

Description

The present invention relates to a secret or privacy signal transmission system which sends out an audio signal or like analog signal after transforming it into a privacy signal.

A transmission system of the type described is not only capable of keeping eavesdroppers from communications between two parties but also capable of eliminating leak of messages when the parties are accidentally connected to a third party due to failure in the transmission line.

Privacy signal transmission systems heretofore proposed may generally be classified into two types, i.e., a spectrum inversion type and a type which allows messages to be exchanged using privacy codes (e.g. key codes or PN codes) and digitally processing them for privacy. The spectrum inversion type system is not a perfect privacy implementation, however, since it inherently allows sound volumes to be identified and even part of voice overhead to allow one to presume the content of communication. It is also threatened with leak of conversations in the event of common channel interference in a radio system when the receivers are of a same type, if independent. The privacy code type system, on the other hand, is free from the possibility of eavesdropping or leak, since conversations are exchanged between only specific individuals which share common privacy codes (e.g. key codes or PN codes). Nevertheless, this brings about a problem in the aspect of reproduction quality because transmission of a signal at a low rate, which is required to limit the transmission band in digital signal transmission, introduces quantization noise in the reproduced voice or substantial wave distortion due to quantization. If no limitation is imposed on the transmission frequency band to allow signals to be fed at a high rate, an encryption circuit will have to be scaled up and, therefore, expensive, even though the waveform distortion due to quantization noise may be suppressed.

Reference may be made to the following documents for details of the privacy code type signal transmission system:

(1) Whitfield Diffie et al. "New Directions in Cryptography", IEEE Transactions of Information Theory, Vol. IT-22, No. 6, p.p. 644-654, November 1976.

(2) Horst Feistel et al. "Some Cryptographic Techniques for Machine-to-Machine Data Communication", Proceedings of the IEEE, Vol. 63, No. 11, p.p. 1545-1555, November, 1975.

(3) US-A-3,784,743.

FR-A-2 209 260 discloses a signal transmission system with partially coded and partially analogous modulated signal groups and focuses on a reduction of the quantization error. This system, however, does not suggest an encryption of the digital signal only, and moreover there is no modulation between the digital signal pulses and the variable signal pulse.

It is an object of the present invention to

provide a privacy signal transmission system which is capable of transmitting quality analog signals despite the use of an inexpensive digital encryption circuit.

In accordance with the present invention, there is provided a privacy signal transmission system comprising a transmitter including digital pulse modulator means for converting a first analog signal into a first digital signal, extractor means for extracting a first analog error signal representative of a difference between a second analog signal provided by analog conversion of the first digital signal and the first analog signal, and transmission means for transmitting the first analog error signal and the first digital signal; and a receiver including means for receiving the first analog error signal and the first digital signal to individually generate a second analog error signal and a second digital signal, digital pulse demodulator means for converting the second digital signal into a third analog signal, and reproduction means for reproducing the first analog signal by adding the second analog error signal to the third analog signal. This transmission system is characterized in that the transmitter further comprises encryption means connected between the digital pulse modulator means and the transmission means, for converting only the first digital signal into a first digital privacy signal, thereby transmitting the first digital privacy signal, instead of the first digital signal to the receiver; and that the receiver further comprises decryption means connected between the means and the digital pulse demodulator means for converting only the first digital privacy signal into the second digital signal.

Preferred embodiments of the present invention will be described with reference to the accompanying drawings in which:

Figure 1 is a block diagram of a privacy signal transmission system embodying the present invention;

Figures 2A-2E are waveform diagrams representing the operation of the system shown in Figure 1; and

Figure 3 is a block diagram of another embodiment of the present invention.

