(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 2 178 235 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
21.04.2010 Bulletin 2010/16

(51) Int Cl.:
H04K 1/04 *(2006.01)*

(21) Application number: **08390001.9**

(22) Date of filing: **17.10.2008**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MT NL NO PL PT RO SE SI SK TR
Designated Extension States:
AL BA MK RS

(71) Applicant: **SignalGeneriX Ltd.**
3504 Limassol (CY)

(72) Inventors:
- **Kounoudes, Anastasis**
  c/o SignalGeneriX Ltd.
  3504 Limassol (CY)
- **Doumenis, Demosthenis**
  c/o SignalGeneriX Ltd.
  3504 Limassol (CY)
- **Doukas, Nikolaos**
  c/o SignalGeneriX Ltd.
  3504 Limassol (CY)

(74) Representative: **Röthinger, Rainer**
Wuesthoff & Wuesthoff
Patent- und Rechtsanwälte
Schweigerstrasse 2
81541 München (DE)

(54) Encryption of information signals

(57) The invention relates to techniques for encrypting and decrypting information signals, for example digital voice signals in mobile communications, based on polyphase filter banks. A method embodiment of the invention for encrypting information signals comprises the steps of splitting, based on multiple analysis subband filters, an input information signal into a set of signal subbands; performing an encryption operation on one or more subbands of the set of subbands; and synthesizing, based on multiple synthesis subband filters, the encrypted set of subbands into an output information signal, wherein a particular synthesis filter is the product of all analysis filters except the analysis filter corresponding in subband to the particular synthesis filter.

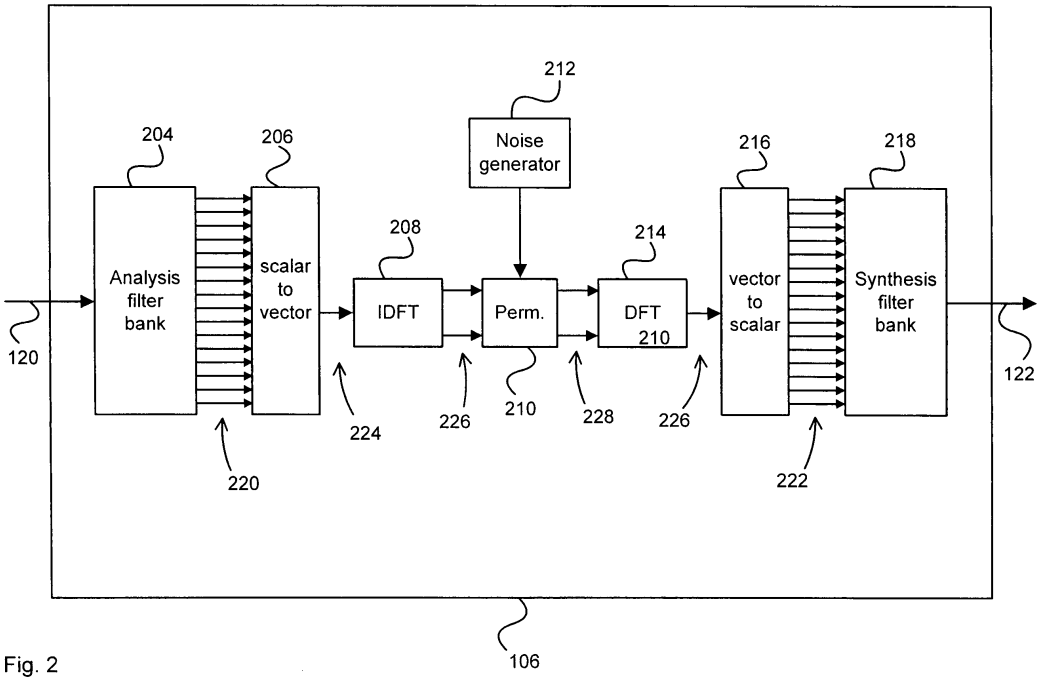


Fig. 2

EP 2 178 235 A1

Description

Technical Field

[0001] The invention relates to techniques for encrypting and decrypting information signals, for example digital voice signals. More particularly, the invention relates to the encryption and decryption of information signals based on polyphase filter banks.

Background

[0002] Keeping privacy in telecommunications, for example telephone conversations, is an important requisite in many areas, such as in business, governmental or military fields. While various techniques for the encryption of for example voice or speech in real time exist, such techniques generally require considerable processing power. For this reason, encryption technologies are typically not included as a standard feature in communication devices. Encryption solutions for mobile devices such as cellular phones additionally need to observe the particular requirements imposed by the limited available energy in such a device and the small dimensions thereof.

[0003] For these reasons voice encryption technologies are often provided as a separate unit (an 'add-on' device) to communication devices such as mobile phones. In principle, an analogue voice signal is captured by a microphone, digitized and input into the encryption add-on. After encryption, the add-on outputs the encrypted voice signal to the mobile phone. The encrypted signal is then transmitted via a mobile network to the receiving party, which may be another mobile phone. The encrypted signal is provided to a decryption add-on, which reverts the encryption and outputs the decrypted signal, for example back to the mobile phone.

[0004] One conventional technique for voice encryption is the subband analysis of speech signals by using polyphase filters and the encryption of the signal via permutation of individual subbands. On the one hand, such technology may avoid a complex synchronization procedure such as a key exchange between encryption device and decryption device. On the other hand, however, existing implementations of encryption and decryption devices based on polyphase filter banks typically lead to a considerable deterioration of speech quality which is due to the fact that an optimal reconstruction of the original voice signal is not achieved. Moreover, in many implementations confidentiality is compromised from time to time or depending on individual speakers, which appears to be due to the fact that the permutation of subbands as performed in the current implementations is not sufficient, such that the speech remains recognizable for at least some parts of the communication.

Summary

[0005] There is a demand for a realtime encryption and decryption technique for information signals such as voice signals, which achieves an appropriate level of confidentiality while also meeting further requirements such as those discussed above including, for example, minimizing complexity for a given degree of confidentiality, minimizing processing resources, minimizing energy consumption or minimizing size of an encryption or decryption device.

[0006] This demand is satisfied by a method of encrypting information signals. The method comprises the steps of splitting, based on multiple analysis subband filters, an input information signal into a set of signal subbands; performing an encryption operation on one or more subbands of the set of subbands; and synthesizing, based on multiple synthesis subband filters, the encrypted set of subbands into an output information signal, wherein a particular synthesis filter is the product of all analysis filters except the analysis filter corresponding in subband to the particular synthesis filter. In some implementations, each of the synthesis filters of the synthesis filter bank is configured in this way.

[0007] The above demand is further satisfied by a method of decrypting information signals. This method comprises the steps of splitting, based on multiple analysis subband filters, an input information signal into a set of signal subbands; performing a decryption operation on one or more subbands of the set of subbands; and synthesizing, based on multiple synthesis subband filters, the decrypted set of subbands into an output information signal, wherein a particular synthesis filter is the product of all analysis filters except the analysis filter corresponding in subband to the particular synthesis filter. In some implementations, each of the synthesis filters of the synthesis filter bank is configured in this way.

[0008] The above methods may be applied to any kind of digital (or analogue) information signal including for example digital audio signals or digital voice or speech signals.

[0009] The signal subbands may be interleaved subbands. The analysis and/or synthesis subband filters in both the above-outlined methods may be polyphase subband (component) filters. The analysis subband filters may be chosen such that the product of all analysis subband filters is all-pass, i.e. an input information signal would pass a filter implementing the product of all analysis subband filters essentially unchanged.

[0010] In some implementations of either of the above methods, the multiple analysis filters may be derived from a single prototype subband filter. In this case, the configuration of the particular synthesis filter may be simplified. The prototype subband filter may for example be a (proprietary or standardized) low pass finite impulse response filter. The analysis / synthesis subband or component filters may be derived from the prototype filter using, e.g., a factorization technique.

[0011] In some realizations of either one of the above methods, the number of signal subbands can be varied in time. The time variation (or non-uniformity) of the signal subbands may be selected according to a complexity of the information to be encrypted or decrypted, which may be based on a measure of an energy distribution of the input information signal in frequency. The number of signal subbands may be chosen such that the bit distribution of the encoding is proportional to the complexity of information. The analysis filters and correspondingly the synthesis filters may be adapted accordingly.

[0012] The encryption or decryption operation may comprise transforming the signal subbands into frequency subbands. For example, a Fourier transformation, Laplace transformation or Z-transformation may be performed. A corresponding inverse or back transformation may also be included in the encryption (decryption) operation. In some modes of either one of the methods, the analysis transformation may be an inverse Fourier or Z-transformation, while the synthesis transformation is a corresponding back transformation.

[0013] The encryption or decryption operation may comprise a permutation of at least two subbands. For example, in case the signal subbands are transformed into frequency subbands, two or more frequency subbands may be permuted. In some implementations, the permutation of subbands may be varied in time. The subbands to be currently permuted may either be signalled from an encrypting device to a decrypting device, or the permutation may be controlled by a control scheme which is in the same way or similarly implemented in both devices. As an example, a permutation of subbands may be based on a signal energy contained therein. For instance, the two subbands containing most of the signal energy may be permuted with each other. This permutation could be reverted in the decryption operation.

[0014] Additionally or alternatively to permuting subbands, the encryption operation may comprise replacing at least one subband by noise. The noise has to be configured such that the output information signal is unrecognisable with high probability. A corresponding decryption operation may comprise removing noise from at least one subband based on, for example, the detection that a noise level in a subband exceeds a predetermined threshold or the detection of a pre-defined, particular signature imprinted on the noise by the encryption operation.

[0015] The above-mentioned demand is satisfied by a further method for encrypting information signals. This method comprises the steps of splitting, based on multiple analysis subband filters, an input information signal into a set of signal subbands; performing an encryption operation on one or more subbands of the set of subbands, wherein the encryption operation comprises replacing at least one subband by noise; and synthesizing, based on multiple synthesis subband filters, the encrypted set of subbands into an output information signal.

