

Description

The invention relates to a television transmission system for the transmission and reception of a television signal in which the vision components are scrambled to allow only for their authorised reception, a vision scrambling or de-scrambling key being provided for the respective line-by-line scrambling prior to transmission or de-scrambling on reception of said vision components, said vision scrambling/de-scrambling key comprising a first pulse signal having a first pseudo random configuration locally generated at a first rate which corresponds to that of the line frequency, the first pulse signal being periodically set, in response to random control data which accompanies said television signal having a rate which is low compared with that of the line frequency, to a particular pulse configuration which first pulse signal thereafter is stepped under the control of a first clock signal to produce a fresh scrambling/de-scrambling word per television line in accordance with said first pseudo random configuration, said television signal additionally containing digitally modulated sound or data components which are packet multiplexed such that individual packets represent a sound or a data component which packets are time division multiplexed within periods allotted in said television signal. The invention also relates to transmission and receiving equipment for use with such a system.

A system 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 vision scrambling key at the transmission source and a corresponding random vision de-scrambling key locally generated in the television receiver. Both scrambling and de-scrambling keys 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 for the vision components.

With the above known system no provision is made for scrambling or de-scrambling either sound or data signals transmitted with the vision components of the television signal and there are circumstances where such scrambling could be required to prevent their unauthorised reception.

It is an object of the invention to provide a television transmission system where the scrambling or de-scrambling of sound or data signals may readily be achieved.

The invention provides from a first aspect a television transmission system for the transmission and reception of a television signal in which the vision components are scrambled to allow only for their authorised reception, a vision scrambling or de-scrambling key being provided for the respective line-by-line scrambling prior to transmission or de-scrambling on reception of

said vision components, said vision scrambling/de-scrambling key comprising a first pulse signal having a first pseudo random configuration locally generated at a first rate which corresponds to that of the line frequency, the first pulse signal being periodically set, in response to random control data which accompanies said television signal having a rate which is low compared with that of the line frequency, to a particular pulse configuration which first pulse signal thereafter is stepped under the control of a first clock signal to produce a fresh scrambling/de-scrambling word per television line in accordance with said first pseudo random configuration, said television signal additionally containing digitally modulated sounder data components which are packet multiplexed such that individual packets represent a sound or a data component which packets are time division multiplexed within periods allotted in said television signal, characterised in that one of said sound/data components is scrambled to allow only for authorised reception, a packet scrambling or de-scrambling key being provided for the packets of the sound/data component which is to be respectively scrambled prior to transmission or de-scrambled on reception, said packet scrambling/de-scrambling key comprising a second pulse signal having a second pseudo random configuration locally generated at a second rate corresponding to the rate at which said packets appear either prior to or after multiplexing prior to transmission or demultiplexing on reception, the second pulse signal being periodically set, in response to said random control data, to a particular pulse configuration which differs each time the second pulse signal is set and thereafter is stepped under the control of a second clock signal in accordance with said second pseudo random configuration.

Where further of said sound/data components are scrambled to allow only for their authorised reception, a separate packet scrambling or de-scrambling key may be provided for each further sound/data component which is to be respectively scrambled prior to transmission or de-scrambled on reception. In order to produce these separate packet scrambling/de-scrambling keys the system may further include further second pulse signals each having a pseudo random configuration locally generated at the rates at which the packets of the further sound/data components appear either prior to or after multiplexing prior to transmission or demultiplexing on reception, which further second pulse signals are periodically set, in response to said random control data, to respective particular pulse configurations which differ each time the further second pulse signals are set and thereafter are stepped under the control of said second clock signal in accordance with their pseudo random configuration.

A third pulse signal having a third pseudo random configuration may be produced at a rate less than that of said line frequency but greater than that of said random control data, said third

pulse signal being periodically set in response to said random control data, to a particular pulse configuration which differs each time the third pulse signal is set and thereafter is stepped under the control of a third clock signal in accordance with said third pseudo random configuration, the or each second pulse signal being periodically set by said third pulse signal. The use of such a third pulse signal provides an intermediate frequency rate which may have particular benefits. The rate of this third pulse signal may conveniently correspond to the frame frequency of the television signal.

The random control data may be conveyed in encrypted form as an encryption key which forms part of the transmission with said sound/data components, this giving added security to the system.

The invention also provides television transmission equipment for use with the above transmission system, said equipment comprising a source of vision components, means for performing line-by-line scrambling of said vision components under the control of a vision scrambling key to allow only for their authorised reception, means for generating random control data at a rate which is low compared with the line frequency of said television signal, means for generating a first pulse signal having a first pseudo random configuration at a first rate corresponding to that of said line frequency which first pulse signal forms the vision scrambling key, means for periodically setting said first pulse signal, in response to said random control data, to a particular pulse configuration which first pulse signal is thereafter stepped under the control of a first clock signal to produce a fresh scrambling word per television line in accordance with said first pseudo random configuration, and means for applying said scrambled vision components as part of a television signal to a transmission medium, sources of digitally modulated sound or data components, and means for packet multiplexing said sound/data components such that individual packets represent a sound or a data component which packets are multiplexed within allotted periods, characterised in that said equipment additionally comprises means for scrambling one of said sound/data components under the control of a packet scrambling key to allow only for authorised reception, means for generating a second pulse signal having a second pseudo random configuration at a second rate corresponding to the rate at which said packets appear, either prior to or after multiplexing, which second pulse signal forms said packet scrambling key, means for periodically setting said second pulse signal in response to said random control data to a particular pulse configuration which differs each time the second pulse signal is set and thereafter is stepped under the control of a second clock signal in accordance with said second pseudo random configuration, and means for applying said packet multiplexed sound/data components as part of said television signal to the transmission medium.

Such transmission equipment may additionally comprise means for scrambling further of said sound/data components each under the control of a separate packet scrambling key to allow only for authorised reception, means for generating further second pulse signals each having a pseudo random configuration at rates at which the packets of the further sound/data components appear either prior to or after multiplexing which further second pulse signal form the respective separate packet scrambling keys, means for periodically setting said further second pulse signals, in response to said random control data, to particular pulse configurations which differ each time the further second pulse signals are set and thereafter are stepped under the control of said second clock signal in accordance with their respective pseudo random configurations.

Further generating means may be provided for generating a third pulse signal having a third pseudo random configuration at a rate which is less than that of the line frequency but greater than that of said random control data, means for periodically setting said third pulse signal, in response to said random control data, to a particular pulse configuration which differs each time the third pulse signal is set and thereafter is stepped under the control of a third clock signal in accordance with said third pseudo random configuration, and means for periodically setting the or each further second pulse signal by said third pulse signal. This means for generating said third pulse signal may generate said third pulse signal at a rate corresponding to the frame frequency of said television signal.

With transmission equipment as above means may also be provided for encrypting said random control data to form an encryption key which encryption key forms one of the sound/data components.

The invention further provides television receiver equipment for use with the above transmission system which comprises means for receiving said television signal and for deriving the scrambled vision components therefrom, means for performing line-by-line de-scrambling of said scrambled vision components under the control of a vision de-scrambling key, means for generating a first pulse signal having a first pseudo random configuration at a first rate corresponding to that of the line frequency which first pulse signal forms said vision de-scrambling key, means for periodically setting said first pulse signal, in response to received random control data, which control data has a rate which is low compared with that of the line frequency, to a particular pulse configuration which first pulse signal thereafter is stepped under the control of a first clock signal to produce a fresh de-scrambling word per television line in accordance with said first pseudo random configuration, said television signal additionally containing digitally modulated sound or data components which are packet multiplexed such that individual packets represent a sound or a data component which packets are time division multiplexed within

periods allotted in said television signal, characterised in that one of said sound/data components is scrambled to allow only for authorised reception, said equipment additionally comprising means for deriving said one scrambled sound/data component from said received television signal, means for performing descrambling of said scrambled sound/data component under the control of a packet de-scrambling key, means for generating a second pulse signal having a second pseudo random configuration at a second rate corresponding to the rate at which said packets appear, either prior to or after de-multiplexing, which second pulse forms said packet de-scrambling key, means for periodically setting said second pulse signal, in response to said received random control data, to a particular pulse configuration which differs each time the second pulse signal is set and thereafter is stepped under the control of a second clock signal in accordance with said second pseudo random configuration.