Referring to Figure 1 of the drawings, a privacy signal transmission system of the present invention is shown and includes a transmitter 100. A first analog audio signal X_{in} to be transmitted is applied to an input terminal T_{in} of the transmitter 100. A digital pulse modulator, indicated by a phantom block 1, transforms the input analog signal X_{in} into a digital signal X_1 . In this particular embodiment, the digital pulse modulator 1 comprises a ΔM modulator which is well known in the art (e.g. MOTOROLA MC 3417, MC 3418, MC 3517 or MC 3518). As shown, the ΔM modulator 1 is made up of a comparator 8, a D-type flip-flop (D-FF) 9, and an integrator 10. The comparator 8 compares a second analog audio signal, which is a reproduced signal X_{10} , with the first analog audio signal X_{in} coming in through the input terminal T_{in} . The output X_8 of the comparator 8 is

extracted by the D-FF 9 using clock pulses CLK, which are generated by a clock pulse generator (not shown). The output of the D-FF 9 is in turn converted by the integrator 10 into the previously mentioned second analog audio signal X_{10} . It should be born in mind that the integrator output or second analog signal X_{10} is always subordinate to the first analog signal X_{in} and has a waveform analogous to that of the latter.

The digital audio signal $X_1 (=X_9)$ is fed from the ΔM modulator 1 to an encryption, scrambling or private circuit 2 which is adapted to perform digital encryption on the input signal using private codes such as PN codes and timed to the clock pulses CLK. The output of the encryption circuit 2 is fed through a bandpass filter 24 to an FM (frequency modulation) modulator 3 to be thereby converted into an FM wave. Taking into account the need for band limitation in the transmission path, BT is usually selected to be equal to or smaller than about 0.5 where B is the transmission band width and $1/T$ corresponds to the transmission rate.

Most of the audio signal is transmitted as a digital signal in the manner described above. In accordance with the present invention, even the rest of the signal ($X_{in}-X_{10}$), i.e., quantization error signal, is transmitted.

A subtractor 4 included in the transmitter 100 serves to provide an error signal $X_4=X_{in}-X_{10}$. The subtractor 4 is connected to a low pass filter 5. The output of the FM modulator 3 is applied to an AM (amplitude modulation) modulator 6 at which it is subjected to amplitude modulation by an output X_5 of the low pass filter 5. The degree of amplitude modulation is selected to lie in a range which does not extremely widen the transmission band or effect the transmission error probability of the digital signal X_1 (approximately 0.1—0.2). The resulting AM wave X_6 is converted by a transmitting section 25 into a radio frequency and, then, sent out through an antenna 7.

A receiver 101 receives the high frequency which comes in through an antenna 11. In the receiver 101, a receiving section 12 transforms the high frequency into an intermediate frequency. The output of the receiving section 12 is applied to a limiter 13 and an AM detector 18. The limiter 13 removes the AM component from the intermediate frequency, while an FM discriminator 14 connected to the limiter 13 reproduces a digital privacy signal X_{14} . A decryption circuit or private circuit 15 deciphers the privacy signal X_{14} using the same privacy code as one used at the transmitter, thereby providing a digital audio signal X_{15} . Here, the privacy code is shared by the specific transmitter and receiver only and not identical with those of other receivers. That is, only the receiver assigned with a same code as one assigned to the transmitter is capable of receiving messages. The digital audio signal X_{15} is converted into an analog audio signal by a digital pulse demodulator 16. In this embodiment, the digital pulse demodulator 16 comprises a ΔM demodulator (e.g. MOTOROLA MC 3417, MC 3418, MC 3517 or MC 3518).

So long as the transmission line is free from

errors, the received digital audio signal X_{15} represents information which is identical with the information represented by the transmitted digital audio signal X_1 ; the waveform of the output X_{16} of the ΔM demodulator 16 is identical with that of the second analog audio signal X_{10} in the ΔM modulator 1. A clock recovery circuit 17 recovers the clock pulses out of the FM discriminator output X_{14} , so that the recovered clock pulses may be used for operating the decryption circuit 15 and ΔM demodulator 16.

