SCRAMBLED TELEVISION SOUND SIGNALS

This invention relates to the scrambling and descrambling of television signals which contain scrambled sound and/or data information.

A method is known of generating vision scrambling control words for the line-by-line scrambling or descrambling of the vision components of a television signal, in which control data having a rate which is low relative to that of the line rate of the television signal is employed to control the generation of the vision scrambling control word for each line of said vision components.

A method of the above type is known where each line of the vision components of a television signal is scrambled, by cutting the line and changing the cut-point for each line. This is done in a random manner by a locally generated random sequence at the transmission source and a corresponding random sequence locally generated in the television receiver. Both random sequences are periodically reset by control data at a rate which is low relative to that of the line rate of the television signal which control data is transmitted with the television signal. Such a method provides a relatively secure scrambling system.

It is a first object of the invention to provide a method of the above type which also makes provision for the scrambling and descrambling of sound/data signals.

The invention provides in one aspect a method of generating scrambling control words for the line-by-line scrambling or descrambling of the vision components of a television signal, in which control data having a rate which is low relative to that of the line rate of the television signal is employed to control the generation of the vision scrambling control word for each line of said vision components, and said television signal additionally contains digitally modulated sound and/or data information multiplexed into blocks, said control data also being employed to control the generation of block scrambling control words one for each block of said sound/data information, for controlling the scrambling or descrambling of each of those blocks required to be so

scrambled or descrambled.

The above method has the distinct advantage that the control data may be employed not only to control the generation of the vision scrambling control words but also to control the generation of the sound/data scrambling control words and thus it is not necessary to transmit separate control data over separate channels for the vision and sound/data components respectively.

Where each block is longer than the digital components contained in two lines, the means generating each control word can additionally generate, during each line period, a part of a block scrambling control word, each block scrambling control word being assembled from the parts in a number of lines preceding that line in which the associated block commences which number corresponds to the nearest whole number which is less than that number of lines in a block.

Preferably each block scrambling control word resets a pseudo-random binary sequence at the start of each such block for the modification of said sequence to the data stream in that block for the purpose of scrambling or descrambling.

Each block scrambling control word can be stored together with the block with which it is associated. Each block scrambling control word and associated block can be subsequently read and the block interrogated to determine whether the block requires descrambling or not.

The invention also provides in a second aspect a television receiver for receiving and processing scrambled vision components and scrambled digitally modulated sound and/or data information, comprising means for additionally receiving control data which has a rate which is low relative to that of the line rate of said television signal, generating means for generating vision scrambling control words for the line-by-line descrambling of the said vision components, said generating means producing a control word for each line of said vision components which generating means is periodically reset by said control data, and the receiver additionally comprising generating means for generating block scrambling control words, one for each block of sound/data information, for controlling the descrambling of each block

requiring descrambling, and which is also periodically reset by said control data.

With a receiver where each block is longer than the digital components in two lines the generating means for generating the block scrambling control words can comprise a generator producing, during a line period, a part of a block scrambling control word, said block scrambling control word being formed by combining the said parts produced during a number of lines which number is the nearest whole number of line periods which is less than the number of lines in a block.

The receiver preferably further comprises a store in which each block scrambling control word is stored together with the block with which it is associated. It may also include means for selectively reading each block and associated control word from said store and means for interrogating the block to determine whether said block requires descrambling or not. The selectively read control word may then be used to reset a block descrambling generator at the start of a block, which generator produces during said block a pseudo-random binary sequence which is applied together with said block to a descrambler wherein the bit stream of said block is modified by said binary sequence to achieve descrambling. With such a receiver the block descrambling generator may be inhibited when said block does not require descrambling.

In a further aspect the invention provides a television receiver for receiving a television signal containing scrambled digitally modulated sound and/or data information in blocks which is time multiplexed with vision information, and comprising descrambling means for generating descrambled sound/data signals from the received television signal, and means for additionally receiving control data which has a rate which is low relative to that of the line rate of the television signal for use in descrambling, characterised by control word generating means responsive to the control data for generating a control word for each block, means for storing each control word together with the block with which it is associated, and means for conditioning the descrambling means for descrambling each block in response to the associated stored control word.

In a preferred example to be described, the control word generating means generates a pseudo-random binary sequence, which is periodically reset in response to the received control data. The descrambling means comprises a second pseudo-random binary sequence generator, and a combining circuit for combining the output of the said second generator bit-by-bit with the bits of the sound/data blocks to effect descrambling. The said second generator is reset for each block to a value dependent upon the associated control word. In this way the second generator is able to operate at the output sound/data bit rate, which can be very much lower than the input rate in the received signal, while retaining synchronism with the sound/data information even in unfavourable circumstances.