Where further of the sound/data components are scrambled to allow only for their authorised reception, the equipment may additionally comprise means for deriving said further scrambled sound/data components from said received television signal, means for performing descrambling of said further scrambled sound/data components under the control of separate packet de-scrambling keys, means for generating further second pulse signals each having a pseudo random configuration at rates at which the packets of the further scrambled sound/data components appear, either prior to or after demultiplexing, which further second pulse signals form the respective separate packet de-scrambling keys, means for periodically setting said further second pulse signals, in response to said received random control data, to particular pulse configurations which differ each time the further second pulse signals are set and thereafter are stepped under the control of said second clock signal in accordance with their respective pseudo random configurations.

Such receiver equipment may additionally comprise means for generating a third pulse signal having a third pseudo random configuration at a rate which is less than that of said line frequency but greater than that of said random control data, means for periodically setting said third pulse signal, in response to said received random control data, to a particular configuration which differs each time the third pulse signal is set and thereafter is stepped under the control of a third clock signal in accordance with said third pseudo random configuration, and means for periodically setting the or each further second pulse signal by said third pulse signal. The means for generating the third signal may be included in a sub-system which means that the pulses at the output of this sub-system are at a rate which is lower than the packet. This means for generating said third pulse signal may generate this third pulse signal at a rate corresponding to the frame frequency of said television signal.

If the random control data is conveyed in the sound/data components of said television signal in encrypted form as an encryption key, said equipment may further comprise means for deriving said encryption key from said sound/data components and means for decrypting said encryption key to produce said control data.

The above and other features of the invention will be more readily understood from the following description with reference to the 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 television transmitter for use with the present invention.

Figure 1 shows a block diagram of a television receiver for use with a direct broadcast satellite television transmission system and in the case of Figure 1 it is assumed the system used is the C-MAC system along the lines disclosed in the Independent Broadcasting Authorities Experimental Development Report 118/82, entitled "MAC—A Television System for High-Quality Satellite Broadcasting", dated August 1982, pages 6 to 9 of that report disclosing a C-MAC system each television line of which sequentially contains a period of digital sound/data information, a period of compressed chrominance information and a period of compressed luminance information. Each television line is effectively divided into 1296 sample periods at a sampling rate of 20.25M bits/second and page 7 contains a table indicating the number of samples allotted to each component. Since the publication of the above report the number of samples allotted to the various components has been amended but this is not important for an understanding of the present invention. A draft technical standard for a C-MAC packet system containing these changes and the construction and positioning of the packets appears in the European Broadcasting Union document SPB 284 dated June 1983 "Draft New Report—Television Standards for 625 line, 12 GHz Satellite Broadcasting".

In Figure 1 the reference 1 indicates a dish aerial suitable for receiving satellite television signals in the 12GHz band, the aerial having a down converter 2 attached to it which frequency converts the incoming television signal to a frequency within the 1 to 2GHz band depending of course on the frequency of the incoming signal. The down converted signal is applied over a co-axial cable 3 to a terminal 4 forming the input for the television receiver this terminal 4 being connected to an r.f. amplifier and frequency changer stage 5 which amplifies and transforms the incoming signal to a suitable i.f. frequency of say 134MHz which is further amplified by an i.f. amplifier 6. The output of the amplifier 6 is applied to a frequency demodulator 7 as the vision components of the broadcast satellite television signal are frequency modulated, the demodulated output of the demodulator 7 being applied to a vision signal processor 8 in which the compressed chrominance and luminance components are processed

such that they are expanded to occupy a line period and available simultaneously. Under certain circumstances, signals received by the aerial 1 will be scrambled so as to permit only authorised subscribers to receive the incoming signals in an intelligible manner in which case the vision processor 8 will need to incorporate a de-scrambling stage in which the scrambled vision components are restored to their normal state. One suitable method of scrambling the vision components is known as "line cut" where the chrominance and luminance components for each television line are each cut at randomly determined positions such that each component is divided and the positions of the divided components transposed such that the latter part of a component (that part after the cut) appears before the first part of that component. The cut will not be at the same place in each line but may be made at one of a possible 256 positions. A de-scrambling key will then be required at the receiver which is the same as the scrambling key at the transmitter to provide the necessary information as to where the cut actually takes place and such a key for a possible 256 cut positions per line will need to be an 8 bit binary word per television line. In Figure 1, such an 8 bit word is applied to the input S of the vision signal processor 8.

The output of the i.f. amplifier 6 is also applied to a digital demodulator stage 9 where the incoming digital signals which are 2-4 PSK modulated (phase-shift keying where the digital information is conveyed differentially between four possible phases) are converted to normal binary form and from which synchronising information and various clock frequencies are produced. The binary signal output from the handling stage 9 is applied to a sound/data signal processor 10 in which the various sound and data channels transmitted with the C-MAC signal are separated one from the other and further processed. As in the case with the vision signal some or all of the sound/data channels may also be scrambled to prevent unauthorised reception of this information and again it will be necessary to provide a de-scrambling key or keys for these sound/data channels to ensure their de-scrambling. The sound/data channels are assumed to be packet multiplexed where a plurality of packets from the different sound/data channels are time multiplexed within periods allotted in the television signal assembled during a given period. One proposal for use with the C-MAC television system is that 162 such packets for 8 sound/data channels shall be present during each television frame. A scrambling technique which can be used with the digital sound/data channels is that where the unscrambled digital signal is added to a pseudo random sequence by means of an exclusive OR-gate.

In order to reproduce the various de-scrambling required in the receiver a slow rate encryption key is transmitted with the broadcast television signal, preferably with the sound/data components, and which is hence received by the

aerial 1, a suitable rate for this encryption key being one byte per second or one byte every two seconds with each byte containing say, 64 bits to the Data Encryption Standard (D.E.S.). This encryption key is separated from the incoming digital information by the sound/data processor 10 and appears at an output 11 of that processor for application to an integrated circuit 12 which may be mounted on a plastic card (of a similar size to a credit card) which the subscriber obtains and which is inserted into an appropriate aperture in the television receiver, which aperture contains suitable connections which make contact with corresponding contacts on the card. The card itself is indicated by the broken line 13. The integrated circuit 12 contains a converter 12A which produces the inverse of the D.E.S. algorithm to provide de-encrypted a random control data signal, which is generated as described in relation to Figure 2, and acts as a trigger for a master pseudo random binary sequence generator (PRBS) 12B forming part of the integrated circuit 12. The master PRBS 12B is a pseudo random number generator which may be a highly secure pseudo random generator according to the Data Encryption Standard producing output sequences of bytes at a rate of one byte per television frame each byte having a pseudo random configuration of 64 bits. The master PRBS 12B is set either once per second or once every two seconds in response to the random control data signal to a particular pulse configuration which differs every time it is set with the output sequence thereafter being stepped in accordance with its random configuration. In addition it will be necessary to provide clocking pulses for the master PRBS 12B at the appropriate frequency of 1.6KHz which pulses are obtained from an output 14 of the demodulator stage 9 and applied to a clock input C of the integrated circuit 12. In this way, data being transferred between the television receiver and the master PRBS 12B on the card 13 are at suitable low rates, which rates are substantially lower than the sampling rate of 20.25M bits/second of the C-MAC system or the sound/data rate for one channel (352 K bits/second). The output from the master PRBS 12B is applied to a slave pseudo random bit sequence generator 15 for the vision signal (vision slave PRBS) which may also be of a highly secure type and producing one byte of 8 bits per television line. The output of the vision slave PRBS 15 is applied to the input S of the vision signal processor 8 and forms the de-scrambling key for the scrambled vision signal. The output of the vision slave PRBS 15 has a pseudo random configuration which is set once per frame to a particular pulse configuration which differs every time it is set by the output of the master PRBS 12B whereafter the vision slave PRBS output is stepped in accordance with its random configuration. A clock signal of 125KHz is derived from an output 16 of the demodulator stage 9 and applied to the clock input C of the vision slave PRBS 15.