[0016] A corresponding method for decrypting information signals comprises the steps of splitting, based on multiple analysis subband filters, an input information signal into a set of signal subbands; performing a decryption operation on one or more subbands of the set of subbands, wherein the decryption operation comprises removing noise from at least one subband; and synthesizing, based on multiple synthesis subband filters, the decrypted set of subbands into an output information signal.

[0017] Various implementations, realizations and modes of these methods may be considered which are similar to the implementations, realizations and modes of the first pair of methods outlined further above.

[0018] The above-mentioned demand is further satisfied by a computer program product, which comprises program code portions for performing the steps of one or more of the methods and method aspects described herein when the computer program product is executed on one or more computing devices, for example one or both of an encryption device and a decryption device. The computer program product may be stored on a computer readable recording medium, such as a permanent or rewriteable memory within or associated with a computing device or a removable CD-ROM, DVD or USB-stick. Additionally or alternatively, the computer program product may be provided for download to a computing device, for example via a data network such as the Internet or a communication line such as a telephone line or wireless link.

[0019] Still further, the above-mentioned demand is satisfied by an encryption device for encrypting information signals. The device comprises a component adapted to split, based on multiple analysis subband filters, an input information signal into a set of signal subbands; a component adapted to perform an encryption operation on one or more subbands of the set of subbands; and a component adapted to synthesize, based on multiple synthesis subband filters, the encrypted set of subbands into an output information signal, wherein a particular synthesis filter is the product of all analysis filters except the analysis filter corresponding in subband to the particular synthesis filter.

[0020] The above-mentioned demand is also satisfied by a decryption device for decrypting information signals. The decryption device comprises a component adapted to split, based on multiple analysis subband filters, an input information signal into a set of signal subbands; a component adapted to perform a decryption operation on one or more subbands of the set of subbands; and a component adapted to synthesize, based on multiple synthesis subband filters, the decrypted set of subbands into an output information signal, wherein a particular synthesis filter is the product of all analysis filters except the analysis filter corresponding in subband to the particular synthesis filter.

[0021] Regarding still another aspect, the above-mentioned demand is also satisfied by a further encryption device for encrypting information signals. This device comprises a component adapted to split, based on mul-

tiple analysis subband filters, an input information signal into a set of signal subbands; a component adapted to perform an encryption operation on one or more subbands of the set of subbands, wherein the encryption operation comprises replacing at least one subband by noise; and a component adapted to synthesize, based on multiple synthesis subband filters, the encrypted set of subbands into an output information signal.

[0022] A corresponding device for decrypting information signals also satisfies the above demand and comprises a component adapted to split, based on multiple analysis subband filters, an input information signal into a set of signal subbands; a component adapted to perform a decryption operation on one or more subbands of the set of subbands, wherein the decryption operation comprises removing at least one subband which represents noise; and a component adapted to synthesize, based on multiple synthesis subband filters, the decrypted set of subbands into an output information signal.

[0023] The abovementioned demand is further satisfied by an encryption (decryption) device comprising the encryption device as outlined above and the decryption device as outlined above. The encryption (decryption) device may be adapted to the encryption (decryption) of voice or speech signals and may be particularly configured as an add-on device for mobile phones.

[0024] The abovementioned demand is still further satisfied by a communication device, wherein the communication device comprises at least one of the encryption device and the decryption device as outlined above. The communication device may comprise a mobile phone, wherein the encryption device and/or decryption device may be implemented as hardware, software, or a combination thereof. Another implementation of the communication device comprises a headset connectable to a mobile phone. For example, the headset may be an external headset with processing capabilities for connection with a mobile phone via Bluetooth or a similar wireless connection technique.

[0025] Any of the above-outlined devices may be implemented based on an FPGA (Field-Programmable Gate Array). Additionally or alternatively, at least a portion of a circuitry of any one of the above-outlined devices may be adapted for parallel processing. For example, the parallel processing may be realized based on the aforementioned prototype subband filter. An implementation of the above-mentioned headset may comprise an encryption and/or decryption device implemented on an FPGA with parallel processing capabilities.

Brief Description of the Drawings

[0026] In the following, the invention will further be described with reference to exemplary embodiments illustrated in the figures, in which:

Fig. 1 schematically illustrates an embodiment of a system for encrypting and decrypting an information signal;

Fig. 2 illustrates functional blocks of an encryption device of the system of Fig. 1;

Fig. 3 is a flow diagram illustrating an operation of the encryption device of Fig. 2;

Fig. 4 illustrates functional blocks of a decryption device of the system of Fig. 1;

Fig. 5 is a flow diagram illustrating an operation of the decryption device of Fig. 4;

Fig. 6 is a flow diagram illustrating encryption operations performed by the encryption device of Fig. 2;

Fig. 7 is a flow diagram illustrating decryption operations performed by the decryption device of Fig. 4; and

Figs. 8a-d illustrate functional aspects of the analysis / synthesis filters of the devices of Figs. 2 and 4.

Detailed Description of Preferred Embodiments

[0027] In the following description, for purposes of explanation and not limitation, specific details are set forth in order to provide a thorough understanding of the current invention. It will be apparent to one skilled in the art that the current invention may be practiced in other embodiments that depart from these specific aspects. For example, the skilled artisan will appreciate that the current invention may be practised not only with mobile (cellular, cordless) phones or more general with mobile or wireless communications, but also with wireline communications, i.e. wireline, landline or stationary phones including, e.g. IP phones ("Voice over IP").

[0028] The techniques described below may not only be applied to encryption and decryption of digital voice or speech signals, but to any kind of audio signals or more generally information signals including, for example, video signals, facsimilie data, electronic files (file transfer) or electronic data. Besides that, the techniques described herein may not only be used in conjunction with digital signal processing, but also analogue signal processing.

[0029] Those skilled in the art will further appreciate that functions explained hereinbelow may be implemented using individual hardware circuitry, but also using software functioning in conjunction with a programmed microprocessor, field-programmable gate array (FPGA), application specific integrated circuit (ASIC) and/or one or more digital signal processors (DSPs). Further, instead of being provided as an add-on to, e.g., cellular phones, an encryption and/or decryption device may also

be implemented purely software-based depending on the processing capabilities of current or future general purpose processing hardware available for, e.g., mobile phones.

[0030] Fig. 1 illustrates an embodiment of a system 100 for the encryption and decryption of digital audio signals. The system comprises an analogue audio input device 102, an Analogue-to-Digital(A/D) unit 104, an encryption device 106 and a cellular phone 108 in communication via a mobile network 110 with a receiving mobile phone 112, a decryption device 114, a Digital-to-Analogue (D/A) unit 116 and an analogue audio output device 118. The audio input device 102 may be a microphone, while the audio output device 118 may be a loudspeaker.

[0031] The encryption device 106 may be a hardware add-on which may or may not be specifically adapted to the mobile phone 108. For example, the encryption device 106 may be connected to a conventional interface to the mobile phone 108, such as a headset interface as it is conventionally used for hands-free operation of mobile phones. In this way, the encryption device may replace a headset or may be connected in between the headset and the mobile phone. The A/D-unit 104 may be provided on a common hardware with either one or both of the microphone 102 and encryption device 106 or may be provided as a stand-alone unit. In some configurations the audio input 102 may be a microphone integrated in mobile phone 108.

[0032] A user speaks into the audio input device 102, which generates an analogue electrical representation of the voice or speech input. The electrical signal is provided to the A/D-unit 104, which samples the signal and generates a digital representation 120 thereof. The digital voice signal 120 is input to the encryption device 106, which encrypts the signal as will be described in detail further below. The encrypted output signal 122 is provided to the mobile phone 108 in digital or analogue form. In the embodiment described here it is assumed that the encryption device 106 outputs digital encrypted voice signals.

[0033] The signal 122 provided to the mobile phone 108 is transmitted via the mobile network 110 towards the receiving party, i.e. mobile phone 112. From there, the received encrypted voice signal is forwarded 124 to the decryption device 114. It depends on the details of the implementation whether the received encrypted voice signal 124 is provided to the decryption device 114 in digital or analogue form. In the embodiment described here, it is assumed that the signal 124 is input to the decryption device as a digital signal.

[0034] The decryption device 114 decrypts the encrypted voice signal 124. The decrypted voice signal 126 is fed to the D/A-unit 116 which provides an analogue representation of the audio signal 126 to the audio output 118. The decryption device 114 may, for example, be connected in between the mobile phone 112 and a headset which includes the D/A-unit 116 and audio output 118. As one alternative, the D/A-unit 116 may be implemented on a common hardware with the decryption device 114. In some configurations the audio output 118 may be a loudspeaker 118 integrated in mobile phone 112.

[0035] Any of the encryption device 106 and the decryption device 114 may, for example, be implemented on an FPGA platform and may, depending on the concrete operational environment, include A/D-converter and/or D/A-converter, although these are illustrated as separate units in Fig. 1. An encryption device (decryption device) may further comprise various connectors for microphone, earphones, USB port, Ethernet interface, RS-232 port, etc.

[0036] Fig. 2 illustrates functional building blocks of the encryption device 106 of Fig. 1. The input voice signal 120 is processed by an analysis filter bank 204, a scalar-to-vector conversion unit 206, a transformation component 208, a permutation component 210 and a noise generator 212 associated therewith, a further transformation component 214, a vector-to-scalar conversion unit 216 and a synthesis filter bank 218, which outputs the encrypted audio signal 122 (cf. Fig. 1).

[0037] An operation of the encryption device 106 will now be described with reference to the flow diagram of Fig. 3. Generally, the encryption device 106 operates to encrypt digital information signals, more particularly the digital voice signal 120. In other embodiments, an input information signal may be an analogue signal. An encryption device may then comprise an A/D-unit similar to A/D-unit 104 of Fig. 1.

[0038] In step 302, the input voice signal 120 is provided to the analysis filter bank 204, which operates to split the input voice signal 120 into a set of signal subbands. It is assumed that the filter bank 204 is a polyphase filter bank comprising multiple analysis subband filters (component filters) generating a set of interleaved subbands. While in the example illustrated in Fig. 2 the input signal 120 is split into 16 subbands 220, in other embodiments a smaller or larger number of subbands may be configured. The multiple analysis filters of the filter bank 204 may be derived from a single prototype subband filter, which may be a standardized or a proprietary lowpass finite impulse response (FIR) filter. The desired number of analysis subband filters (polyphase component filters), may be derived therefrom by using a factorization technique.