The invention also provides a method of scrambling or descrambling a television signal containing scrambled digitally modulated sound and/or data information in blocks which is time multiplexed with vision information, comprising the steps of providing control data which has a relatively low rate, producing a first binary sequence in response to said control data, which first binary sequence has a rate which is higher than that of said control data, producing a second binary sequence which is pseudo-random and which is periodically set from said first binary sequence, said second binary sequence having a rate which is higher than that of said first binary sequence, and employing said second binary sequence for the scrambling or descrambling of blocks of the sound/data information.

The above and other features of the invention will now be described, by way of example, with reference to the following description and accompanying drawings in which:-

Figure 1 is a block diagram of a television receiver for use with the present invention, and

Figure 2 is a block diagram of a modification of the television receiver shown in Figure 1.

In the diagram of Figure 1 the reference 1 indicates a dish aerial for receiving off-air transmissions of a television signal from a direct broadcasting satellite (DBS), the received signals being of the C-MAC Packet Type conforming to the proposed European Broadcasting Union (EBU) standard for satellite broadcasting present in the EBU document Com. T481 dated April 1983 which was subsequently updated in the EBU Draft New Report "Television Standards for 625-line 12 GHz Satellite Broadcasting", SPB 284 dated June 1983. The received C-MAC Packet signals are applied to an input 2 of a television receiver which is connected to circuits 3 for processing the incoming signal to produce at a first output V a vision signal, and at a second output D the data bursts of the C-MAC Packet signal containing the sound and/or data information in multiplexed block (packet) form. From the above EBU documents it will be seen that the television signal is time multiplexed during a line period. The vision signal is in component form (a chrominance component and a luminance component) and may be scrambled, whilst the sound/data information is transmitted in packets of 751 bits,

195 bits out of 203 bits in the data burst of each line contributing to a packet or packets. Thus each sound/data packet occupies approximately 3.85 lines of data burst. The vision signal is applied to circuits (not shown) for further processing including descrambling to produce a television display from the incoming television signal.

The separated data bursts from terminal D are applied to a packet demultiplexer circuit 4 where the data bursts are assembled into their individual packets, the packet-by-packet output P of this circuit being applied to a first input of an adder 5. An output E of the packet demultiplexer circuit 4 provides low rate encrypted control data (e.g. once per second) which is passed from the transmission source to the receiver via a securely encrypted data channel in the off-air transmission, and may form part of the data burst. This encrypted data is applied to the inputs of a decryption sub-system 6 which may be in the form of a plastic card (of a similar size to a credit card) which a subscriber obtains separately from the receiver and which is inserted into an appropriate aperture in the television receiver, the aperture containing suitable connections to make contact with corresponding contacts on the card. The card carries an integrated circuit which decrypts the encrypted control data and produces a control sequence, preferably a pseudo random bit sequence (P.R.B.S.) which is periodically reset by the decrypted control data. In the illustrated example the P.R.B.S. comprises 16 bits per television line.

The output of the decryption sub-system 6 is applied to the input of a sound/data descrambling control word generator 7 and is also applied to a terminal VS from which the first 8 bits per line are taken for use as the vision descrambling control word for each line of the vision signal, which signal may have been scrambled by being cut at one out of 256 possible positions. The descrambling control word generator 7 takes the remaining 8 bits per line and assembles these bits from three successive lines to form a 24 bit sound/data packet descrambling control word ($\underline{x}$) which is associated with a packet which commences in the line following the third of these lines. For instance, if a packet were to start during the

data burst in line 12 then the required 24 bits would be derived during the 8 further bits generated during lines 9, 10 and 11. This packet descrambling control word from the control word generator 7 is applied to the second input of the adder 5, the output of which is applied to a main packet buffer store 8. Synchronism between the packet descrambling control word and its associated packet is preserved by storing the value of the descrambling control word for a particular packet, together with its associated sound/data packet in the main packet buffer store 8.

The packet buffer store 8 operates as a FIFO (first-in-first-out) and one packet and its associated descrambling control word are picked out for descrambling one at a time by a "next packet" selector 9, an output of which is applied to the selector input S of the buffer store 8 for this purpose. The selected packet is conveyed by the packet selector 9 via a further output to a packet identification circuit 10 to check the Packet Type (PT) byte in the packet header in order to establish whether the packet content is sound/data signal itself or sound/data control information, as interpretation packets (BI) are not scrambled and hence the descrambling arrangement must be inhibited when such an interpretation packet is identified by the identification circuit 10 which then does not produce an enable signal at its output. For a scrambled sound/data signal packet the descrambling arrangement must operate.