The output of the master PRBS 12B is also

applied to a number of slave pseudo random pulse sequence generators for the sound and data channels (sound/data PRBS) depending on the number of such channels subjected to scrambling. In Figure 1, three such sound/data slave PRBS's are shown indicated by the references 17, 18 and 19 and which are respectively associated with first and second sound channels (sound (I), sound (II)) and a data channel. The slave PRBS's 17, 18 and 19 may be of a similar type to that of the slave PRBS vision signal 15 but the rate at which they produce their pseudo random configuration is that rate at which the packets are received for their respective sound/data channels. Inputs S1, S2 and S3 of the sound/data processor 10 respectively receive the outputs of the slave PRBS's 17, 18 and 19 which are applied as respective de-scrambling keys for the sound/data channels. In the sound/data processor 10 the de-scrambling keys are used to provide further sequences of pseudo random numbers at the sound/data bit rate required for the de-scrambling of the individual sound/data channels. As with the vision slave PRBS 15, the sound/data slave PRBS's are periodically set at frame rate to different points in their pseudo random sequences by the output of the master PRBS 12B. The sound/data slave PRBS's 17, 18 and 19 also receive pulse trains of a clock frequency at their clock inputs C from an output 20 of the demodulator stage 9, the clock frequency being dependent on the packet rate at which the scrambling keys are to be produced.

The output of the vision signal processor 8 is shown in Figure 1 to be applied to a display arrangement D where the expanded and de-scrambled vision components are employed to produce a television display. An output of the sound/data processor 10 is shown connected to a loud-speaker system 21 where the appropriate sound channel is reproduced whilst a further output of this processor 10 is shown applied to the display D for the display of data material such as teletext.

In the above description it is assumed that the integrated circuit 12 on the card 13 contains a PRBS 12B producing an output of one byte per frame. This is not necessary and the PRBS may be omitted so that the output of the integrated circuit corresponds to the rate of the received encryption key i.e. one byte per second or every two seconds which sets the slave PRBS's 15, 17, 18 and 19.

Television transmission equipment for use with the present invention is shown in Figure 2 in which a vision signal source 23 which may be a television camera or a video tape recorder has its output connected to a video signal processor 24 in which if the signal is for the C-MAC system the chrominance and luminance components will be compressed in the known manner. In addition, if the vision signal is to be scrambled (such as by the above described "line cut" method) the scrambling of the vision components will also take place in the vision processor 24. The output from the vision processor 24 is applied to a

frequency modulator 25 and the modulated output applied to a suitable transmitter 27 via an adder circuit 26, the transmitter producing a modulated output in the 12GHz band from which it will be applied to a suitable aerial system 28 from which it can be beamed-up to the satellite. In order to generate the necessary scrambling key for the scrambling of the vision signal a random control data signal is generated by a random control data generator 29 which control signal is the same as that required in the receiver in Figure 1, the rate at which the control signal is generated being controlled by clock pulses received at an input C from a clock frequency generator 30 which produces clock pulses at this and other frequencies. The control signal from control generator 29 is applied to a converter stage 22 where the control signal is encrypted to the Data Encryption Standard to produce an encryption key. This encryption key is applied to an input of a sound/data signal processor 31 where the encryption key is inserted either once per second or once every two seconds in the sound/data components of the C-MAC signal. The 2-4 PSK modulated output of the sound/data processor 31 is applied to a second input of the adder circuit 26 for addition to the vision components prior to, transmission.

The random control data signal from the control data generator 29 is also applied to a master pseudo random binary sequence generator (PRBS) 32 which is of the same type and produces the same pseudo random output as the corresponding master PRBS 12B in the receiver and which is set at the same time as that in the receiver to the same particular pulse configuration which differs every time the master PRBS is set. Clock signals of frequency 1.6KHz are applied to the clock input C of the master PRBS 32 from the generator 30. The output of the master PRBS 32 is at frame rate and is applied to a vision slave pseudo random binary sequence generator 33 which is of the same type and produces the same pseudo random output as the corresponding vision slave PRBS 15 in the receiver. This produces the same 8 bits per byte pseudo random sequence with one byte appearing on each line as the vision slave PRBS 15, the vision slave PRBS 33 being periodically set by the master PRBS 32 at the same time as the vision slave PRBS 15 in the receiver to the same particular pulse configuration which differs every time it is set. The output of the vision slave PRBS 33 forms the scrambling key for the scrambling of the vision signal and is applied to an input S of the vision signal processor 24 to control the line cut point for each television line.

Sources of sound signals 34 and 35 (sound I and sound II) are also applied to the sound/data signal processor 31 as is a data signal source 36, the sound/data signal processor 31 processing the various inputs into a packet multiplex form as used with the transmission. These sound and data signals may also be scrambled to prevent unauthorised reception and for this purpose the

output of the master PRBS 32 is applied to respective sound/data slave pseudo random binary sequence generators (sound/data slave PRBS) 37, 38 and 39 which correspond with the slave PRBS 17, 18 and 19 in the receiver and produce corresponding outputs which are set to particular pulse configurations at the same time as for those in the receiver which differ every time these slave PRBS's are set. The outputs of these sound/data slave PRBS 37, 38 and 39 are applied to respective inputs S1, S2 and S3 of the sound/data processor 31 to form the scrambling keys for the scrambling of the sound and data channels at packet level. In the sound/data processor 31 the scrambling keys are used to provide further sequences of pseudo random numbers at the sound/data bit rate required for scrambling the individual sound/data channels. In the same way as for the receiver in Figure 1 the vision and sound/data slave PRBS's 33, 37, 38 and 39 will receive clock signals at their clock inputs C, that for the vision slave PRBS 33 being at 125KHz and derived from an output of the generator 30 whilst that for the remaining slave PRBS's 37, 38 and 39 being at the appropriate frequency as previously described and also being derived from the generator 30.

As with the receiver equipment it is not essential to incorporate a master PRBS 32 in the transmitter which may be omitted and the slave PRBS's 33, 37, 38 and 39 set by the control data from the control data generator 29.

Claims

1. A television transmission system for the transmission and reception of a television signal in which the vision components are scrambled to allow only for their authorised reception, a vision scrambling or de-scrambling key being provided for the respective line-by-line scrambling prior to transmission or de-scrambling on reception of said vision components, said vision scrambling/de-scrambling key comprising a first pulse signal having a first pseudo random configuration locally generated at a first rate which corresponds to that of the line frequency, the first pulse signal being periodically set, in response to random control data which accompanies said television signal having a rate which is low compared with that of the line frequency, to a particular pulse configuration which first pulse signal thereafter is stepped under the control of a first clock signal to produce a fresh scrambling/de-scrambling word per television line in accordance with said first pseudo random configuration, said television signal additionally containing digitally modulated sound or data components which are packet multiplexed such that individual packets represent a sound or a data component which packets are time division multiplexed within periods allotted in said television signal, characterised in that one of said sound/data components is scrambled to allow only for authorised reception, a packet scrambling key being provided for

the packets of the sound/data component which is to be respectively scrambled prior to transmission or de-scrambled on reception, said packet scrambling/de-scrambling key comprising a second pulse signal having a second pseudo random configuration locally generated at a second rate corresponding to the rate at which said packets appear either prior to or after multiplexing prior to transmission or demultiplexing on reception, the second pulse signal being periodically set, in response to said random control data, to a particular pulse configuration which differs each time the second pulse signal is set and thereafter is stepped under the control of a second clock signal in accordance with said second pseudo random configuration.

2. A transmission system as claimed in Claim 1, characterised in that further of said sound/data components are scrambled to allow only for their authorised reception, a separate packet scrambling or de-scrambling key being provided for the packets of each further sound/data component which is to be respectively scrambled prior to transmission or de-scrambled on reception, said separate packet scrambling/de-scrambling keys comprising further second pulse signals each having a pseudo random configuration locally generated at the rates at which the packets of the further sound/data components appear either prior to or after multiplexing prior to transmission or demultiplexing on reception, which further second pulse signals are periodically set, in response to said random control data, to respective particular pulse configurations which differ each time the further second pulse signals are set and thereafter are stepped under the control of said second clock signal in accordance with their respective pseudo random configuration.

3. A transmission system as claimed in Claim 1 or 2, characterised in that a third pulse signal having a third pseudo random configuration is generated at a rate less than that of said line frequency but greater than that of said random control data, said third pulse signal being periodically set, in response to said random control data, to a particular pulse configuration which differs each time the third pulse signal is set and thereafter is stepped under the control of a third clock signal in accordance with said third pseudo random configuration, the or each second pulse signal being periodically set by said third pulse signal.

4. A transmission system as claimed in Claim 3, characterised in that said third pulse signal has a rate which corresponds to the frame frequency of said television signal.

5. A transmission system as claimed in Claim 1, 2, 3 or 4, characterised in that said random control data is conveyed in encrypted form as an encryption key which forms part of the transmission with said sound/data components.