[0039] In step 304, at least one encryption operation is performed on one or more subband of the set of subbands 220 generated by the filter bank 204. Details on the encryption operations will be described with reference to Fig. 6 further below. As a result of the encryption operations performed, in step 306 an encrypted set of subbands 222 is provided to the synthesis filter bank 218, which operates to synthesize the encrypted set of subbands 222 into the output voice signal 122. The filter bank 218 may be configured similarly as the analysis filter bank 204, i.e. may also be a polyphase filter bank comprising multiple (synthesis) subband filters. As will be discussed

further below, the synthesis filters are adjusted in a way complementary to the analysis filters of filter bank 204. Specifically, each of the synthesis filters is a product of all analysis filters of filter bank 204 except the analysis filter which corresponds in subband to the particular synthesis filter. The reasons for this choice will be discussed with reference to Figs. 8a-8d.

[0040] Fig. 4 illustrates functional building blocks of the decryption device 114 of Fig. 1. The encrypted input voice signal 124 is processed by an analysis filter bank 402, a scalar-to-vector conversion unit 404, a transformation component 406, a permutation component 408, a noise remover 410, a further transformation component 412, a vector-to-scalar conversion unit 414 and a synthesis filter bank 416, which outputs the decrypted audio signal 126 (cf. Fig. 1).

[0041] An operation of the decryption device 114 will be described with reference to the flow diagram of Fig. 5. Generally, the decryption device 114 operates to decrypt digital information signals, more particularly the digital voice signal 124. In other embodiments, an encrypted input information signal may be an analogue signal. A decryption device may then comprise an A/D-unit. Generally, the components 402 - 416 may be configured similar in various aspects to the components 204 - 218 of the encryption device 106. A repetition of such aspects is therefore omitted.

[0042] In step 502, the analysis filter bank 402 operates to split the (encrypted) input voice signal 124 into a set of signal subbands. The analysis subband filters of the filter bank 402 may be configured similar to the filters of filter bank 204 in the encryption device 106. For example, the same prototype filter may be used to derive the filters for the banks 204 and 402 therefrom. In step 504, at least one decryption operation is performed on one or more of the set of subbands 418 output by the analysis filter bank 402. Details on the decryption operations will be described with reference to Fig. 7 below. In step 506, the decrypted set of subbands 420 is provided to the synthesis filter bank 416, which operates to synthesize, based on multiple synthesis subband filters, the decrypted set of subbands 420 into the decrypted output voice signal 126 (cf. Fig. 1).

[0043] Fig. 6 illustrates encryption operations which may be performed in the course of step 304 of Fig. 3 and which are described taking reference of the encryption device 106 in Fig. 2. In step 602 the signal subbands generated in filter bank 204 are transformed into frequency subbands. Specifically, the scalar-to-vector conversion unit 206 converts the signal subbands 220 into a vector 224 which is then input into the transformation component 208. This component performs an Inverse Discrete Fourier Transformation (IDFT) of the input vector 224. The resulting output is a set of frequency subbands 226. It is to be noted that the scalar-to vector conversion unit 206 operates to specifically configure the subbands 220 for input to the IDFT component 208. In other embodiments, a component different from unit 206 may be provided. In still other embodiments, no component at all may be provided and the subbands generated by the filter bank may be input directly into a transformation component. Similar considerations hold for the vector-to-scalar conversion unit 216 discussed below.

[0044] In step 604, the permutation component 210 performs a permutation of at least two of the set of subbands 226. This permutation may be performed the same all the time or may be varied in time during the operation of the encryption device 106. A time variation of the permutation may be performed following a fixed predefined scheme and/or may be controlled dependent on properties of the voice signal to be encrypted. As an example, a signal energy may be detected for at least a subset of the set of frequency subbands. Permutations may then, for example, be performed on those subbands containing most of the signal energy. This will in typical situations lead to an appropriate encryption of voice or similar information carrying signals, as an insufficient scrambling due to a permutation of empty subbands is avoided. Further, the permutation process may be easily reverted in the decryption device without the need for an extra signalling. Consider a permutation of the two subbands containing most of the signal energy: Performing exactly the same processing in the decryption device would revert the permutation and would in this way decrypt the encrypted signal. However, in some embodiments in which time-varying encryption is applied, parameters for properly controlling a decryption may be signalled to the decryption device. Such signalling may be performed inline, i.e. embedded within the encrypted information signal, or in any other way.

[0045] In step 606, the noise generator 212 operates to replace at least one of the frequency subbands 226 by noise. The noise may be, for example, white noise which may or may not be randomly generated. An intensity of the noise has to be sufficient such that the speech signal becomes unrecognizable and that cryptoanalytic attacks on the encrypted information signal are prevented. The noise intensity may be predetermined or may be controlled based on, for example, a signal energy measured from one or more of the subbands or the input information signal 120. For instance, the signal energies measured for controlling a permutation process may also be used for controlling the noise to be injected into the signal. In some embodiments, an in-line signalling may be imprinted on the noise in order that the decryption device may properly control a decryption, as discussed above.

[0046] The subband(s) to be replaced by noise may be fixed. For example, a frequency subband known to generally carry low signal energy for the case of human speech may be chosen. Additionally or alternatively, based on a measurement of subband signal energies, one or more subbands containing a signal energy below a predetermined threshold or containing the lowest signal energy in the set of subbands may be selected for noise injection.

[0047] In step 608, the transformation component 214 perform the inverse transformation to the transformation performed by the transformation component 208. In the embodiment illustrated in Fig. 2, the transformation component 214 performs a Discrete Fourier transformation (DFT). The resulting vector 230 is fed to the vector-to-scalar conversion unit 216 which outputs the encrypted set of signal subbands 222 to the synthesis filter bank 218, as has been described already above.

[0048] While the steps 604 and 606 are illustrated in Fig. 6 as following on each other, it is to be noted that subband permutation and noise injection may be performed in any order and may also be performed in parallel to each other. Further, an encryption device may perform only one of these operations. For example, a particular encryption device may only perform the subband permutation or may only perform noise injection. Still other encryption devices may be set into different confidentiality modes according to a desired confidentiality level (security level). Such a level may be measured, for example, by estimates of the efforts (processing power) required for an attacker to decrypt the encrypted information signal. The device confidentiality modes may differ from each other by switching on or off or configuring in different ways one or more of the above encryption operations. Moreover, such a multi-mode encryption (or decryption) device may be manually or automatically adjusted to its decryption (or encryption) counterpart, which may be of a different model series etc., at the other end of the communication line.

[0049] Fig. 7 illustrates decryption operations which may be performed in the course of step 504 of Fig. 5 and which are described taking reference of the decryption device 114 of Fig. 4. It is generally to be noted that many units and components of the decryption device 114 may operate similarly to the corresponding units and components of the encryption device 106 (in some embodiments, all units and components may operate similar). In particular, the filter banks 402 and 416 of device 114 may exactly correspond to the filter banks 204 and 218 of device 106. In case of a combined device for encryption and decryption, which may be used in an ongoing communication to encrypt outgoing signals and decrypt incoming signals in an alternating fashion, one and the same combination of analysis filter bank and synthesis filter bank may be used for the encryption and the decryption. Thus, only a single analysis filter bank and a single synthesis filter bank may be required. Similarly, only one set of encryption and decryption components may be required for performing the encryption and decryption operations (however, the noise injection cannot simply be reverted).

[0050] In step 702 the encrypted signal subbands 418 are transformed into frequency subbands. The components 404 and 406 of the encryption device 114 may operate similar to the components 206 and 208 of the encryption device in Fig. 2; therefore the detailed description of step 602 applies similarly also to the components 404 and 406. The output of the transformation component 406 is a set of frequency subbands 422. In step 704, the permutation component 408 operates to perform a permutation of at least two subbands from the set of subbands 422. In order for a successful decryption, the permutation performed by the permutation component 210 in the encryption device 106 has to be reverted. How to correctly reverse the permutation process performed in the encryption device 106 depends on the details thereof.

[0051] In case a fixed permutation scheme is implemented by the permutation device 210, the reverse permutation scheme will also be a fixed scheme, and may even be exactly the same scheme. In case the permutation is varied in time according to a prescribed scheme, the component 408 may apply a similar scheme, however, some time synchronization would then be required between components 210 and 408. In case of a random permutation scheme, a more extensive signalling would be required which indicates the momentary permutation configuration to the permutation component 408. Such signalling mechanism may comprise in-line signalling, which may for example be imprinted on the noise by the noise generator 212 in Fig. 2.

[0052] In case a permutation is controlled by parameters related to properties of the current information signal, both the permutation components 210 and 408 may determine parameters from the (encrypted) signal in the same way. This requires that parameters are used as permutation control parameters which are not changed by the permutation or any other encryption operations. As an example, the signal energy contained in each of the frequency subbands may be determined. This parameter set will not be changed by permutation, and noise injection may preferably only affect low energy subbands. Thus, in case the encryption permutation comprises permuting the two frequency bands containing most of the signal energy, this can be reverted in the decryption stage without any signalling. In this specific case, the permutation component 408 may act exactly similar as the permutation component 210 in order to revert the permutation performed therein.

[0053] In step 706, the noise remover 410 operates to remove noise from those subbands to which noise has been added by the noise generator 212 in the encryption device 106. In case the noise generator 212 replaces a signal by noise in fixedly prescribed subbands, the noise remover 410 may replace noise by silence (zero signal energy) in these subbands. In case the noise generator 212 determines subbands with low signal energy, the noise remover 410 has to detect the one or more subbands of the set of subbands 422 which contain noise. The component 410 requires decision logic in this respect in order to decide whether a subband is filled, for example, by white noise. In case the noise generator 212 in the encryption device 106 imprints a particular "noise ID" signature on the noise, the noise remover 410 may specifically search for such noise ID in the set of frequency subbands 422. In case such a noise ID is detected in a

frequency subband, the signal in this subband is replaced by silence.

[0054] In step 708, the transformation components 412 and 414 act to back-transform the decrypted frequency subbands 424. The back transformation may be performed in a way as has been described with reference to the components 214 and 216 of the encryption device 106; this description may therefore be referred to.