A further output of the packet selector 9 is connected to a descrambling control word register 11 which is loaded with the descrambling control word ($\underline{x}$) associated with a packet when the packet content is to be applied from the packet selector 9 to a descrambler 12. Scrambling of the sound/data signal is achieved at its transmission source by adding, modulo-two, a pseudo-random binary sequence (P.R.B.S.) produced by a suitable generator bit by bit to the serialised digital bit stream of the sound/data signal. In the receiver sound/data descrambling is achieved by adding, modulo-two, the same P.R.B.S. generated by a local generator. This local generator is synchronised to the local data stream with the same relationship as that held by the P.R.B.S. generator at the transmission source. Security of the system is obtained by

resetting the P.R.B.S. generator at the transmission source at intervals, namely at the start of each packet to a particular (variable) point in its sequence, the corresponding generator in the receiver being correspondingly reset, or initialised.

In Figure 1 a P.R.B.S. generator 13 provides the serial sequence for descrambling which is applied to a further input of the descrambler 12 (which takes the form of an exclusive OR gate) to be added bit by bit, modulo-two, to the data stream of a packet emerging from the packet buffer store 8. The P.R.B.S. generator 13 is reset at packet rate by the packet descrambling control word (x) from the descrambling control word register 11 such that the P.R.B.S. generator 13 is reset to a value set by the packet descrambling control word at the start of each packet.

The output of the packet identification circuit 10 enables the P.R.B.S. generator 13 when descrambling is required, but absence of an enable signal at this output inhibits the operation of this generator so that descrambling is not performed.

The descrambled sound/data information from the descrambler 12 is applied to a connecting terminal 14 which forms the output to error protection and other circuits for the further processing of the packet information to recover the sound/data information in the receiver.

It will be seen that the P.R.B.S. generator 13 operates at the bit rate of the sound/data output at terminal 14 and does not have to operate at the very high bit rate of the input packet data. Nevertheless it retains synchronism with the received sound/data packets.

In the arrangement of Figure 1 a high-speed data transfer of 250 Kbits per second is used to carry the 16 bits per line between the decryption sub-system 6 and the vision and sound descrambling circuits of the television receiver. In some cases it may be preferred not to employ such a high data bit rate across the interface between the sub-system and the receiver, in which case data must be transferred at a lower speed, for instance over a so-called D^2B digital data bus. A receiver for such a lower speed data transfer is shown in Figure 2 where corresponding components are given the same reference as are employed in Figure 1.

In Figure 2 the output E from the packet demultiplexer 4 is applied to a decryption sub-system 15 again of the card type. However, the sub-system in the case does not directly generate the required P.R.B.S. but produces at its output the decrypted control data at the low rate (say once per second) and conveys it over the D^2B bus 16 to a P.R.B.S. generator 17 in the receiver which generates the required 16 bits per television line. The decrypted control data is used periodically (e.g. once per second) to 'seed' or reset the contents of the P.R.B.S. generator 17. The output of this generator 17 is applied to the terminal VS and to the input of the packet descrambling control word generator 7 in the same manner as in Figure 1, the operation of the remaining parts of Figure 2 being the same as that for Figure 1.

Although Figures 1 and 2 are respectively concerned with the relatively high and low speed transfer of data between the sub-system and the receiver it may be required to produce a receiver capable of both modes of operation. In such a case the two modes could be combined in one receiver and the operations would be compatible if it is designed so that data transferred via the higher-speed interface (if present) overwrites that internally generated within the receiver.

In the above description reference has been made to the descrambling of the vision and sound/data signals in the receiver and it will be realised that substantially the same techniques may be employed at the transmission source for the scrambling of these signals.

* C L M S *

CLAIMS

1. A television receiver for receiving a television signal containing scrambled digitally modulated sound and/or data information in blocks which is time multiplexed with vision information, and comprising descrambling means for generating descrambled sound/data signals from the received television signal, and means for additionally receiving control data which has a rate which is low relative to that of the line rate of the television signal for use in descrambling, characterised by control word generating means responsive to the control data for generating a control word for each block, means for storing each control word together with the block with which it is associated, and means for conditioning the descrambling means for descrambling each block in response to the associated stored control word.

2. A television receiver as claimed in claim 1, in which the control word generating means generates a pseudo-random binary sequence.

3. A television receiver as claimed in claim 2, in which the pseudo-random binary sequence generated by the control word generating means is periodically reset in response to the received control data.