6. Television transmission equipment for generating a television signal for use with a television transmission system as claimed in any



output of the master PRBS 32 is applied to respective sound/data slave pseudo random binary sequence generators (sound/data slave PRBS) 37, 38 and 39 which correspond with the slave PRBS 17, 18 and 19 in the receiver and produce corresponding outputs which are set to particular pulse configurations at the same time as for those in the receiver which differ every time these slave PRBS's are set. The outputs of these sound/data slave PRBS 37, 38 and 39 are applied to respective inputs S1, S2 and S3 of the sound/data processor 31 to form the scrambling keys for the scrambling of the sound and data channels at packet level. In the sound/data processor 31 the scrambling keys are used to provide further sequences of pseudo random numbers at the sound/data bit rate required for scrambling the individual sound/data channels. In the same way as for the receiver in Figure 1 the vision and sound/data slave PRBS's 33, 3738 and 39 will receive clock signals at their clock inputs C, that for the vision slave PRBS 33 being at 125KHz and derived from an output of the generator 30 whilst that for the remaining slave PRB's 37, 38 and 39 being at the appropriate frequency as previously described and also being derived from the generator 30.

As with the receiver equipment it is not essential to incorporate a master PRBS 32 in the transmitter which may be omitted and the slave PRB's 33, 37, 38 and 39 set by the control data from the control data generator 29.

Claims

1. A television transmission system for the transmission and reception of a television signal in which the vision components are scrambled to allow only for their authorised reception, a vision scrambling or de-scrambling key being provided for the respective line-by-line scrambling prior to transmission or de-scrambling on reception of said vision components, said vision scrambling/de-scrambling key comprising a first pulse signal having a first pseudo random configuration locally generated at a first rate which corresponds to that of the line frequency, the first pulse signal being periodically set, in response to random control data which accompanies said television signal having a rate which is low compared with that of the line frequency, to a particular pulse configuration which first pulse signal thereafter is stepped under the control of a first clock signal to produce a fresh scrambling/de-scrambling word per television line in accordance with said first pseudo random configuration, said television signal additionally containing digitally modulated sound or data components which are packet multiplexed such that individual packets represent a sound or a data component which packets are time division multiplexed within periods allotted in said television signal, characterised in that one of said sound/data components is scrambled to allow only for authorised reception, a packet scrambling key being provided for

the packets of the sound/data component which is to be respectively scrambled prior to transmission or de-scrambled on reception, said packet scrambling/de-scrambling key comprising a second pulse signal having a second pseudo random configuration locally generated at a second rate corresponding to the rate at which said packets appear either prior to or after multiplexing prior to transmission or demultiplexing on reception, the second pulse signal being periodically set, in response to said random control data, to a particular pulse configuration which differs each time the second pulse signal is set and thereafter is stepped under the control of a second clock signal in accordance with said second pseudo random configuration.

2. A transmission system as claimed in Claim 1, characterised in that further of said sound/data components are scrambled to allow only for their authorised reception, a separate packet scrambling or de-scrambling key being provided for the packets of each further sound/data component which is to be respectively scrambled prior to transmission or de-scrambled on reception, said separate packet scrambling/descrambling keys comprising further second pulse signals each having a pseudo random configuration locally generated at the rates at which the packets of the further sound/data components appear either prior to or after multiplexing prior to transmission or demultiplexing on reception, which further second pulse signals are periodically set, in response to said random control data, to respective particular pulse configurations which differ each time the further second pulse signals are set and thereafter are stepped under the control of said second clock signal in accordance with their respective pseudo random configuration.

3. A transmission system as claimed in Claim 1 or 2, characterised in that a third pulse signal having a third pseudo random configuration is generated at a rate less than that of said line frequency but greater than that of said random control data, said third pulse signal being periodically set, in response to said random control data, to a particular pulse configuration which differs each time the third pulse signal is set and thereafter is stepped under the control of a third clock signal in accordance with said third pseudo random configuration, the or each second pulse signal being periodically set by said third pulse signal.

4. A transmission system as claimed in Claim 3, characterised in that said third pulse signal has a rate which corresponds to the frame frequency of said television signal.

5. A transmission system as claimed in Claim 1, 2, 3 or 4, characterised in that said random control data is conveyed in encrypted form as an encryption key which forms part of the transmission with said sound/data components.

6. Television transmission equipment for generating a television signal for use with a television transmission system as claimed in any



one of the preceding Claims, said equipment comprising a source of vision components, means for performing line-by-line scrambling of said vision components under the control of a vision scrambling key to allow only for their authorised reception, means for generating random control data at a rate which is low compared with the line frequency of said television signal, means for generating a first pulse signal having a first pseudo random configuration at a first rate corresponding to that of said line frequency which first pulse signal forms the vision scrambling key, means for periodically setting said first pulse signal, in response to said random control data, to a particular pulse configuration which first pulse signal thereafter is stepped under the control of a first clock signal to produce a fresh scrambling word per television line in accordance with said first pseudo random configuration, means for applying said scrambled vision components as part of a television signal to a transmission medium sources of digitally modulated sound or data components, and means for packet multiplexing said sound/data components such that individual packets represent a sound or a data component which packets are multiplexed within allotted periods characterised in that said equipment additionally comprises means for scrambling one of said sound/data components under the control of a packet scrambling key to allow only for authorised reception, means for generating a second pulse signal having a second pseudo random configuration at a second rate corresponding to the rate at which said packets appear, either prior to or after multiplexing, which second pulse signal forms said packet scrambling key, means for periodically setting said second pulse signal, in response to said random control data, to a particular pulse configuration which differs each time the second pulse signal is set and thereafter is stepped under the control of a second clock signal in accordance with said second pseudo random configuration, and means for applying said packet multiplexed sound/data components as part of said television signal to the transmission medium.

7. Transmission equipment as claimed in Claim 6, characterised in that said equipment further comprises means for scrambling further of said sound/data components each under the control of a separate packet scrambling key to allow only for authorised reception, means for generating further second pulse signals each having a pseudo random configuration at rates at which the packets of the further sound/data components appear, either prior to or after multiplexing, which further second pulse signals form the respective separate packet scrambling keys, means for periodically setting said further second pulse signals, in response to said random control data, to particular pulse configurations which differ each time the further second pulse signals are set and thereafter are stepped under the control of said second clock signal in accordance with their respective pseudo random configurations.

8. Transmission equipment as claimed in Claim 6 or 7, characterised in that said equipment additionally contains means for generating a third pulse signal having a third pseudo random configuration at a rate which is less than that of the said line frequency but greater than that of said random control data, means for periodically setting said third pulse signal, in response to said random control data, to a particular pulse configuration which differs each time the third pulse signal is set and thereafter is stepped under the control of a third clock signal in accordance with said third random configuration, and means for periodically setting the or each further second pulse signal by said third pulse signal.

9. Transmission equipment as claimed in Claim 8, characterised in that said means for generating said third pulse signal generate said third pulse signal at a rate corresponding to the frame frequency of said television signal.

10. Transmission equipment as claimed in Claim 6, 7, 8 or 9, characterised in that said equipment further comprises means for encrypting said random control data to form an encryption key which encryption key forms one of the sound/data components.

11. Television receiving equipment for use with a television transmission system as claimed in any of the preceding Claims 1 to 5, in which the vision components of a television signal are scrambled to allow only for their authorised reception, said equipment comprising means for receiving said television signal and for deriving the scrambled vision components therefrom, means for performing line-by-line descrambling of said scrambled vision components under the control of a vision de-scrambling key, means for generating a first pulse signal having a first pseudo random configuration at a first rate corresponding to that of the line frequency which first pulse signal forms said vision de-scrambling key, means for periodically setting said first pulse signal, in response to received random control data which control data has a rate which is low compared with that of the line frequency, to a particular pulse configuration which first pulse signal thereafter is stepped under the control of a first clock signal to produce a fresh de-scrambling word per television line in accordance with said first pseudo random configuration, said television signal additionally containing digitally modulated sound or data components which are packet multiplexed such that individual packets represent a sound or a data component which packets are time division multiplexed within periods allotted in said television signal, characterised in that one of said sound/data components is scrambled to allow only for authorised reception, said equipment additionally comprising means for deriving said one scrambled sound/data component from said received television signal, means for performing de-scrambling of said scrambled sound/data component under the control of a packet de-scrambling key, means for generating a second pulse signal having a second



pseudo random configuration at a second rate corresponding to the rate at which packets appear either prior to or after de-multiplexing which second pulse forms said packet de-scrambling key, means for periodically setting said pulse signal, in response to said received random control data to a particular pulse configuration which differs each time the second pulse signal is set and thereafter is stepped under the control of a second clock signal in accordance with said second pseudo random configuration.