[0055] The sequence of steps 704 and 706 may be performed in any order, parallel to each other, or only one of these steps may be performed. The corresponding discussion of steps 604 and 606 is referred to.

[0056] Turning to the configuration in detail of the filter banks in the encryption device 106 and decryption device 114, it is generally to be noted that the analysis and synthesis of the unencrypted voice signal in the encryption device 106 and of the encrypted voice signal in the decryption device 114 may be performed in the same way. Therefore, while for the sake of brevity in the following it is only referred to the analysis filter bank 204 and synthesis filter bank 218 of the encryption device 106, it is to be understood that these considerations hold similarly for the analysis filter bank 402 and the synthesis filter bank 416 of the decryption device 114.

[0057] In order to minimize speech deterioration during encryption and decryption of a voice signal, it is required that the synthesis subband filters are configured complementary to the analysis subband filters. More specifically, one or more of each of the filter functions for the synthesis subband filters may be configured as the product of all filter functions of the analysis filters except the filter function for the analysis filter corresponding in subband to the synthesis filter to be configured. A derivation is presented in the following proving plausibility of this concept.

[0058] The analysis filters (filter functions, polyphase components or subphase filters of the analysis filter bank) are denoted as E_i, i = 0, 1, ..., M-1; i.e., there are M polyphase components in the analysis filter bank. Further, H denotes the product of all analysis filters E_i, $H = \prod_i E_i$. Then, the concept that a particular synthesis filter should be the product of all analysis filters except the analysis filter corresponding in subband to the particular synthesis filter can be formulated as: The kth polyphase component in the synthesis filter bank should be H/Ek.

[0059] Fig. 8a schematically illustrates a signal processing system accepting a digital input signal x [n] and providing an output signal y [n]. The signal x [n] is processed by M branches, each branch applying the product of filter functions $F_1(z)$, $F_2(z)$, ..., $F_M(z)$ =u[n]. As the system of Fig. 8a is intended as a model for the encryption and decryption of an information signal without signal deterioration, it is demanded that the behaviour of the system should be all-pass, i.e. x[n] = y[n] (ignoring factors of 1/M). Let X(z), Y(z) and $U_k(z)$ represent the z-transforms of x(z), y(z) and $u_k(z)$. In this case,

$$U_k(z) = X(z)\, F_1(z)\, F_2(z) \ldots F_M(z),$$

and

$$Y(z) = \sum_{k=1}^{M} U_k(z) = M\, U_1(z)$$

[0060] For the system behaviour being all-pass, the filter functions have to satisfy the condition that $\prod_i F_i(z)$ is all-pass.

[0061] Fig. 8b illustrates the system of Fig. 8a wherein the filter functions F(z) have been rearranged. Still, the system behaviour is all-pass. An identity matrix may be inserted at the point A indicated in Fig. 8b, which also leaves the operation of the system unchanged.

[0062] In order to apply the system arranged as in Fig. 8b to the analysis and synthesis of information signals, we identify the filter functions F(z) with the polyphase coefficients E(z) and insert at the point A in Fig. 8b the product of the inverse and direct FFT matrices as the identity matrix. The resulting filter H is depicted in Fig. 8c. Insertion of H as shown in Fig. 8c into the system of Fig. 8b leads to the system of in Fig. 8d, which schematically illustrates an operation principle of encryption device 106 or decryption device 114. Note that the encryption or decryption operations discussed above are performed at the point indicated by arrow 802.

[0063] Assuming the filter bank (set of analysis filters) 204 of the device 106 is represented by the set of filters 804 in Fig. 8d, the filter bank 218 is represented by the set of filters 806 in Fig. 8d. The synthesis filters 806 are complementary to the analysis filters 804. For example, the synthesis filter corresponding to the analysis filter E_0 (i.e. the synthesis filter which corresponds to the analysis filter in the 0^{th} subband) is $E_1\, E_2 \ldots E_{M-1}$, the synthesis filter corresponding to the analysis filter E_1 is $E_0\, E_2 \ldots E_{M-1}$, etc., and the synthesis filter corresponding to the analysis filter E_{M-1} is $E_0\, E_1, .. E_{M-2}$.

[0064] In an embodiment in which the multiple analysis filters 804 are derived from a single prototype subband filter E, the synthesis filters 806 can be constructed based only on the prototype E in order to achieve an optimal reconstruction of the original input information signal x [n]. The original signal is approximated as

$$\hat{x}[n] = \frac{1}{M}\, y[n] \quad .$$

[0065] The above-described approach allows static and dynamic filter banks. For instance, the signal subbands can be varied in time, i.e. non-uniform filter banks can be realized, wherein the bit distribution of the encoding is proportional to the complexity of the information

carried in each subband. In this way, the signal subbands may be varied in time based on an energy distribution of the information signal in frequency. In other embodiments, the signal subbands may be varied in time according to a predefined scheme, which would have to be known to the receiver also. As a general example for a time-variation, in a non-uniform filter bank one or more of the vertical stages of the analysis and synthesis filter banks may be omitted leading to ½ or ¼ of the resolution.

[0066] The techniques proposed herein allow an optimized reconstruction of the original information signal after encryption and decryption. This is based on the fact that the filters used in the synthesis phase of the encryption and decryption devices are configured complementary to the filters used in the analysis phase, and this avoids alias components appearing in the synthesized signal. At the same time, the complementary approach allows a simplified construction of the synthesis filters, which are based on the analysis filters. In case a prototype (or sample or template) filter is used for construction of the analysis filters, the construction of the synthesis filters is also particularly simplified. In some embodiments the prototype filter, which may be provided e.g. in the form of a hardware implementation, is re-used for all filters of the analysis and synthesis filter banks. This allows a considerable reduction of resource usage, power consumption and size of the encryption or decryption device.

[0067] Further, employing subband-based technology allows parallel processing which in turn leads to low energy consumption and/or a minimization of latency being an important factor for man-man synchronous communication. The parallel processing may, for example, ensure that latency is uniformly distributed across the frequency spectrum. An FPGA may be used for implementing the parallel processing, which further reduces complexity and power consumption. In another approach to save processing efforts, the number of encoded and encrypted bits may be selected based on, for example, the distribution of signal energy over the frequency spectrum. The proposed techniques allow further optimizations related to a detection and deletion of silence periods in the voice signal.

[0068] The conventional encryption by frequency permutation often do not lead to a satisfying scrambling of the original signal, which is basically due to the relatively narrowband nature of human speech in a transmission channel. As proposed herein, confidentiality can be increased by exploiting the typically non-uniform distribution of energy in the information signal over the frequency spectrum. For example, a signal energy distribution of frequency subbands can be determined. Preferably subbands carrying high signal energy may be permuted. Moreover, it is proposed the option to add noise to subbands, for example subbands of low signal energy. Vice versa, a given desired level of confidentiality may be reached - employing the techniques proposed herein - with less processing efforts, which serves to reduce the processing efforts and required bandwidths. Further, a decryption device may be configured to ignore some of the frequency bands which the device knows to contain noise, which may lead to further savings in terms of processing resources, energy consumption, etc.

[0069] It is also proposed an encryption/decryption system with a configurable level of security (confidentiality), i.e. a system allowing an adjustment of the complexity of the encryption operation(s). For example, different security levels may be defined based on the number of frequency bands permuted and/or the number of frequency bands which are replaced by noise. The analysis of the (frequency) subbands, for example with regard to the distribution of the signal energy, may also be adjusted according to the required security level, i.e. complexity of encryption or decryption operations.

[0070] On the other hand, an encryption and/or decryption system operating according to the techniques proposed herein may also be implemented on a common hardware with a communication device, for example in a smartphone, notebook, etc.

[0071] The proposed techniques allow implementing an encryption device, decryption device or combined device on a simplified circuitry with small footprint and which is straightforwardly connectable to a communication device such as a mobile phone and with minimal requirements on processing power, memory and/or power supply. No further external peripheral devices may be needed.

[0072] While the current invention has been described in relation to its preferred embodiments, it is to be understood that this description is for illustrative purposes only. Accordingly, it is intended that the invention be limited only by the scope of the claims appended hereto.

Claims

1. A method of encrypting information signals, the method comprising the steps of

   - splitting (302), based on multiple analysis subband filters (204), an input information signal (120) into a set of signal subbands (220);
   - performing (304) an encryption operation on one or more subbands of the set of subbands; and
   - synthesizing (306), based on multiple synthesis subband filters (218), the encrypted set of subbands (222) into an output information signal (122),

   wherein a particular synthesis filter is the product of all analysis filters except the analysis filter corresponding in subband to the particular synthesis filter.

2. A method of decrypting information signals, the method comprising the steps of

- splitting (502), based on multiple analysis subband filters (402), an input information signal (124) into a set of signal subbands (418);
- performing (504) a decryption operation on one or more subbands of the set of subbands; and
- synthesizing (506), based on multiple synthesis subband filters (416), the decrypted set of subbands (420) into an output information signal (126),

wherein a particular synthesis filter is the product of all analysis filters except the analysis filter corresponding in subband to the particular synthesis filter.

3. The method according to claim 1 or 2, wherein the product of all analysis subband filters (204, 402) is all-pass.

4. The method according to any one of the preceding claims, wherein the multiple analysis filters (204, 402) are derived from a single prototype subband filter.

5. The method according to any one of the preceding claims, wherein the encryption or decryption operation comprises transforming (602) the signal subbands (220, 418) into frequency subbands (226, 422).

6. The method according to any one of the preceding claims, wherein the encryption or decryption operation comprises a permutation (604) of at least two subbands.

7. The method according to claim 6, wherein the permutation is varied in time.

8. The method according to any one of claims 1 and 3 to 7, wherein the encryption operation comprises replacing (606) at least one subband by noise.

9. The method according to any one of claims 1 and 3 to 8, wherein the number of signal subbands is varied in time.

10. A method of encrypting information signals, the method comprising the steps of

- splitting (302), based on multiple analysis subband filters (204), an input information signal (120) into a set of signal subbands (220);
- performing (304) an encryption operation on one or more subbands of the set of subbands, wherein the encryption operation comprises replacing (606) at least one subband with noise; and
- synthesizing (306), based on multiple synthesis subband filters (218), the encrypted set of subbands (222) into an output information signal (122).