The error signal received by the receiving section 12 is detected by the AM detector 18 and then delayed by a delay circuit 19. The delay to be effected by the delay circuit 19 is preselected to be equal to a time lag between the instant when the first analog signal X_{in} applied to the transmitter is converted by the ΔM modulator 1 into a digital audio signal X_1 and the instant when the second analog signal is reproduced in the receiver by the ΔM demodulator 16. The delay circuit 19 is omissible, however, so long as the delay concerned is not substantial. The second analog signal X_{16} output from the ΔM demodulator 16 and the error signal X_{19} output from the delay circuit 19 are added together by an adder 20. The summation output X_{20} of the adder 20 has a waveform which resembles that of the first analog signal X_{in} very much. Further, the output X_{20} of the adder 20 is passed through a low pass filter 21 for removal of noise, thereby reproducing the desired first analog signal X_{21} . The audio signal X_{21} is delivered as an output signal X_{out} from an output terminal T_{out} .

Waveforms shown in Figure 2 represent the operation of the system described above with reference to Figure 1. Figure 2A indicates the transmitter input signal X_{in} (first analog audio signal) and the signal X_{10} in the ΔM modulator 1 (second analog audio signal). Although the signal X_{10} is always subordinate to the input signal X_{in} as described, the quantization accuracy is lowered when the signal rate is low, as shown in Figure 2A, preventing the waveform of the input signal X_{in} from being reproduced as it is. Figure 2B represents an error signal between the input signal X_{in} and the signal X_{10} , $X_4=X_{in}-X_{10}$. Figure 2C shows the output X_{16} of the ΔM demodulator 16 which is reproduced at the receiver. Concerning the waveform, the signal shown in Figure 2C is identical with a version of the signal X_{10} which is shifted by a transmission time τ . Due to quantization error, should the signal X_{16} be applied directly to the filter, quantization noise is substantial and, therefore, the error is too large to represent the input signal X_{in} . In the case of a ΔM modulation system whose data rate is on the order of 20 kb/S, for example, the demodulated output when simply applied to a filter would result in a significant degree of quantization noise or a noticeable waveform distortion due to quantization, the attainable sound quality being quite poor. Figure 2D represents the error signal X_{19} reproduced at the receiver. While the error signal X_{19} corresponds to the signal X_4 (Figure 2B) which has been left unquantized by the ΔM modulator 1, its

waveform is somewhat blunted compared to the signal X_4 due to frequency band limitation. Figure 2E indicates the output X_{20} of the adder 20 representative of the sum of the signal X_{18} (Figure 2C) and the signal X_{19} (Figure 2D). It will be seen that the summation output X_{20} shown in Figure 2E is quite analogous in waveform to the input signal X_{in} at the transmitter (Figure 2A). Although the signal X_{20} is locally somewhat angled, high quality reproduction of the first analog audio signal X_{21} is achievable by applying it to the low pass filter 21.

Now, from the privacy standpoint, the system shown and described is perfect regarding the transmission path as an FM path, since information converted into a digital audio signal is subjected to digital processing for privacy. Regarding the transmission path as an AM path, the error signal failed to be converted into a digital signal is sent out from the transmitter to the receiver. However, the privacy will not be detrimented in practice in view of the fact that a majority of the energy components representative of audio information is transmitted as a digital signal, that is, it is difficult to extract the audio information from the remaining error signal. In this manner, the present invention is successful to fulfill two different considerations at the same time: privacy concerning the transmission path, and quality concerning a reproduced audio signal.

Referring to Figure 3, another embodiment of the present invention is shown which includes a transmitter 200 and a receiver 201. The transmitter 200 includes a ΔM modulator 1, an encryption circuit 2, a subtractor 4, a low pass filter 5, a bandpass filter 24, and a transmitting section 25 which are respectively identical in function with those shown in Figure 1. Therefore, the operation of these structural elements will not be described any further for simplicity purpose.

