW/OCW where there is a change of access conditions from one phase to another (change of PPID, programme number, etc.). In this case, a group parameter PG is also needed.

MSB	ECW (64)	LSB

Figure C.11: Even Control Word cryptogram (ECW)

C.3.1.12 Odd Control Word cryptogram (OCW)

PI = E9 hex.
LI = 08 hex.
value = odd control word cryptogram.
name = OCW.

This parameter describes the cryptogram of the Odd Control Word (OCW) (see figure C.12) which is in use when the PPI is set to 1. The control word cryptogram is obtained from the encryption of the control word by the operation key indicated by PPID.

It can be used (in conjunction with ECW) in place of ECW/OCW when there is a change of access conditions from one phase to another. In this case, a group parameter PG is also needed.

MSB	OCW (64)	LSB

Figure C.12: Odd Control Word cryptogram (OCW)

C.3.1.13 Odd and Even Control Word cryptograms (ECW/OCW)

PI = EA hex.
LI = 10 hex.
value = odd and even control word cryptograms.
name = ECW/OCW.

This parameters is composed of two fields containing the cryptograms for two control words (see figure C.13). The first field contains the cryptogram of the control word in use when the PPI set to 0 (ECW). The second field contains the cryptogram of the control in use when the PPI is set to 1 (OCW). The cryptograms are obtained from the encryption of the control words by the service key indicated by PPID.

The cryptograms are 8 octets long.

MSB	ECW (64)	OCW (64)	LSB

Figure C.13: Odd and Even Control Word cryptograms (ECW/OCW)

C.3.1.14 HASH signature

PI = F0 hex.
LI = 08 hex.
value = signature of sensitive parameters in the ECM message.
name = HASH.

The presence of this parameter is mandatory in ECM messages (see figure C.14). It gives the signature of the sensitive parameters of the message and assures the security processor that the message has not been modified.

The signature mechanism uses the service key indicated by PPID.

The parameters involved in the signature mechanism are the PI parameters such that D8 hex $\leq$ PI $\leq$ EA hex.

MSB	HASH (64)	LSB

Figure C.14: Signature parameter

C.3.2 Description of ECM messages with examples

C.3.2.1 Subscription per theme/level

Examples below take no account of PH and PT octets for the estimation of the ECM size because they depend on the needs of the transport layer.

The ECM messages contain:

- the programme provider identifier PPID;
- the current date + theme/level of the programme CDATE + THEME/LEVEL;
- the control word cryptograms ECW/OCW;
- the message signature HASH.

The ECM message is 43 octets long. The structure of the ECM message is illustrated in figure C.15.

PH	PT	CI	27	PI	03	PPID	PI	04	CDATE + THEME/LEVEL	PI	10	ECW/OCW	PI	08	HASH
8	8	8	8	8	8	24	8	8	32	8	8	128	8	8	64

Length of ECM message = 43 octets. underlined numbers are in hexadecimal.

Figure C.15: ECM message for subscription per theme/level

C.3.2.2 Impulse pay-per-view per programme

The ECM message contains:

- the programme provider identifier PPID;
- the programme number and programme cost PNUMB + PPV/P;
- the control word cryptograms ECW/OCW;
- the message signature HASH.

The length of the ECM is 44 octets. Its structure is described in figure C.16.

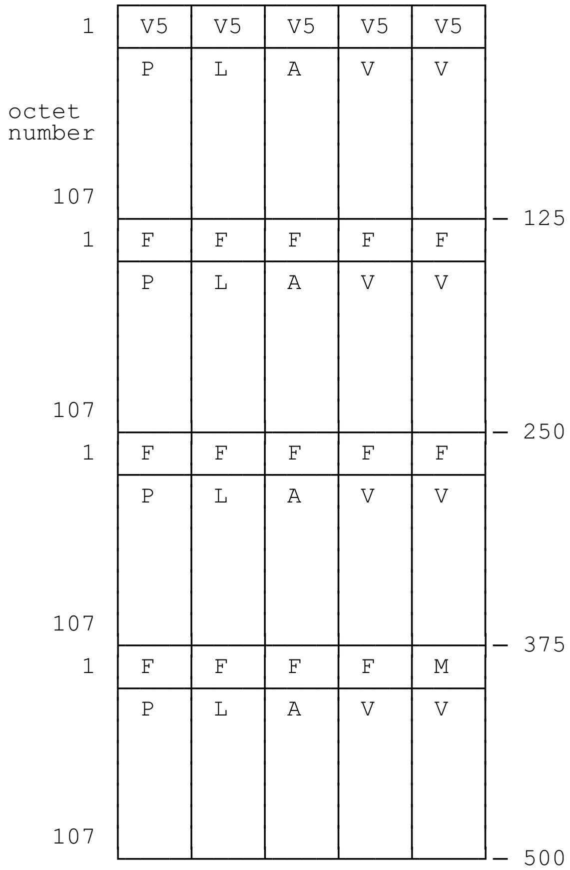
PH	PT	CI	28	PI	03	PPID	PI	05	PNUMB + PPV/P	PI	10	ECW/OCW	PI	08	HASH
8	8	8	8	8	8	24	8	8	40	8	8	128	8	8	64

Length of ECM message = 44 octets. underlined numbers are in hexadecimal.

Figure C.16: ECM message for impulse pay-per-view per programme

Annex D (informative): Network adaptation to SDH VC-2 5C

If the TU-2 5c of the SDH is used for transmission, the TV container is mapped into the VC-2 5c by dropping the two R octets and mapping the remaining 530 octets into one frame of the VC-2 5c as shown in figure D.1. The remaining capacity may be used for transmitting the FAWs of a preceding PDH section.



V5 = VC-2 path overhead.
P,L,A,V = TV container - see subclause 10.2.
M = octet reserved for transmission of M octets for DQDB.
F = octet reserved for transmission of CCITT Recommendation G.751 [2] FAW.

Figure D.1: Structure of the VC-2 5c in a 500 µs multiframe

Some network operators currently monitor the CCITT Recommendation G.751 [2] Frame Alignment Word (FAW) to operate protection switching arrangements. For the protection switching to operate correctly in mixed plesiochronous and SDH connections, the CCITT Recommendation G.751 [2] FAWs from a PDH section must be carried without modification through a SDH section.

The transmission of the 10-bit CCITT Recommendation G.751 [2] FAWs requires 1790/(16 * 8) or about 13,98 octets per 500 µs multiframe. The structure shown in figure 19 gives 14 F octets per 500 µs multiframe.

Justification is performed by storing incoming CCITT Recommendation G.751 [2] FAWs in a buffer and reading out the contents of the buffer in octets into the time-slots F in figure 19. When the buffer is empty, ten bits representing the inverse of the CCITT Recommendation G.751 [2] FAW are inserted into the next ten bit-spaces.

History

Document history	
November 1992	First Edition
February 1996	Converted into Adobe Acrobat Portable Document Format (PDF)