12. Receiving equipment as claimed in Claim 11, characterised in that said television signal has further of said sound/data components which are scrambled to allow only for their authorised reception, said equipment further comprising means for deriving said further scrambled sound/data components from said received television signal, means for performing de-scrambling of said further scrambled sound/data components under the control of separate packet scrambling keys, means for generating further second pulse signals each having a pseudo random configuration at rates at which the packets of the further scrambled sound/data components appear, either prior to or after demultiplexing, which further second pulse signals form the respective separate packet de-scrambling keys, means for periodically setting said further second pulse signals, in response to said received random control data to particular pulse configurations which differ each time the further second pulse signals are set and thereafter are stepped under the control of said second clock signal in accordance with their respective pseudo random configurations.

13. Receiving equipment as claimed in Claim 11 or 12, characterised in that said equipment additionally comprises means for generating a third pulse signal having a third pseudo random configuration at a rate which is less than that of said line frequency but greater than that of said random control data, means for periodically setting said third pulse signal in response to said received random control data to a particular configuration which differs each time the third pulse signal is set and thereafter is stepped under the control of a third clock signal in accordance with said pseudo random configuration, and means for periodically setting the or each further second pulse signal by said third pulse signal.

14. Receiving equipment as claimed in Claim 13, characterised in that said means for generating said third pulse signal generates said third pulse signal at a rate corresponding to the frame frequency of said television signal.

15. Receiving equipment as claimed in Claim 11, 12, 13 or 14 characterised in that said random control data is conveyed in the sound/data components of said television signal in encrypted form as an encryption key, said equipment further comprising means for deriving said encryption key from said sound/data components and means for decrypting said encryption key to produce said random control data.

Patentansprüche

1. Sicheres Fernsehübertragungssystem zur Übertragung und zum Empfang eines Fernsehsignals, wobei die Bildanteile verschlüsselt sind, damit nur ein genehmigter Empfang möglich ist, wobei zur betreffenden zeilenweisen Verschlüsselung vor der Übertragung oder Entschlüsselung bei Empfang der genannten Bildanteile ein Bild-Verschlüsselungs- oder -Entschlüsselungsschlüssel vorgesehen ist, der ein erstes Impulssignal mit einer ersten Pseudorandom-Konfiguration aufweist, das örtlich mit einer ersten Frequenz erzeugt wird, die der Horizontal-Frequenz entspricht, wobei das erste Impulssignal in Antwort auf Randomssteuerdaten, die das genannte Fernsehsignal begleiten und eine Frequenz aufweisen, die im Vergleich zu der Horizontal-Frequenz niedrig ist, auf eine spezifische Impulskonfiguration eingestellt wird, wonach das erste Impulssignal unter Ansteuerung eines ersten Taktimpulssignals entsprechend der genannten ersten Pseudorandom-Konfiguration schrittweise weiterläuft zum Erzeugen eines neuen Verschlüsselungs-/Entschlüsselungswortes je Fernsehzeile, wobei das genannte Fernsehsignal außerdem digital modulierte Ton- oder Datenanteile aufweist, die derart paketverschachtelt sind, daß einzelne Pakete einen Ton- oder Datenanteil darstellen, wobei diese Pakete zeitverschachtelt sind innerhalb zugeordneter Perioden in dem genannten Fernsehsignal, dadurch gekennzeichnet, daß einer der genannten Ton/Datenanteile verschlüsselt wird, damit nur genehmigter Empfang möglich ist, wobei für die Pakete des Ton-/Datenanteils, der vor der Übertragung verschlüsselt oder bei Empfang entschlüsselt werden muß, ein Paketverschlüsselungsschlüssel vorgesehen ist, der ein zweites Impulssignal aufweist mit einer zweiten Pseudorandom-Konfiguration, die örtlich erzeugt wird mit einer zweiten Frequenz, die der Frequenz entspricht, mit der die genannten Pakete erscheinen entweder vor oder nach dem Verschachteln vor der Übertragung oder Entschachteln bei Empfang, wobei das zweite Impulssignal in Antwort auf die genannten Randomssteuerdaten auf eine spezifische Impulskonfiguration eingestellt wird, die jeweils anders ist, wenn das zweite Impulssignal eingestellt wird, und danach unter Ansteuerung eines zweiten Taktsignals entsprechend der genannten zweiten Pseudorandom-Konfiguration schrittweise weiterläuft.

2. Übertragungssystem nach Anspruch 1, dadurch gekennzeichnet, daß weitere der genannten Ton-/Datenanteile verschlüsselt sind, damit nur ein genehmigter Empfang möglich ist, wobei für die Pakete jedes weiteren Ton-/Datenanteils, der vor der Übertragung verschlüsselt oder bei Empfang entschlüsselt werden muss, ein einzelner Paketverschlüsselungs- oder -entschlüsselungsschlüssel vorgesehen ist, wobei diese einzelnen Schlüssel weitere zweite Impulssignale aufweisen, die je eine Pseudorandom-Konfiguration aufweisen, die örtlich mit einer Frequenz

erzeugt werden, mit der die Pakete weiterer Ton-/Datenanteile entweder vor oder nach dem Verschachteln vor der Übertragung oder Entschachteln bei Empfang erscheinen, wobei diese weiteren zweiten Impulssignale in Antwort auf die genannten Randomssteuerdaten auf spezifische Impulskonfigurationen eingestellt werden, die jeweils anders sind, wenn die weiteren zweiten Impulssignale eingestellt werden und danach unter Ansteuerung des genannten zweiten Taktsignals entsprechend der genannten Pseudorandom-Konfiguration schrittweise weiterlaufen.

3. Übertragungssystem nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß ein drittes Impulssignal mit einer dritten Pseudorandom-Konfiguration mit einer Frequenz erzeugt wird, die niedriger ist als die Horizontal-Frequenz aber höher als die der genannten Randomssteuerdaten, wobei das genannte dritte Impulssignal in Antwort auf die genannten Randomssteuerdaten periodisch auf eine bestimmte Impulskonfiguration eingestellt wird, die jeweils anders ist, wenn das dritte Impulssignal eingestellt wird und danach unter Ansteuerung eines dritten Taktsignals entsprechend der genannten dritten Pseudorandom-Konfiguration weiterläuft, wobei das oder jedes zweite Impulssignal durch das genannte dritte Impulssignal eingestellt wird.

4. Übertragungssystem nach Anspruch 3, dadurch gekennzeichnet, daß das genannte dritte Impulssignal eine Frequenz aufweist, die der Teilbildfrequenz des genannten Fernsehsignals entspricht.

5. Übertragungssystem nach Anspruch 1, 2, 3 oder 4, dadurch gekennzeichnet, daß die genannten Randomssteuerdaten in verschlüsselter Form als Verschlüsselungsschlüssel übertragen werden, der einen Teil der Übertragung mit den genannten Ton/Datenanteilen bildet.