What distinguishes the transmission system shown in Figure 3 from that of Figure 1 is the manner of transmission of an error signal. As shown in Figure 3, the data X_2 output from the encryption circuit 2 is amplitude-modulated at an AM modulator 22 by the error signal X_6 output from the low pass filter 5. Again, the degree of modulation at the modulator 22 is so selected as not to enhance the transmission error rate of the digital audio signal. The error signal will be satisfactorily transmitted if data is subjected to amplitude modulation. For example, assuming a transmission path whose data rate is 20 kb/S, frequency components not higher than 3 kHz effective as an audio signal can be readily entrained out of the entire error signal by a wave having a rate 20 kb/S. The output of the AM modulator 22 is a frequency-modulated by the FM modulator 3 and, then, sent out through the antenna 7.

The receiver 201 in Figure 3, like the receiver 101 in Figure 1, includes an antenna 11, a receiving section 12 for high frequency to intermediate frequency conversion, a limiter 13, an FM dis-

criminator 14, a decryption circuit 15, a ΔM demodulator 16, a clock recovery circuit 17, an adder 20, and a low pass filter 21. Thus, the receiver 201 operates in the same manner as the receiver 101 in processing an audio signal which comes in through the antenna 11 as a digital privacy signal.

In the second embodiment shown in Figure 3, in order to reproduce a received error signal, use is made of an AM detector 23 in the receiver which measures an amplitude from a received data waveform X_{14} output from the FM demodulator 14. The output of the AM detector 23 is delayed by a delay circuit 19 by an amount which, as previously discussed, is equal to the time lag between the transmission of a digital signal which the ΔM modulator 1 of the transmitter provided by the conversion of an audio signal and the appearance of an analog signal from the ΔM demodulator 16 of the receiver.

As discussed in conjunction with the first embodiment, it is more preferable to listen to the summation signal of the signal X_{18} output from the ΔM demodulator 16 and the error signal X_{19} than to listen to the demodulator output X_{18} only, regarding the quality of audio signal reproduction. Based on the same principle as stated in the first embodiment, the second embodiment of Figure 3 insures privacy in the transmission path.

In the embodiment of Figure 3, the modulator 22 comprises an AM modulator and use is made of an AM detector 23 accordingly. This is not restrictive, however, and may be replaced by any other suitable modulation system if the data rate is sufficiently high compared to the audio band (3 kHz). For example, modulation may be effected on the phase of data at the transmitter and detected at the receiver.

Furthermore, a ΔM demodulator has been employed in each of the foregoing embodiments in order to modulate an analog audio signal into a digital audio signal or to demodulate a digital audio signal into an analog audio signal. It will be apparent to those skilled in this art, however, that such is only illustrative and may be substituted for by a demodulator operable with any other digital pulse demodulation principle (e.g. ordinary PCM (pulse code modulation) or DPCM (differential pulse code modulation)).

In summary, it will be seen that the present invention converts an analog audio signal into a digital signal and sends it out after digital encryption for privacy, while also transmitting the remaining error signal which has failed to be converted into a digital signal. In the transmission line, therefore, the digital privacy signal and the hardly eligible error signal insure privacy in combination. Meanwhile, when common channel interference occurs in the radio system, another receiver is capable of overhearing nothing but noise if the incoming digital audio signal is converted into an analog signal, due to a different privacy code assigned thereto. Adding the reproduced error signal to such an analog signal would allow no information to be eavesdropped at all.

Concerning the quality of audio signal reproduction, the receiver is constructed to compensate a demodulated analog signal by adding a received error signal thereto. This reproduces an audio signal quite analogous in waveform to a transmitter input signal, thereby promoting high quality audio signal reproduction.