11. A method of decrypting information signals, the method comprising the steps of

- splitting (502), based on multiple analysis subband filters (402), an input information signal (124) into a set of signal subbands (418);
- performing (504) a decryption operation on one or more subbands of the set of subbands, wherein the decryption operation comprises removing (706) noise from at least one subband; and
- synthesizing (506), based on multiple synthesis subband filters (416), the decrypted set of subbands (420) into an output information signal (126).

12. A computer program product comprising program code portions for performing the method according to any one of the preceding claims when the computer program product is executed on one or more computing devices.

13. An encryption device (106) for encrypting information signals, comprising:

- a component (204) adapted to split, based on multiple analysis subband filters, an input information signal (120) into a set of signal subbands (220);
- a component (206 - 216) adapted to perform an encryption operation on one or more subbands of the set of subbands; and
- a component (218) adapted to synthesize, based on multiple synthesis subband filters, the encrypted set of subbands (222) into an output information signal (122),

wherein a particular synthesis filter is the product of all analysis filters except the analysis filter corresponding in subband to the particular synthesis filter.

14. A decryption device for decrypting information signals, comprising:

- a component (402) adapted to split, based on multiple analysis subband filters, an input information signal (124) into a set of signal subbands (418);
- a component (404 - 414) adapted to perform a decryption operation on one or more subbands of the set of subbands; and
- a component (416) adapted to synthesize, based on multiple synthesis subband filters, the

decrypted set of subbands (420) into an output information signal (126),

wherein a particular synthesis filter is the product of all analysis filters except the analysis filter corresponding in subband to the particular synthesis filter.

15. An encryption and decryption device comprising the encryption device according to claim 13 and the decryption device according to claim 14, adapted in particular as an add-on device for mobile phones.

16. A communication device, in particular a mobile phone or a headset connectable to a mobile phone, comprising at least one of the encryption device according to claim 13 and the decryption device according to claim 14.

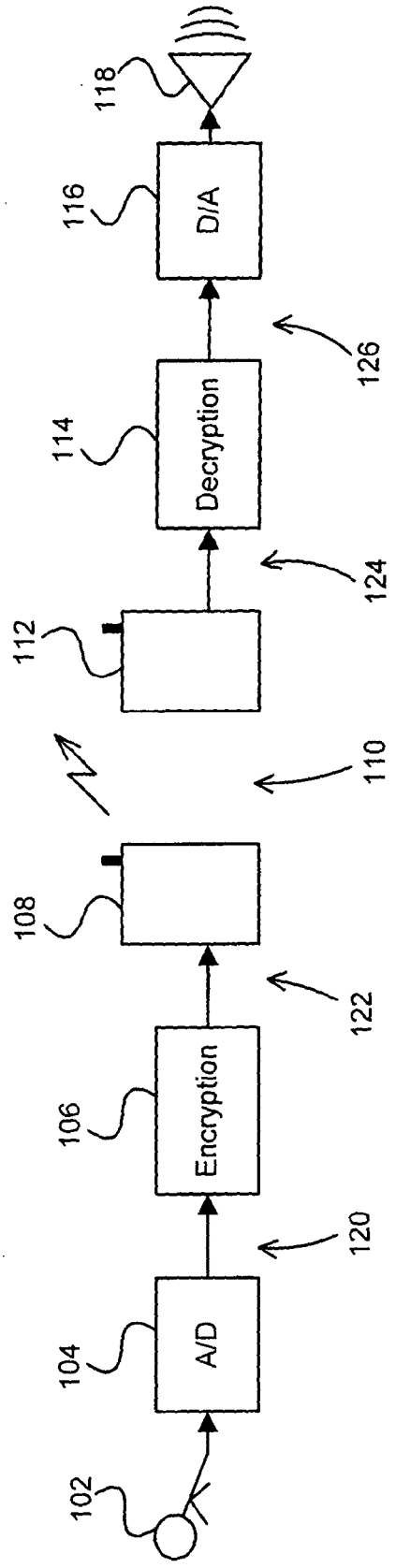

102
A/D
104
120
Encryption
106
122
108
110
112
124
Decryption
114
126
D/A
116
118
100

Fig. 1

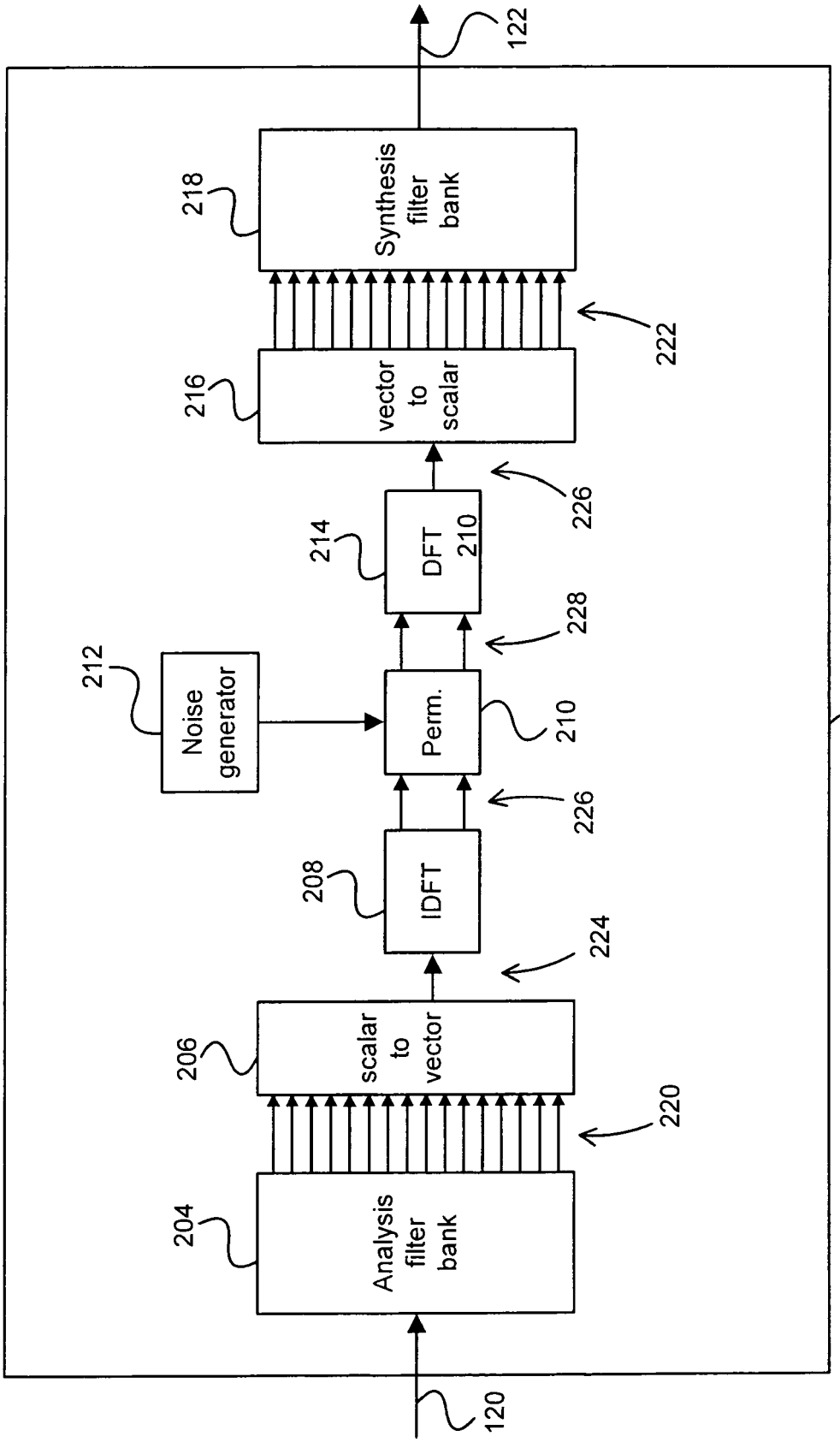

122
218
Synthesis filter bank
222
216
vector to scalar
226
214
DFT 210
228
212
Noise generator
Perm.
210
106
226
208
IDFT
224
206
scalar to vector
220
204
Analysis filter bank
120