6. Fernsehübertragungsanordnung zum Erzeugen eines Fernsehsignals zum Gebrauch in einem Fernsehübertragungssystem nach einem der vorstehenden Ansprüche, wobei diese Anordnung eine Quelle von Bildanteilen aufweist, Mittel zum Durchführen einer zeilenweisen Verschlüsselung der genannten Bildanteile unter Ansteuerung eines Bildverschlüsselungsschlüssels, damit nur ein genehmigter Empfang möglich ist, Mittel zum Erzeugen von Randomssteuerdaten mit einer Frequenz, die im Vergleich zu der Horizontal-Frequenz des genannten Fernsehsignals niedrig ist, Mittel zum Erzeugen eines ersten Impulssignals mit einer ersten Pseudorandom-Konfiguration mit einer ersten Frequenz entsprechend der genannten Horizontal-Frequenz, wobei dieses erste Impulssignal den Bildverschlüsselungsschlüssel bildet, Mittel um das genannte erste Impulssignal in Antwort auf die genannten Randomssteuerdaten periodisch auf eine spezifische Impulskonfiguration einzustellen, wobei dieses erste Impulssignal danach unter Ansteuerung eines ersten Taktsignals zum Erzeugen eines neuen Verschlüsselungswortes je Fernsehzeile entsprechend der genannten ersten Pseudorandom-Konfiguration schrittweise weiterläuft, Mit-

tel zum Zuführen der genannten verschlüsselten Bildanteile als Teil eines Fernsehsignals zu einem Übertragungsmittel, Quellen digital modulierter Ton- oder Datenanteile, und Mittel zur Paketverschachtelung der genannten Ton-/Datenanteile, derart, daß einzelne Pakete einen Ton- oder einen Datenanteil darstellen, wobei diese Pakete innerhalb zugeordneter Perioden verschachtelt werden, dadurch gekennzeichnet, daß die genannte Anordnung außerdem Mittel aufweist zum unter Ansteuerung eines Paketverschlüsselungsschlüssels Verschlüsseln eines der genannten Ton-/Datenanteile, damit nur ein genehmigter Empfang möglich ist, Mittel zum Erzeugen eines zweiten Impulssignals mit einer zweiten Pseudorandom-Konfiguration mit einer zweiten Frequenz, die der Frequenz entspricht, mit der die genannten Pakete erscheinen, entweder vor oder nach dem Verschachteln, wobei das zweite Impulssignal den genannten Paketverschlüsselungsschlüssel bildet, Mittel zum periodischen Einstellen des genannten zweiten Impulssignals, in Antwort auf die genannten Randomssteuerdaten, auf eine spezifische Impulskonfiguration, die jeweils anders ist, wenn das zweite Impulssignal eingestellt wird und danach unter Ansteuerung des zweiten Taktsignals entsprechend der genannten Pseudorandom-Konfiguration schrittweise weiterläuft, und Mittel zum Zuführen der genannten paketverschachtelten Ton-/Datenanteile als Teil des genannten Fernsehsignals zu dem Übertragungsmittel.

7. Übertragungsanordnung nach Anspruch 6, dadurch gekennzeichnet, daß diese Anordnung weiterhin Mittel aufweist zum Verschlüsseln weiterer Ton-/Datenanteile, je unter Ansteuerung eines einzelnen Paketverschlüsselungsschlüssels, damit nur ein genehmigter Empfang möglich ist, Mittel zum Erzeugen weiterer zweiter Impulssignale mit je einer Pseudorandom-Konfiguration mit einer Frequenz, mit der die genannten Pakete der weiteren Ton-/Datenanteile erscheinen, entweder vor oder nach dem Verschachteln, wobei die weiteren zweiten Impulssignale die genannten Paketverschlüsselungsschlüssel bilden, Mittel zum periodischen Einstellen der genannten weiteren zweiten Impulssignale, in Antwort auf die genannten Randomssteuerdaten, auf spezifische Impulskonfigurationen, die jeweils anders sind, wenn die weiteren zweiten Impulssignale eingestellt werden und danach unter Ansteuerung des zweiten Taktsignals entsprechend der genannten Pseudorandom-Konfigurationen schrittweise weiterlaufen.

8. Übertragungsanordnung nach Anspruch 6 oder 7, dadurch gekennzeichnet, daß die genannte Anordnung außerdem Mittel aufweist zum Erzeugen eines dritten Impulssignals mit einer dritten Pseudorandom-Konfiguration mit einer Frequenz, die niedriger ist als die genannte Horizontal-Frequenz aber höher als die der genannten Randomssteuerdaten, Mittel zum periodischen Einstellen des genannten dritten Impulssignals, in Antwort auf die genannten Randomssteuerdaten, auf eine spezifische Impuls-



konfiguration, die jeweils anders ist, wenn das dritte Impulssignal eingestellt wird und danach unter Ansteuerung eines dritten Taktsignals entsprechend der genannten dritten Random-Konfiguration schrittweise weiterläuft, und Mittel zum periodischen Einstellen des oder jedes weiteren zweiten Impulssignals durch das genannte dritte Impulssignal.

9. Übertragungsanordnung nach Anspruch 8, dadurch gekennzeichnet, daß die genannten Mittel zum Erzeugen des genannten dritten Impulssignals das genannte dritte Impulssignal mit einer Frequenz entsprechend der Teilbildfrequenz des genannten Fernsehsignals erzeugen.

10. Übertragungsanordnung nach Anspruch 6, 7, 8 oder 9, dadurch gekennzeichnet, daß die genannte Anordnung weiterhin Mittel aufweist zum Verziffern der genannten Randomssteuerdaten zum Bilden eines Verzifferungsschlüssels, der einen der Ton-/Datenanteile bildet.

11. Fernsehempfangsanordnung zum Gebrauch in einem Fernsehübertragungssystem nach einem der vorstehenden Ansprüche 1 bis 5, wobei die Bildanteile eines Fernsehsignals verschlüsselt werden damit nur ein genehmigter Empfang möglich ist, wobei diese Anordnung Mittel aufweist zum Empfangen des genannten Fernsehsignals und zum Ableiten der verschlüsselten Bildanteile aus demselben, Mittel zum Durchführen einer zeilenweisen Entschlüsselung der genannten verschlüsselten Bildanteile unter Ansteuerung eines Bildentschlüsselungsschlüssels, Mittel zum Erzeugen eines ersten Impulssignals mit einer ersten Pseudorandom-Konfiguration mit einer ersten Frequenz entsprechend der Horizontal-Frequenz, wobei dieses erste Impulssignal den genannten Bildentschlüsselungsschlüssel bildet, Mittel zum periodischen Einstellen des genannten ersten Impulssignals, in Antwort auf empfangene Randomssteuerdaten, wobei diese Steuerdaten eine Frequenz aufweisen, die im Vergleich zu der Horizontal-Frequenz niedrig ist, auf eine spezifische Impulskonfiguration, wobei das erste Impulssignal danach unter Ansteuerung eines ersten Taktimpulssignals entsprechend der genannten ersten Pseudorandom-Konfiguration schrittweise weiterläuft, zum Erzeugen eines neuen Kodewortes je Fernsehzeile, wobei das genannte Fernsehsignal außerdem digital modulierte Ton- oder Datenanteile aufweist, die derart paketverschachtelt sind, daß einzelne Pakete einen Ton- oder einen Datenanteil darstellen, wobei diese Pakete innerhalb zugeordneter Perioden in dem genannten Fernsehsignal zeitverschachtelt sind, dadurch gekennzeichnet, daß einer der genannten Ton-/Datenanteile verschlüsselt ist, damit nur ein genehmigter Empfang möglich ist, wobei die genannte Anordnung außerdem Mittel aufweist zum Ableiten des genannten einen verschlüsselten Ton-/Datenanteil aus dem genannten empfangenen Fernsehsignal, Mittel zum Durchführen der Entschlüsselung des genannten verschlüsselten Ton-/Datenanteils unter Ansteuerung eines Paketentschlüsselungsschlüssels, Mittel zum Erzeugen eines zwei-

ten Impulssignals mit einer zweiten Pseudorandom-Konfiguration mit einer zweiten Frequenz entsprechend der Frequenz, mit der Pakete erscheinen, entweder vor oder nach Entschachtelung, wobei der zweite Impuls den genannten Paketentschlüsselungsschlüssel bildet, Mittel zum periodischen Einstellen des Impulssignals, in Antwort auf die genannten empfangenen Randomssteuerdaten, auf eine spezifische Impulskonfiguration, die jeweils anders ist, wenn das zweite Impulssignal eingestellt wird und danach unter Ansteuerung des zweiten Taktimpulssignals entsprechend der genannten zweiten Pseudorandom-Konfiguration weiterläuft.