Claims

1. A privacy signal transmission system comprising:

a transmitter (100; 200) including digital pulse modulator means (1) for converting a first analog signal (X_{in}) into a first digital signal (X_1), extractor means (10, 4) for extracting a first analog error signal (X_4) representative of a difference between a second analog signal (X_{10}) provided by analog conversion of the first digital signal (X_1) and the first analog signal (X_{in}), and transmission means (25, 7) for transmitting the first analog error signal (X_4 , X_5) and the first digital signal (X_1); and a receiver (101; 201) including means (12, 13, 14, 18, 19; 23, 19) for receiving the first analog error signal and the first digital signal to individually generate a second analog error signal (X_{19}) and a second digital signal (X_{15}), digital pulse demodulator means (16) for converting the second digital signal (X_{15}) into a third analog signal (X_{18}), and reproduction means (20, 21) for reproducing the first analog signal by adding the second analog error signal (X_{19}) to the third analog signal (X_{18}), characterized in that the transmitter further comprises encryption means (2) connected between the digital pulse modulator means (1) and the transmission means (25, 7), for converting only the first digital signal (X_1) into a first digital privacy signal (X_2), thereby transmitting the first digital privacy signal (X_2), instead of the first digital signal (X_1) to the receiver; and the receiver further comprises decryption means (15) connected between the means (12, 13, 14, 18, 19; 23, 19) and the digital pulse demodulator means (16) for converting only the first digital privacy signal (X_2) into the second digital signal (X_{15}).

2. A system as claimed in claim 1, in which the digital pulse modulator means comprises a ΔM modulator (1).

3. A system as claimed in claim 1 or 2, in which the digital pulse demodulator means comprises a ΔM demodulator means (16).

4. A system as claimed in any one of claims 1 to 3, in which the transmission means (100) comprises frequency modulator means (3) for frequency-modulating a carrier with the first digital privacy signal (X_2), amplitude modulator means (6) for amplitude-modulating an output of said frequency modulator means (3) with the first error signal (X_5) and means for transmitting an output of said amplitude modulator means (25, 7).

5. A system as claimed in any one of claims 1 to 3, in which the transmission means (200) comprises amplitude modulator means (22) for amplitude-modulating the first digital privacy signal (X_2) with the first error signal (X_5), fre-

quency modulator means (3) for frequency-modulating a carrier with an output of said amplitude modulator means (22), and means (25, 7) for transmitting an output of said frequency modulator means (3).

6. A system as claimed in any one of claims 1 to 5, in which the transmission means comprises means for phase-modulating the first digital privacy signal with the error signal, frequency-modulating a carrier with the phase-modulated signal, and transmitting said frequency-modulated signal.

Patentansprüche

1. System zum Übertragen eines vertraulichen Signals mit einem Sender (100; 200) mit einem digitalen Impulsmodulator (1) zum Konvertieren eines ersten Analogsignals (X_{in}) in ein erstes Digitalsignal (X_1), einer Abrufeinrichtung (10, 4) zum Extrahieren eines ersten analogen Fehlersignals (X_4), das repräsentativ ist für einen Unterschied zwischen einem zweiten Analogsignal (X_{10}), das durch Analogkonversion des ersten Digitalsignals (X_1) gebildet wird, und dem ersten Analogsignal (X_{in}), und einer Sendereinrichtung (25, 7) zum Senden des ersten analogen Fehlersignals (X_4 , X_5) und des ersten Digitalsignals (X_1); und mit einem Empfänger (101; 201) mit Einrichtungen (12, 13, 14, 18, 19; 23, 19) zum Empfangen des ersten analogen Fehlersignals und des ersten Digitalsignals zum individuellen Generieren eines zweiten analogen Fehlersignals (X_{19}) und eines zweiten Digitalsignals (X_{15}), einem digitalen Impulsdemodulator (16) zum Konvertieren des zweiten Digitalsignals (X_{15}) in ein drittes Analogsignal (X_{18}) und mit einer Reproduziereinheit (20, 21) zum Reproduzieren des ersten Analogsignals durch Addieren des zweiten analogen Fehlersignals (X_{19}) zum dritten Analogsignal (X_{18}), dadurch gekennzeichnet, daß der Sender eine Verschlüsselungseinrichtung (2) aufweist, die zwischen dem digitalen Impulsmodulator (1) und der Sendeeinrichtung (25, 7) geschaltet ist, um lediglich das erste Digitalsignal (X_1) in das erste vertrauliche Digitalsignal (X_2) umzuwandeln und dadurch das erste vertrauliche Digitalsignal (X_2) anstelle des ersten Digitalsignals (X_1) zum Empfänger zu senden; und daß der Empfänger eine Entschlüsselungseinrichtung (15) aufweist, die zwischen der Einrichtung (12, 13, 14, 18, 19; 23, 19) und dem digitalen Impulsdemodulator (16) geschaltet ist, um lediglich das erste vertrauliche Digitalsignal (X_2) in das zweite Digitalsignal (X_{15}) umzuwandeln.