Fig. 2

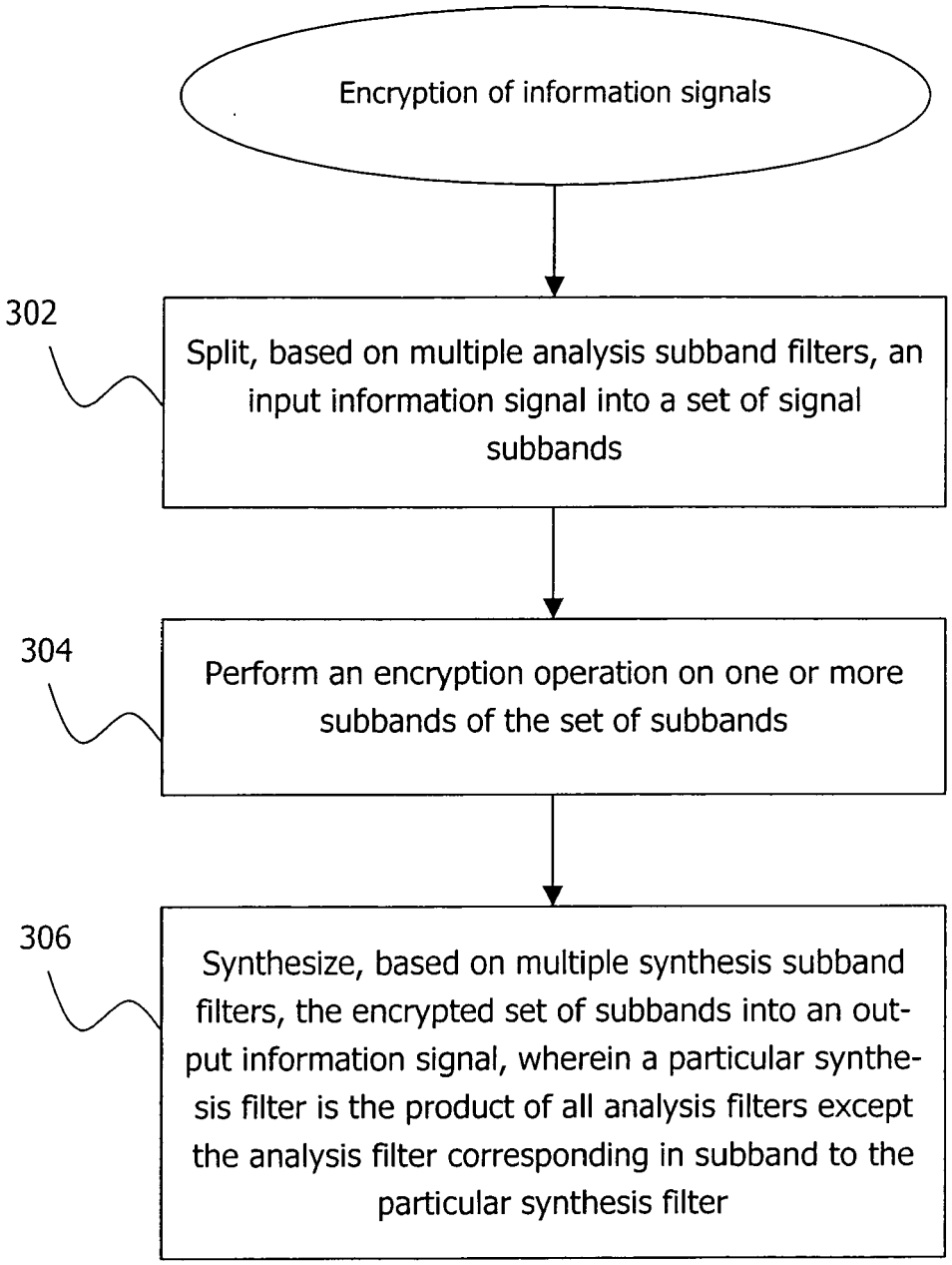

Encryption of information signals
302
Split, based on multiple analysis subband filters, an input information signal into a set of signal subbands
304
Perform an encryption operation on one or more subbands of the set of subbands
306
Synthesize, based on multiple synthesis subband filters, the encrypted set of subbands into an output information signal, wherein a particular synthesis filter is the product of all analysis filters except the analysis filter corresponding in subband to the particular synthesis filter

Fig. 3

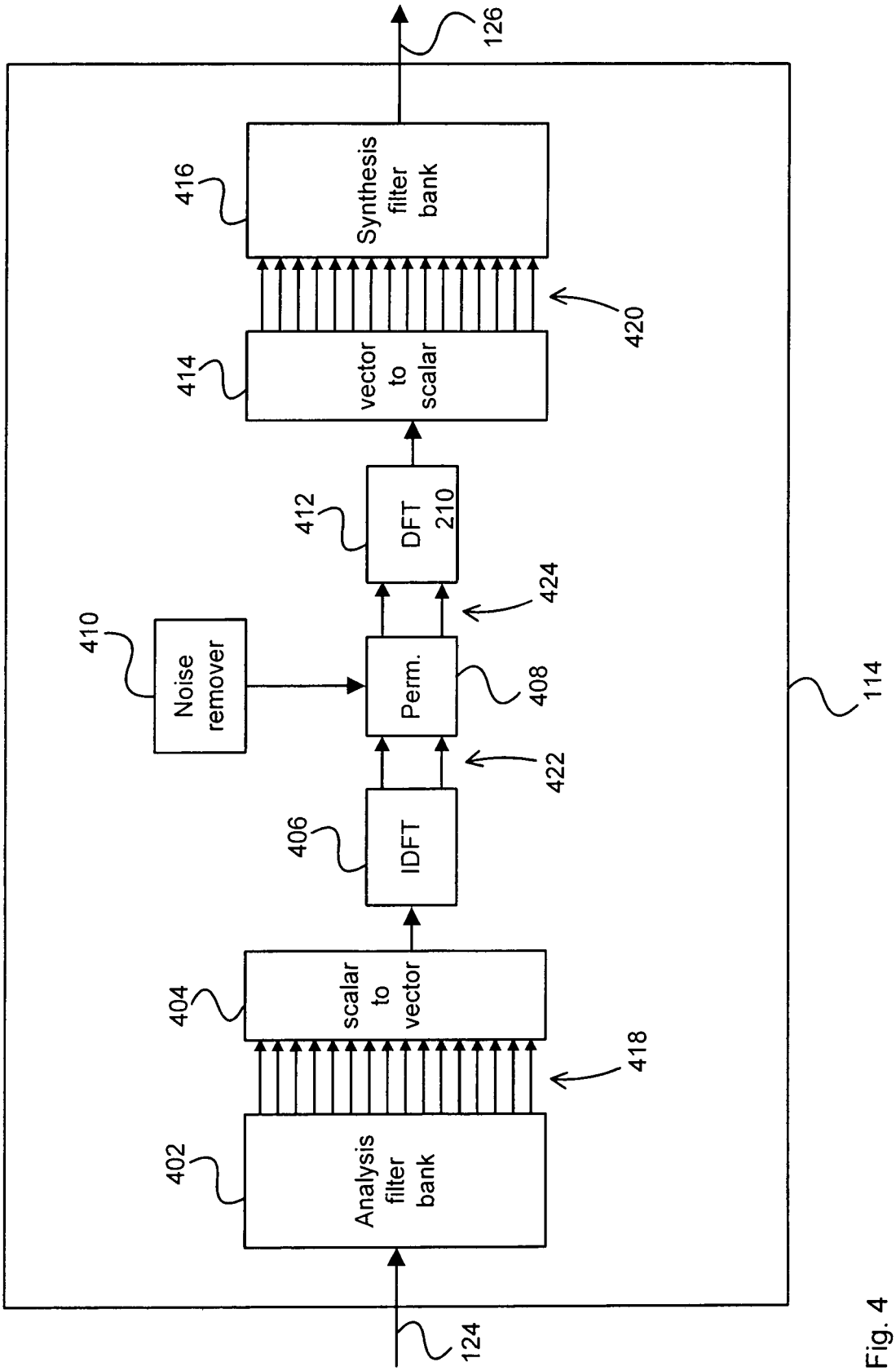

126
416
Synthesis filter bank
420
414
vector to scalar
412
DFT 210
424
410
Noise remover
Perm.
408
422
406
IDFT
404
scalar to vector
418
402
Analysis filter bank
124
114

Fig. 4

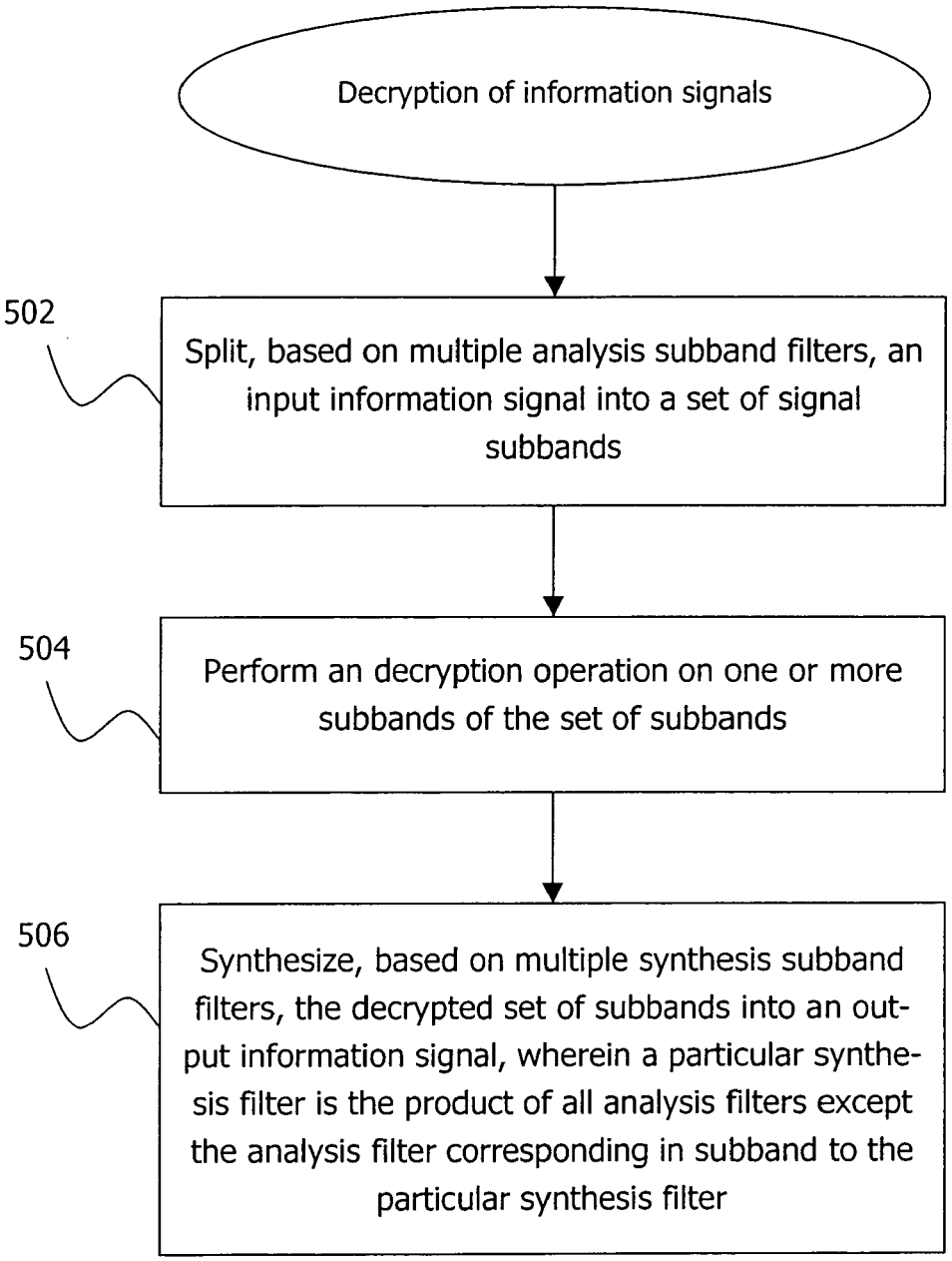

Decryption of information signals
502
Split, based on multiple analysis subband filters, an input information signal into a set of signal subbands
504
Perform an decryption operation on one or more subbands of the set of subbands
506
Synthesize, based on multiple synthesis subband filters, the decrypted set of subbands into an output information signal, wherein a particular synthesis filter is the product of all analysis filters except the analysis filter corresponding in subband to the particular synthesis filter