12. Empfangsanordnung nach Anspruch 11, dadurch gekennzeichnet, daß das genannte Fernsehsignals weitere von den genannten Ton-/Datenanteilen aufweist, die verschlüsselt sind, damit nur ein genehmigter Empfang möglich ist, wobei die genannte Anordnung weiterhin Mittel aufweist zum Ableiten der genannten weiteren verschlüsselten Ton-/Datenanteile von dem empfangenen Fernsehsignal, Mittel zum Durchführen der Entschlüsselung der genannten weiteren verschlüsselten Ton-/Datenanteile unter Ansteuerung einzelner Paketentschlüsselungsschlüssel, Mittel zum Erzeugen weiterer zweiter Impulssignale mit einer Pseudorandom-Konfiguration mit einer Frequenz entsprechend der Frequenz, mit der Pakete weiterer verschlüsselter Ton-/Datenanteile erscheinen, entweder vor oder nach Entschachtelung, wobei die weiteren zweiten Impulssignale die jeweiligen einzelnen Paketentschlüsselungsschlüssel bilden, Mittel zum periodischen Einstellen der genannten weiteren zweiten Impulssignale, in Antwort auf die genannten empfangenen Randomssteuerdaten, auf spezifische Impulskonfigurationen, die jeweils anders sind, wenn die weiteren zweiten Impulssignale eingestellt werden und danach unter Ansteuerung des zweiten Taktimpulssignals entsprechend den genannten zweiten Pseudorandom-Konfigurationen weiterlaufen.

13. Empfangsanordnung nach Anspruch 11 oder 12, dadurch gekennzeichnet, daß die genannte Anordnung außerdem Mittel zum Erzeugen eines dritten Impulssignals aufweist mit einer dritten Pseudorandom-Konfiguration mit einer Frequenz, die niedriger ist als die genannte Horizontal-Frequenz, aber höher als die der genannten Randomssteuerdaten, Mittel zum periodischen Einstellen des genannten dritten Impulssignals in Antwort auf die genannten empfangenen Randomssteuerdaten auf eine spezifische Konfiguration, die jeweils anders ist, wenn das dritte Impulssignal eingestellt wird und danach unter Ansteuerung eines dritten Taktimpulssignals entsprechend der genannten Pseudorandom-Konfiguration weiterläuft, und Mittel zum periodischen Einstellen des oder jedes weiteren zweiten Impulssignals durch das genannte dritte Impulssignal.

14. Empfangsanordnung nach Anspruch 13, dadurch gekennzeichnet, daß die genannten Mittel zum Erzeugen des genannten dritten Impulssi-

gnals das genannte dritte Impulssignal mit einer Frequenz erzeugt, die der Teilbildfrequenz des genannten Fernsehsignals entspricht.

15. Empfangsanordnung nach Anspruch 11, 12, 13 oder 14, dadurch gekennzeichnet, daß die genannten Randomssteuerdaten in den Ton-/Datenanteilen des genannten Fernsehsignals in verzifferter Form als Verzifferungsschlüssel übertragen werden, wobei die genannte Anordnung weiterhin Mittel aufweist zum Ableiten des genannten Verzifferungsschlüssels von den genannten Ton-/Datenanteilen und Mittel zum Entziffern des genannten Verzifferungsschlüssels zum Erzeugen der genannten Randomssteuerdaten.

Revendications

1. Système de transmission de télévision pour l'émission et la réception d'un signal de télévision, dans lequel les composantes vidéo sont embrouillées en vue de ne permettre que leur réception autorisée, une clé d'embrouillage ou de désembrouillage vidéo étant prévue respectivement pour l'embrouillage ligne par ligne avant l'émission ou le désembrouillage à la réception des composantes vidéo, la clé d'embrouillage/désembrouillage vidéo comprenant un premier signal d'impulsion présentant une première configuration pseudoaléatoire engendrée localement à une première cadence qui correspond à celle de la fréquence de ligne, le premier signal d'impulsion étant positionné périodiquement, en réaction à des données de commande aléatoires qui accompagnent le signal de télévision dont la cadence est faible comparée à celle de la fréquence de ligne, sur une configuration d'impulsion particulière, ce premier signal d'impulsion étant ensuite décalé pas à pas sous la commande d'un premier signal d'horloge pour produire un mot d'embrouillage/désembrouillage nouveau par ligne de télévision selon ladite première configuration pseudoaléatoire, le signal de télévision contenant, en outre, des composantes de son ou de données modulées numériquement, qui sont multiplexées par paquets d'une manière telle que des paquets individuels représentent une composante de son ou de données, ces paquets étant multiplexés dans le temps dans les limites de périodes attribuées dans le signal de télévision, caractérisé en ce que l'une des composantes de son/données est embrouillée en vue de ne permettre que la réception autorisée, une clé d'embrouillage de paquets étant prévue pour les paquets de la composante de son/données qu'il faut respectivement embrouiller avant l'émission ou désembrouiller à la réception, la clé d'embrouillage/désembrouillage de paquets comprenant un second signal d'impulsion présentant une seconde configuration pseudoaléatoire engendrée localement à une seconde cadence correspondant à celle à laquelle les paquets apparaissent avant ou après le multiplexage précédant l'émission ou le démultiplexage lors de la réception, le second signal d'impulsion étant posi-

tionné périodiquement, en réaction aux données de commande aléatoires, sur une configuration d'impulsion particulière qui diffère chaque fois que le second signal d'impulsion est positionné, puis décalé pas à pas sous la commande d'un second signal d'horloge en conformité avec la seconde configuration pseudoaléatoire.

2. Système de transmission de télévision suivant la revendication 1, caractérisé en ce que d'autres parmi les composantes de son/données sont embrouillées en vue de ne permettre que leur réception autorisée, une clé d'embrouillage ou de désembrouillage de paquets séparée étant prévue pour les paquets de chaque autre composante de son/données qu'il faut respectivement embrouiller avant l'émission ou désembrouiller à la réception, les clés d'embrouillage/désembrouillage de paquets séparées comprenant d'autres seconds signaux d'impulsions présentant chacun une configuration pseudoaléatoire engendrée localement aux cadences auxquelles les paquets des autres composantes de son/données apparaissent avant ou après le multiplexage précédant l'émission ou le démultiplexage lors de la réception, les autres seconds signaux d'impulsions étant positionnés périodiquement en réaction aux données de commande aléatoires, sur des configurations d'impulsions particulières respectives qui diffèrent chaque fois que les autres seconds signaux d'impulsions sont positionnés, puis décalés pas à pas sous la commande du second signal d'horloge en conformité avec leurs configurations pseudoaléatoires respectives.

3. Système de transmission suivant la revendication 1 ou 2, caractérisé en ce qu'un troisième signal d'impulsion présentant une troisième configuration pseudoaléatoire est engendré à une cadence inférieure à celle de la fréquence de ligne, mais supérieure à celle des données de commande aléatoires, le troisième signal d'impulsion étant positionné périodiquement, en réaction aux données de commande aléatoires, sur une configuration d'impulsion particulière qui diffère chaque fois que le troisième signal d'impulsion est positionné et étant ensuite décalé pas à pas sous la commande d'un troisième signal d'horloge en conformité avec la troisième configuration pseudoaléatoire, le ou chaque deuxième signal d'impulsion étant positionné périodiquement par le troisième signal d'impulsion.

4. Système de transmission suivant la revendication 3, caractérisé en ce que le troisième signal d'impulsion a une cadence qui correspond à la fréquence de trame du signal de télévision.

5. Système de transmission suivant la revendication 1 ou 2, 3 ou 4, caractérisé en ce que les données de commande aléatoires sont transmises sous une forme cryptée en tant que clé de cryptage faisant partie de la transmission avec les composantes de son/données.

6. Equipement d'émission de télévision destiné à engendrer un signal de télévision à utiliser avec son système de transmission de télévision suivant l'une quelconque des revendications précédentes, cet équipement comprenant une source



de composantes vidéo, un moyen pour effectuer l'embrouillage ligne par ligne des composantes vidéo sous la commande d'une clé d'embrouillage vidéo afin de ne permettre que leur réception autorisée, un moyen pour engendrer des données de commande aléatoires à une cadence qui est faible comparée à la fréquence de ligne du signal de télévision, un moyen pour engendrer un premier signal d'impulsion présentant une première configuration pseudoaléatoire à une première cadence correspondant à celle de la fréquence de ligne, le premier signal d'impulsion formant la clé d'embrouillage vidéo, un moyen pour positionner périodiquement le premier signal d'impulsion, en réaction aux données de commande aléatoires, sur une configuration d'impulsion particulière, ce premier signal d'impulsion étant ensuite décalé pas à pas sous la commande d'un premier signal d'horloge pour produire un mot d'embrouillage nouveau par ligne de télévision en conformité avec la première configuration pseudoaléatoire, un moyen pour appliquer les composantes vidéo embrouillées, en tant que partie d'un signal de télévision, à un milieu de transmission, des sources de composantes de son ou de données modulées numériquement, et un moyen pour multiplexer par paquets les composantes de son/données d'une manière telle que des paquets individuels représentent une composante de son ou de données, ces paquets étant multiplexés dans les limites de périodes attribuées, caractérisé en ce que cet équipement comprend, en outre un moyen pour embrouiller l'une des composantes de son/données sous la commande d'une clé d'embrouillage de paquets en vue de ne permettre qu'une réception autorisée, un moyen pour engendrer un second signal d'impulsion présentant une seconde configuration pseudoaléatoire à une seconde cadence correspondant à celle à laquelle les paquets apparaissent, avant ou après multiplexage, le second signal d'impulsion formant la clé d'embrouillage de paquets, un moyen pour positionner périodiquement le second signal d'impulsion en réaction aux données de commande aléatoires, sur une configuration d'impulsion particulière qui diffère chaque fois que le second signal d'impulsion est positionné, puis décalé pas à pas sous la commande d'un second signal d'horloge en conformité avec la seconde configuration pseudoaléatoire, et un moyen pour appliquer les composantes de son/données multiplexées par paquets, en tant que partie du signal de télévision, au milieu de transmission.