2. System nach Anspruch 1, dadurch gekennzeichnet, daß der digitale Impulsmodulator einen ΔM -Modulator (1) aufweist.

3. System nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß der digitale Impulsdemodulator eine ΔM -Demodulatoreinrichtung (16) aufweist.

4. System nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß der Sender (100) einen Frequenzmodulator (3) zum Frequenzmo-

Concerning the quality of audio signal reproduction, the receiver is constructed to compensate a demodulated analog signal by adding a received error signal thereto. This reproduces an audio signal quite analogous in waveform to a transmitter input signal, thereby promoting high quality audio signal reproduction.

Claims

1. A privacy signal transmission system comprising:

a transmitter (100; 200) including digital pulse modulator means (1) for converting a first analog signal (X_{in}) into a first digital signal (X_1), extractor means (10, 4) for extracting a first analog error signal (X_4) representative of a difference between a second analog signal (X_{10}) provided by analog conversion of the first digital signal (X_1) and the first analog signal (X_{in}), and transmission means (25, 7) for transmitting the first analog error signal (X_4 , X_5) and the first digital signal (X_1); and a receiver (101; 201) including means (12, 13, 14, 18, 19; 23, 19) for receiving the first analog error signal and the first digital signal to individually generate a second analog error signal (X_{15}) and a second digital signal (X_{15}), digital pulse demodulator means (16) for converting the second digital signal (X_{15}) into a third analog signal (X_{16}), and reproduction means (20, 21) for reproducing the first analog signal by adding the second analog error signal (X_{15}) to the third analog signal (X_{16}), characterized in that the transmitter further comprises encryption means (2) connected between the digital pulse modulator means (1) and the transmission means (25, 7), for converting only the first digital signal (X_1) into a first digital privacy signal (X_2), thereby transmitting the first digital privacy signal (X_2), instead of the first digital signal (X_1) to the receiver; and the receiver further comprises decryption means (15) connected between the means (12, 13, 14, 18, 19; 23, 19) and the digital pulse demodulator means (16) for converting only the first digital privacy signal (X_2) into the second digital signal (X_{15}).

2. A system as claimed in claim 1, in which the digital pulse modulator means comprises a ΔM modulator (1).

3. A system as claimed in claim 1 or 2, in which the digital pulse demodulator means comprises a ΔM demodulator means (16).

4. A system as claimed in any one of claims 1 to 3, in which the transmission means (100) comprises frequency modulator means (3) for frequency-modulating a carrier with the first digital privacy signal (X_2), amplitude modulator means (6) for amplitude-modulating an output of said frequency modulator means (3) with the first error signal (X_5) and means for transmitting an output of said amplitude modulator means (25, 7).

5. A system as claimed in any one of claims 1 to 3, in which the transmission means (200) comprises amplitude modulator means (22) for amplitude-modulating the first digital privacy signal (X_2) with the first error signal (X_5), fre-

quency modulator means (3) for frequency-modulating a carrier with an output of said amplitude modulator means (22), and means (25, 7) for transmitting an output of said frequency modulator means (3).