Fig. 5

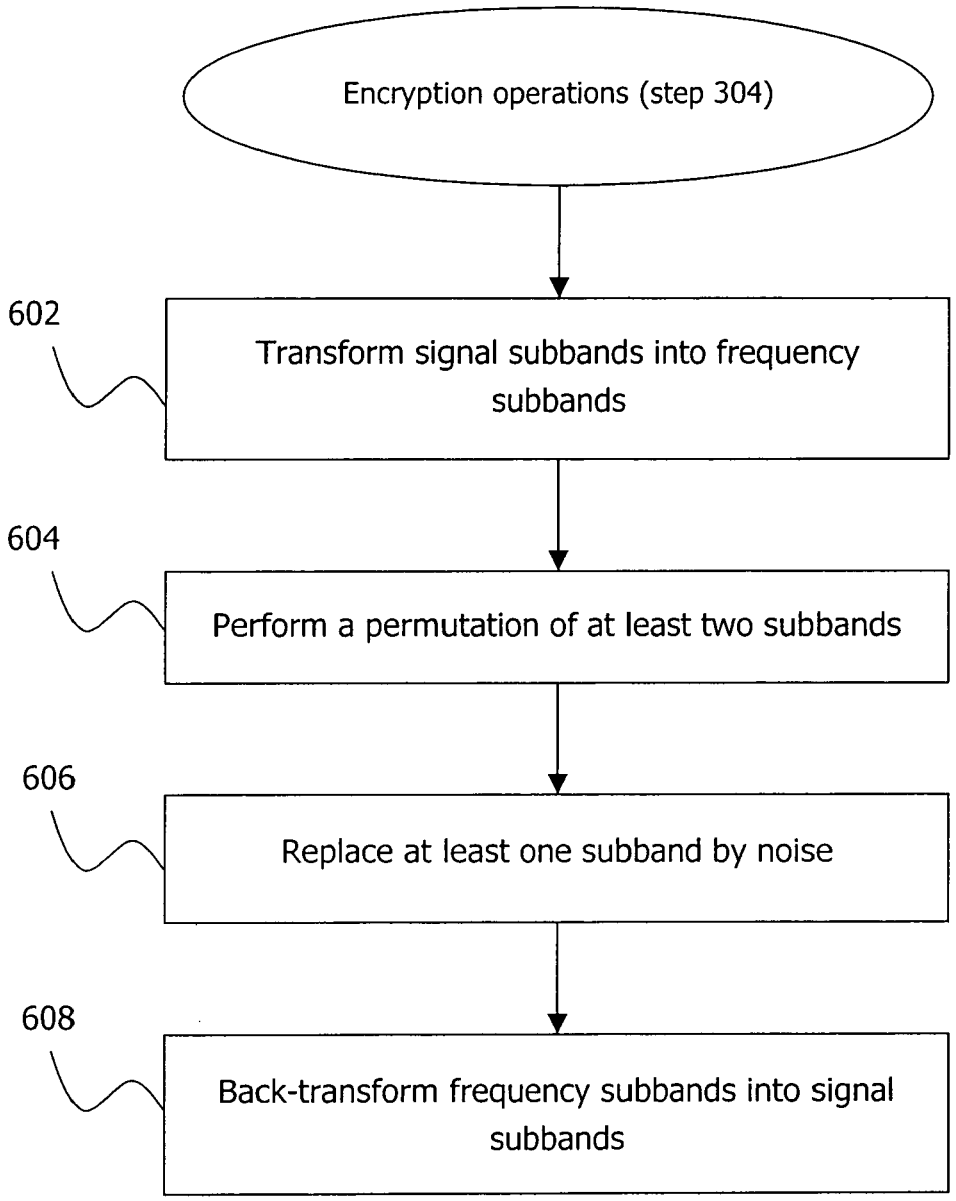

Encryption operations (step 304)
602
Transform signal subbands into frequency subbands
604
Perform a permutation of at least two subbands
606
Replace at least one subband by noise
608
Back-transform frequency subbands into signal subbands

Fig. 6

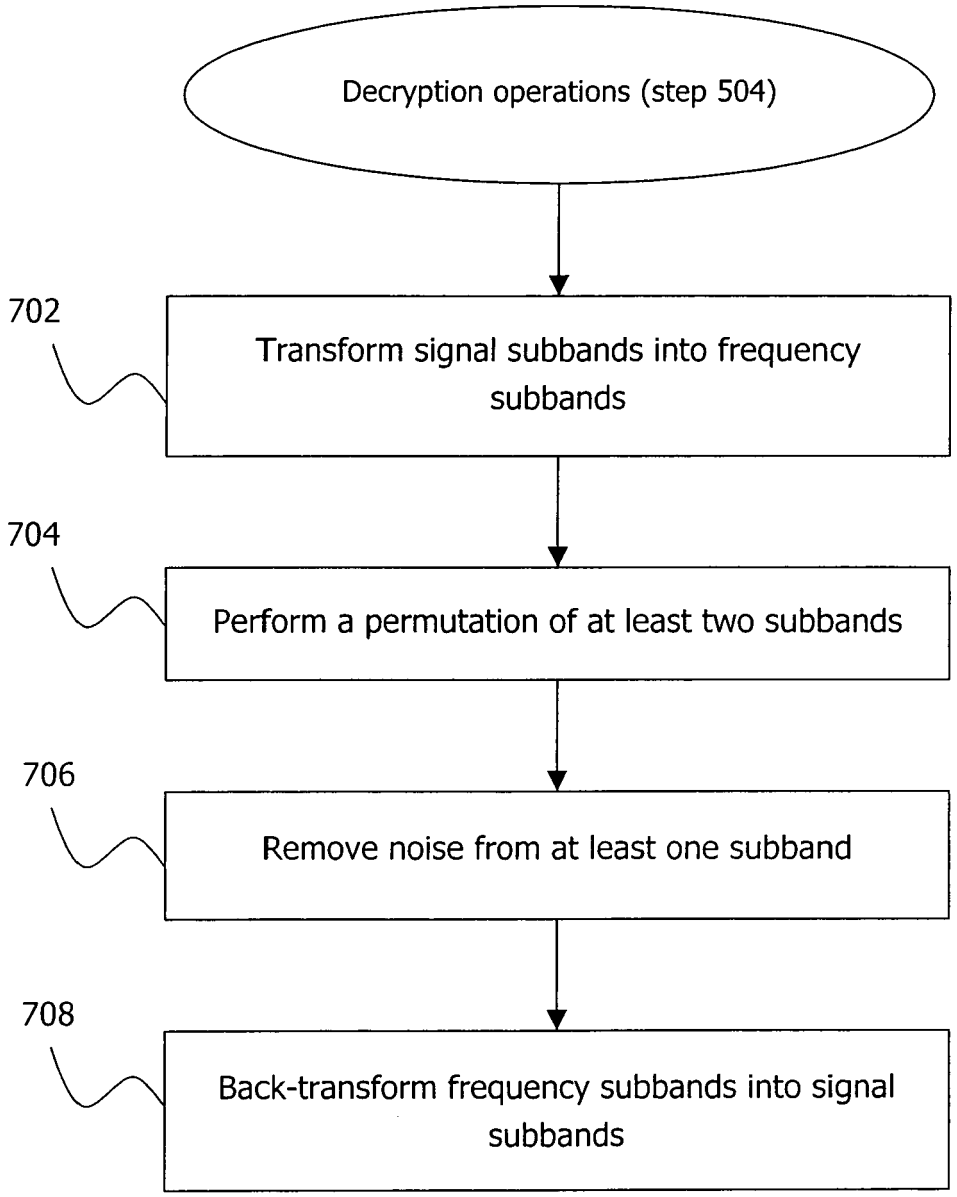

Decryption operations (step 504)
702
Transform signal subbands into frequency subbands
704
Perform a permutation of at least two subbands
706
Remove noise from at least one subband
708
Back-transform frequency subbands into signal subbands

Fig. 7

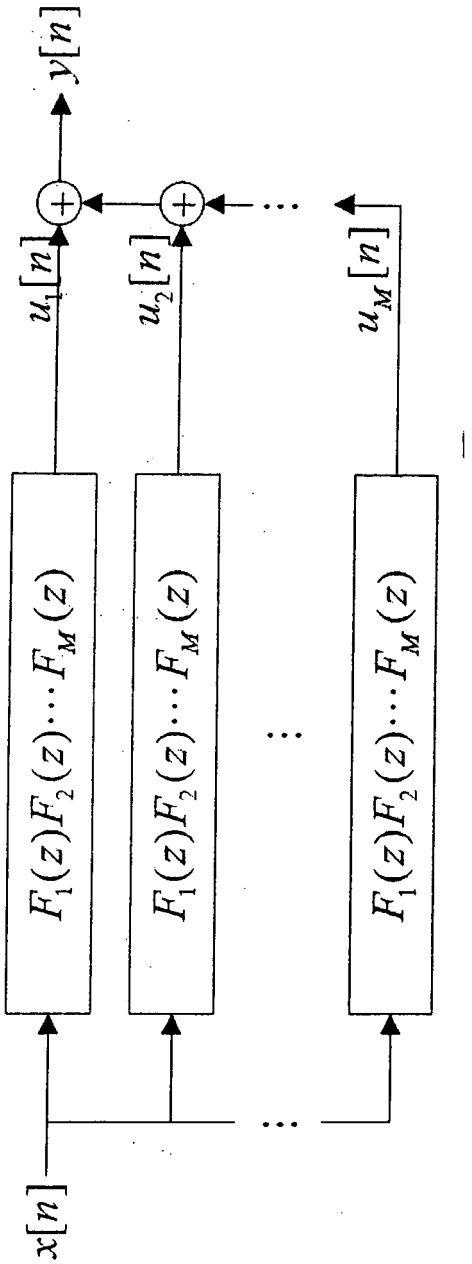

$x[n]$
$F_1(z)F_2(z)\cdots F_M(z)$
$F_1(z)F_2(z)\cdots F_M(z)$
$F_1(z)F_2(z)\cdots F_M(z)$
$u_1[n]$
$u_2[n]$
$u_M[n]$
$y[n]$