4. A television receiver as claimed in claim 1, 2 or 3, in which each block is longer than the digital sound/data components contained in two lines, and, during each line, part of a block scrambling control word is generated, each control word being assembled from the parts in a plurality of lines preceding that line in which the associated block commences.

5. A television receiver as claimed in any preceding claim, including means for interrogating each block to determine whether the block needs descrambling, and, if not, inhibiting the descrambling operation of the descrambling means.

* C L M S *

6. A television receiver as claimed in any preceding claim, in which the descrambling means comprises a pseudo-random binary sequence generator, and means for combining the generator output bit-by-bit with the bits of the sound/data information to effect descrambling.

7. A television receiver as claimed in claim 6, in which the pseudo-random sequence generator is conditioned for each block by being reset to a value dependent upon the associated control word.

8. A method of scrambling or descrambling a television signal containing scrambled digitally modulated sound and/or data information in blocks which is time multiplexed with vision information, comprising the steps of providing control data which has a relatively low rate, producing a first binary sequence in response to said control data, which first binary sequence has a rate which is higher than that of said control data, producing a second binary sequence which is pseudo-random and which is periodically set from said binary sequence, said second binary sequence having a rate which is higher than that of said first binary sequence, and employing said second binary sequence for the scrambling or descrambling of blocks of the sound/data information.

9. A method as claimed in Claim 8, in which said first binary sequence is also pseudo-random and is periodically set by said control data.

10. A method as claimed in Claim 8 or Claim 9, in which the second binary sequence has a bit rate which corresponds to the bit rate of the blocks to be scrambled or descrambled at the point of scrambling or descrambling.

11. A method of generating scrambling control words for the line-by-line scrambling or descrambling of the vision components of a television signal, in which control data having a rate which is low relative to that of the line rate of the television signal is employed to control the generation of the vision scrambling control

* C L M S *

word for each line of said vision components, and said television signal additionally contains digitally modulated sound and/or data information multiplexed into blocks, said control data also being employed to control the generation of block scrambling control words one for each block of said sound/data information, for controlling the scrambling or descrambling of each of those blocks required to be so scrambled or descrambled.

12. A method as claimed in Claim 11, in which each block is longer than the digital components contained in two lines, and, during each line period, a part of a block scrambling control word is generated, each block scrambling control word being assembled from the parts in a plurality of lines preceding that line in which the associated block commences.

13. A method as claimed in Claim 11 or 12, in which each block scrambling control word resets a pseudo-random binary sequence at the start of each such block for the modification of said sequence to the data stream in that block for the purpose of scrambling or descrambling.

14. A method as claimed in Claim 11, 12 or 13, in which each block scrambling control word is stored together with the block with which it is associated.

15. A method as claimed in Claim 14, in which each block scrambling control word and associated block is subsequently read and the block interrogated to determine whether the block requires descrambling.

16. A television receiver for receiving and processing scrambled vision components and scrambled digitally modulated sound and/or data information, comprising means for additionally receiving control data which has a rate which is low relative to that of the line rate of said television signal, generating means for generating vision scrambling control words for the line-by-line descrambling of the said vision components, said generating means producing a control word for each line of said vision components which

* C L M S *

generating means is periodically reset by said control data, and the receiver additionally comprising generating means for generating block scrambling control words, one for each block of sound/data information, for controlling the descrambling of each block requiring descrambling, and which is also periodically reset by said control data.

17. A television receiver as claimed in Claim 16, where each block is longer than the digital components contained in two lines, and in which the generating means for generating the block scrambling control words comprises a generator producing, during a line period, a part of a block scrambling control word, said block scrambling control word being formed by combining the said parts produced during a plurality of lines preceding that line in which the associated block commences.

18. A receiver as claimed in Claim 16 or 17, including a store in which each block scrambling control word is stored together with the block with which it is associated.

19. A receiver as claimed in Claim 18, including means for selectively reading each block and associated control word from said store and means for interrogating the block to determine whether said block requires descrambling or not, and if not, for inhibiting the descrambling.

20. A receiver as claimed in Claim 18 or 19, in which the selectively read control word is used to reset a block descrambling generator at the start of a block, which generator produces during said block a pseudo-random binary sequence which is applied together with said block to a descrambler wherein the bit stream of said block is modified by said binary sequence to achieve descrambling.

21. A television receiver substantially as herein described with reference to either of the figures of the drawings.

* C L M S *

22. A method of generating scrambling control words for the line-by-line scrambling or descrambling of the vision components of a television signal, substantially as herein described with reference to the drawings.