6. A system as claimed in any one of claims 1 to 5, in which the transmission means comprises means for phase-modulating the first digital privacy signal with the error signal, frequency-modulating a carrier with the phase-modulated signal, and transmitting said frequency-modulated signal.

Patentansprüche

1. System zum Übertragen eines vertraulichen Signals mit einem Sender (100; 200) mit einem digitalen Impulsmodulator (1) zum Konvertieren eines ersten Analogsignals (X_{in}) in ein erstes Digitalsignal (X_1), einer Abrufeinrichtung (10, 4) zum Extrahieren eines ersten analogen Fehlersignals (X_4), das repräsentativ ist für einen Unterschied zwischen einem zweiten Analogsignal (X_{10}), das durch Analogkonversion des ersten Digitalsignals (X_1) gebildet wird, und dem ersten Analogsignal (X_{in}), und einer Sendereinrichtung (25, 7) zum Senden des ersten analogen Fehlersignals (X_4 , X_5) und des ersten Digitalsignals (X_1); und mit einem Empfänger (101; 201) mit Einrichtungen (12, 13, 14, 18, 19; 23, 19) zum Empfangen des ersten analogen Fehlersignals und des ersten Digitalsignals zum individuellen Generieren eines zweiten analogen Fehlersignals (X_{15}) und eines zweiten Digitalsignals (X_{15}), einem digitalen Impulsdemodulator (16) zum Konvertieren des zweiten Digitalsignals (X_{15}) in ein drittes Analogsignal (X_{16}) und mit einer Reproduziereinheit (20, 21) zum Reproduzieren des ersten Analogsignals durch Addieren des zweiten analogen Fehlersignals (X_{15}) zum dritten Analogsignal (X_{16}), dadurch gekennzeichnet, daß der Sender eine Verschlüsselungseinrichtung (2) aufweist, die zwischen dem digitalen Impulsmodulator (1) und der Sendereinrichtung (25, 7) geschaltet ist, um lediglich das erste Digitalsignal (X_1) in das erste vertrauliche Digitalsignal (X_2) umzuwandeln und dadurch das erste vertrauliche Digitalsignal (X_2) anstelle des ersten Digitalsignals (X_1) zum Empfänger zu senden; und daß der Empfänger eine Entschlüsselungseinrichtung (15) aufweist, die zwischen der Einrichtung (12, 13, 14, 18, 19; 23, 19) und dem digitalen Impulsdemodulator (16) geschaltet ist, um lediglich das erste vertrauliche Digitalsignal (X_2) in das zweite Digitalsignal (X_{15}) umzuwandeln.

2. System nach Anspruch 1, dadurch gekennzeichnet, daß der digitale Impulsmodulator einen ΔM -Modulator (1) aufweist.

3. System nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß der digitale Impulsdemodulator eine ΔM -Demodolatoreinrichtung (16) aufweist.

4. System nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß der Sender (100) einen Frequenzmodulator (3) zum Frequenzmo-



dulieren eines Trägers mit dem ersten vertraulichen Digitalsignal (X_2), einen Amplitudenmodulator (6) zum Amplitudenmodulieren eines Ausgangssignals des Frequenzmodulators (3) mit dem ersten Fehlersignal (X_5) und eine Einrichtung zum Senden des Ausgangssignals des Amplitudenmodulators (25, 7) aufweist.

5. System nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß der Sender (200) einen Amplitudenmodulator (22) zum Amplitudenmodulieren des ersten vertraulichen Digitalsignals (X_2) mit dem ersten Fehlersignal (X_5), einen Frequenzmodulator (3) zum Frequenzmodulieren eines Trägers mit einem Ausgangssignal des Amplitudenmodulators (22) und eine Einrichtung (25, 7) zum Senden eines Ausgangssignals des Frequenzmodulators (3) aufweist.