Fig. 8a

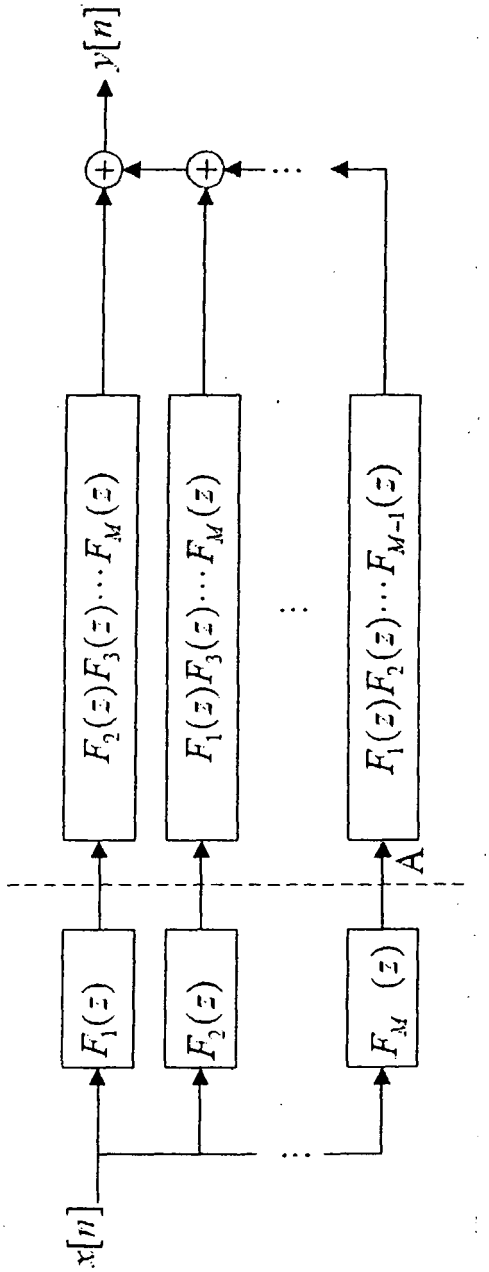
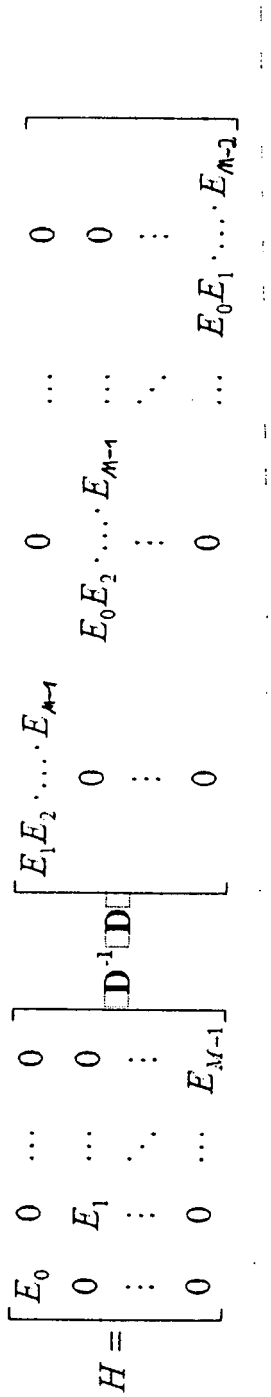

y[n]
$F_2(z)F_3(z)\cdots F_M(z)$
$F_1(z)F_3(z)\cdots F_M(z)$
$F_1(z)F_2(z)\cdots F_{M-1}(z)$
A
$F_1(z)$
$F_2(z)$
$F_M(z)$
x[n]

Fig. 8b



$$H = \begin{bmatrix} E_0 & 0 & \cdots & 0 \\ 0 & E_1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & E_{M-1} \end{bmatrix} \mathbf{D}^{-1} \mathbf{D} \begin{bmatrix} E_1 E_2 \cdots E_{M-1} & 0 & \cdots & 0 \\ 0 & E_0 E_2 \cdots E_{M-1} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & E_0 E_1 \cdots E_{M-2} \end{bmatrix}$$

Fig. 8c

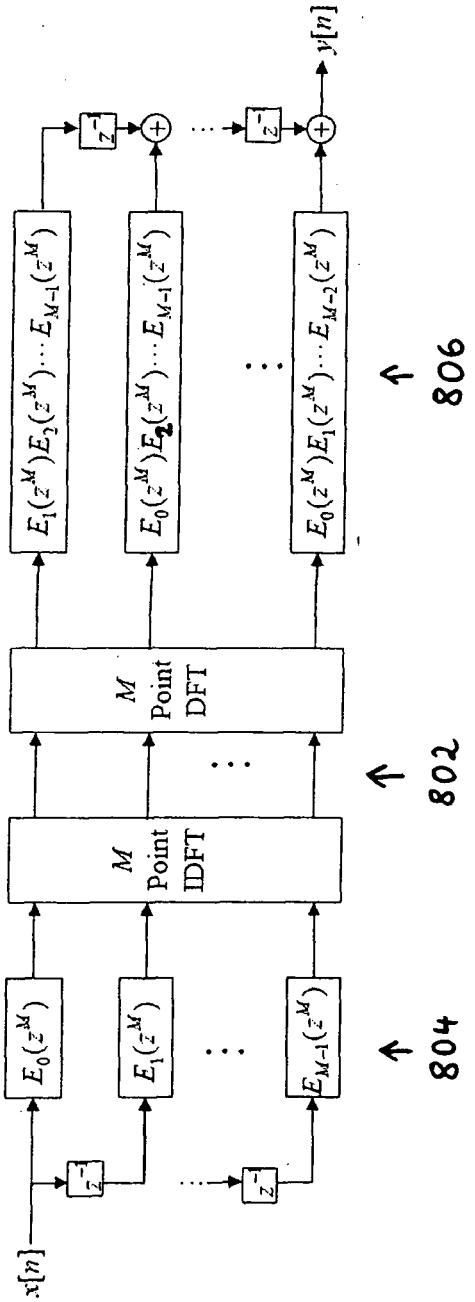


Fig. 8d

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 08 39 0001

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
Y	WADA S ET AL: "SPECTRUM SCRAMBLING BY MEANS OF QMF BANKS FOR SECURE COMMUNICATION" IEICE TRANSACTIONS ON FUNDAMENTALS OF ELECTRONICS,COMMUNICATIONS AND COMPUTER SCIENCES, ENGINEERING SCIENCES SOCIETY, TOKYO, JP, vol. E78-A, no. 8, 1 August 1995 (1995-08-01), pages 1042-1045, XP000536063 ISSN: 0916-8508 * abstract * * page 1042, left-hand column, line 1 - page 1043, left-hand column, line 25 *	1,2,4-9, 12-16	INV. H04K1/04
Y	US 4 829 378 A (LEGALL DIDIER J [US]) 9 May 1989 (1989-05-09) * abstract * * column 2, line 61 - column 5, line 50 * * figures 1A,1B,2 *	1,2,4-7, 9,12-16	
X	GB 1 465 923 A (SIEMENS AG) 2 March 1977 (1977-03-02)	10-12	TECHNICAL FIELDS SEARCHED (IPC)
Y	* page 1, left-hand column, line 9 - page 2, left-hand column, line 32 *	8	H04K H04H H03H
A		5-7	
X	US 4 959 863 A (AZUMA MITSUHIRO [JP] ET AL) 25 September 1990 (1990-09-25)	10-12	
A	* abstract * * column 5, line 65 - column 17, line 66 * * figures 1-27 *	5-8	

-/--

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
The Hague	20 March 2009	Dujardin, Corinne

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

4

Europäisches Patentamt
European Patent Office
Office européen des brevets

EUROPEAN SEARCH REPORT

Application Number
EP 08 39 0001

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
A	SMITH M J T ET AL: "EXACT RECONSTRUCTION TECHNIQUES FOR TREE-STRUCTURED SUBBAND CODERS" IEEE TRANSACTIONS ON ACOUSTICS, SPEECH AND SIGNAL PROCESSING, IEEE INC. NEW YORK, USA, vol. ASSP-34, no. 3, 1 June 1986 (1986-06-01), pages 434-441, XP000828453 ISSN: 0096-3518 * abstract * * page 434, left-hand column, line 1 - page 437, left-hand column, line 14 * * figures 1-3 * -----	1,2,4,5, 12-14	

TECHNICAL FIELDS SEARCHED (IPC)

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
The Hague	20 March 2009	Dujardin, Corinne

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

4

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 08 39 0001

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

20-03-2009

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 4829378 A	09-05-1989	NONE	
GB 1465923 A	02-03-1977	AT 333851 B	10-12-1976
		AU 484739 B2	02-10-1975
		AU 6738374 A	02-10-1975
		BE 813245 A1	03-10-1974
		CH 576215 A5	31-05-1976
		DE 2316647 A1	17-10-1974
		DK 137000 B	27-12-1977
		FR 2224946 A1	31-10-1974
		IE 39093 B1	02-08-1978
		IL 44495 A	31-01-1977
		IT 1011198 B	20-01-1977
		LU 69773 A1	18-07-1974
		NL 7404542 A	07-10-1974
		SE 397035 B	10-10-1977
		ZA 7402085 A	26-03-1975
US 4959863 A	25-09-1990	AU 597177 B2	24-05-1990
		AU 1698688 A	19-01-1989
		CA 1288182 C	27-08-1991
		EP 0293866 A2	07-12-1988
		JP 1302931 A	06-12-1989
		JP 2653830 B2	17-09-1997
		KR 910004405 B1	27-06-1991

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82