7. Equipement d'émission suivant la revendication 6, caractérisé en ce qu'il comprend, en outre, un moyen pour embrouiller de nouvelles composantes de son/données, chaque fois sous la commande d'une clé d'embrouillage de paquets séparée en vue de ne permettre qu'une réception autorisée, un moyen pour engendrer d'autres seconds signaux d'impulsions présentant chacun une configuration pseudoaléatoire à des cadences auxquelles les paquets des nouvelles composantes de son/données apparaissent, soit

avant, soit après le multiplexage, cet autre second signal d'impulsion formant les clés d'embrouillage de paquets séparées respectives, un moyen pour positionner périodiquement les autres seconds signaux d'impulsions, en réaction aux données de commande aléatoires, sur des configurations d'impulsions particulières qui diffèrent chaque fois que les autres seconds signaux d'impulsions sont positionnés, puis décalés pas à pas sous la commande du second signal d'horloge, conformément à leurs configurations pseudoaléatoires respectives.

8. Equipement d'émission suivant la revendication 6 ou 7, caractérisé en ce qu'il contient, en outre, des moyens pour engendrer un troisième signal d'impulsion présentant une troisième configuration pseudoaléatoire à une cadence qui est inférieure à celle de la fréquence de ligne, mais supérieure à celle des données de commande aléatoires, un moyen pour positionner périodiquement le troisième signal d'impulsion, en réaction aux données de commande aléatoires, sur une configuration d'impulsion particulière qui diffère chaque fois que le troisième signal d'impulsion est positionné, puis décalé pas à pas sous la commande d'un troisième signal d'horloge, en conformité avec la troisième configuration pseudoaléatoire, et un moyen pour positionner périodiquement le ou chaque autre second signal d'impulsion par le troisième signal d'impulsion.

9. Equipement d'émission suivant la revendication 8, caractérisé en ce que les moyens destinés à engendrer le troisième signal d'impulsion engendrent ce troisième signal d'impulsion à une cadence correspondant à la fréquence de trame du signal de télévision.

10. Equipement d'émission suivant la revendication 6, 7, 8 ou 9, caractérisé en ce qu'il comprend, en outre, des moyens pour crypter les données de commande aléatoires en vue de former une clé de cryptage qui forme l'une des composantes de son/données.

11. Equipement de réception de télévision à utiliser dans un système de transmission de télévision suivant l'une quelconque des revendications 1 à 5, dans lequel les composantes de vision d'un signal de télévision sont embrouillées pour ne permettre que la réception autorisée, cet équipement comprenant un moyen pour recevoir le signal de télévision et pour en extraire les composantes vidéo embrouillées, un moyen pour effectuer un désembrouillage ligne par ligne de ces composantes vidéo embrouillées sous la commande d'une clé de désembrouillage vidéo, un moyen pour engendrer un premier signal d'impulsion présentant une première configuration pseudoaléatoire à une première cadence correspondant à celle de la fréquence de ligne, ce premier signal d'impulsion formant la clé de désembrouillage vidéo, un moyen pour positionner périodiquement le premier signal d'impulsion, en réaction aux données de commande aléatoires reçues, ces données de commande accusant une cadence faible comparée à celle de

la fréquence de ligne, sur une configuration d'impulsion particulière, le premier signal d'impulsion étant ensuite décalé pas à pas sous la commande d'un premier signal d'horloge pour produire un mot de désembrouillage nouveau par ligne de télévision en conformité avec la première configuration pseudoaléatoire, le signal de télévision contenant, en outre, des composantes de son ou de données modulées numériquement qui sont multiplexées par paquets, d'une manière telle que des paquets individuels représentent une composante de son ou de données, ces paquets étant multiplexés dans le temps dans les limites de périodes qui leur sont attribuées dans le signal de télévision, caractérisé en ce que l'une des composantes de son/données est embrouillée en vue de ne permettre que la réception autorisée, ledit équipement comprenant, en outre, un moyen pour extraire la composante de son/données embrouillée du signal de télévision reçu, un moyen pour procéder au désembrouillage de la composante de son/données embrouillée sous la commande d'une clé de désembrouillage de paquets, un moyen pour engendrer un second signal d'impulsion présentant une seconde configuration pseudoaléatoire à une seconde cadence correspondant à celle à laquelle les paquets apparaissent, soit avant, soit après le démultiplexage, cette seconde impulsion formant la clé de désembrouillage de paquets, un moyen pour positionner périodiquement le second signal d'impulsion, en réaction aux données de commande aléatoires reçues, sur une configuration d'impulsion particulière qui diffère chaque fois que le second signal d'impulsion est positionné, puis est décalé pas à pas sous la commande d'un second signal d'horloge en conformité avec la seconde configuration pseudoaléatoire.

12. Equipement de réception suivant la revendication 11, caractérisé en ce que le signal de télévision comporte de nouvelles composantes de son/données qui sont embrouillées en vue de ne permettre que leur réception autorisée, cet équipement comprenant, en outre, un moyen pour extraire ces nouvelles composantes de son/données embrouillées du signal de télévision reçu, un moyen pour procéder au désembrouillage de ces nouvelles composantes de son/données embrouillées sous la commande de clés de désembrouillage de paquets séparées, un moyen pour engendrer d'autres seconds signaux d'impulsions présentant chacun une configuration

pseudoaléatoire à des cadences auxquelles les paquets des nouvelles composantes de son/données embrouillées apparaissent, soit avant, soit après le démultiplexage, ces autres seconds signaux d'impulsions formant les clés de désembrouillage de paquets séparées respectives, un moyen pour positionner périodiquement les autres seconds signaux d'impulsions, en réaction aux données de commande aléatoires reçues, sur des configurations d'impulsions particulières qui diffèrent chaque fois que les seconds signaux d'impulsions sont positionnés, puis décalés pas à pas sous la commande du second signal d'horloge en conformité avec leurs configurations pseudoaléatoires respectives.

13. Equipement de réception suivant la revendication 11 ou 12, caractérisé en ce qu'il comprend, en outre, un moyen pour engendrer un troisième signal d'impulsion présentant une troisième configuration pseudoaléatoire à une cadence qui est inférieure à celle de la fréquence de ligne, mais supérieure à celle des données de commande aléatoires, un moyen pour positionner périodiquement le troisième signal d'impulsion, en réaction aux données de commande aléatoires reçues, sur une configuration particulière qui diffère chaque fois que le troisième signal d'impulsion est positionné, puis est décalé pas à pas sous la commande d'un troisième signal d'horloge en conformité avec la troisième configuration pseudoaléatoire, et un moyen pour positionner périodiquement le ou chaque autre second signal d'impulsion par le troisième signal d'impulsion.

14. Equipement de réception suivant la revendication 13, caractérisé en ce que le moyen pour engendrer le troisième signal d'impulsion engendre ce troisième signal d'impulsion à une cadence correspondant à la fréquence de trame du signal de télévision.

15. Equipement de réception suivant les revendications 11, 12, 13 ou 14, caractérisé en ce que les données de commande aléatoires sont transmises dans les composantes de son/données du signal de télévision sous une forme cryptée en tant que clé de cryptage, l'équipement comprenant, en outre, un moyen pour extraire la clé de cryptage des composantes de son/données et un moyen pour décrypter la clé de cryptage en vue de produire lesdites données de commande aléatoires.



* C L M S *