6. System nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, daß der Sender eine Einrichtung zum Phasenmodulieren des ersten vertraulichen Digitalsignals mit dem Fehlersignal, zum Frequenzmodulieren eines Trägers mit dem phasenmodulierten Signal und zum Senden des frequenzmodulierten Signals aufweist.

Revendications

1. Système de transmission de signal confidentiel comprenant:

— un émetteur (100; 200) comportant un moyen de modulateur d'impulsions numériques (1) pour transformer une premier signal analogique (X_{in}) en un premier signal numérique (X_1), un moyen d'extracteur (10, 4) pour extraire un premier signal d'erreur analogique (X_4) représentatif d'une différence entre un second signal analogique (X_{10}) fourni par la conversion analogique du premier signal numérique (X_1) et du premier signal analogique (X_{in}), et un moyen de transmission (25, 7) pour transmettre le premier signal d'erreur analogique (X_4 , X_5) et le premier signal numérique (X_1); et un récepteur (101; 201) comprenant des moyens (12, 13, 14, 18, 19; 23, 19) pour recevoir le premier signal d'erreur analogique et le premier signal numérique afin de produire individuellement un second signal d'erreur analogique (X_{19}) et un second signal numérique (X_{15}); un moyen de démodulateur d'impulsions numériques (16) pour transformer le second signal numérique (X_{15}) en troisième signal analogique (X_{16}), et un moyen de reproduction (20, 21) pour reproduire le premier signal analogique en ajoutant le second signal d'erreur analogique

(X_{19}) au troisième signal analogique (X_{16}), caractérisé en ce que l'émetteur comprend en outre un moyen de chiffage (2) monté entre le moyen de modulateur d'impulsions numériques (1) et le moyen de transmission (25, 7) pour transformer seulement le premier signal numérique (X_1) en un premier signal numérique confidentiel (X_2), d'où la transmission du premier signal numérique confidentiel (X_2), à la place du premier signal numérique (X_1), au récepteur; et le récepteur comprend en outre un moyen de déchiffage (15) monté entre les moyens (12, 13, 14, 18, 19; 23, 19) et le moyen de démodulateur d'impulsions numériques (16) pour convertir seulement le premier signal numérique confidentiel (X_2) pour donner le second signal numérique (X_{15}).

2. Système selon la revendication 1, dans lequel le moyen de modulateur d'impulsions numériques comprend un modulateur ΔM (1).

3. Système selon la revendication 1 ou la revendication 2, dans lequel le moyen de démodulateur d'impulsions numériques comprend un moyen de démodulateur ΔM (16).

4. Système selon l'une quelconque des revendications 1 à 3, dans lequel le moyen de transmission (100) comprend un moyen de modulateur de fréquence (3) pour moduler en fréquence une porteuse avec le premier signal numérique confidentiel (X_2), un moyen de modulateur d'amplitude (6) pour moduler en amplitude une sortie du moyen de modulateur de fréquence (3) avec le premier signal d'erreur (X_5) et un moyen pour transmettre une sortie du moyen de modulateur d'amplitude (25, 7).

5. Système selon l'une quelconque des revendications 1 à 3, dans lequel le moyen de transmission (200) comprend un moyen de modulateur d'amplitude (22) pour moduler en amplitude le premier signal numérique confidentiel (X_2) avec le premier signal d'erreur (X_5), un moyen de modulateur de fréquence (3) pour moduler en fréquence une porteuse avec une sortie du moyen de modulateur d'amplitude (22), et un moyen (25, 7) pour transmettre une sortie du moyen de modulateur de fréquence (3).

6. Système selon l'une quelconque des revendications 1 à 5, dans lequel le moyen de transmission comprend un moyen pour moduler en phase le premier signal numérique confidentiel avec le signal d'erreur, pour moduler en fréquence une porteuse avec le signal modulé en phase, et transmettre le signal modulé en fréquence.

