(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 March 2011 (10.03.2011)

PCT

(10) International Publication Number
WO 2011/028175 A1

(51) International Patent Classification:
*G06F 19/00* (2011.01) *H04L 9/36* (2006.01)
*H04L 9/18* (2006.01)

(21) International Application Number:
PCT/SG2009/000307

(22) International Filing Date:
1 September 2009 (01.09.2009)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **AGENCY FOR SCIENCE, TECHNOLOGY AND RESEARCH** [SG/SG]; 1 Fusionopolis Way # 20-10, Connexis, Singapore 138632 (SG).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **LYE, Kin Mun** [SG/SG]; c/o IPTO, Institute for Infocomm Research, 1 Fusionopolis Way #21-01, Connexis South Tower, Singapore 138632 (SG). **RAHARDJA, Susanto** [ID/SG]; c/o IPTO, Institute for Infocomm Research, 1 Fusionopolis Way #21-01, Connexis South Tower, Singapore 138632 (SG). **LI, Te** [CN/SG]; c/o IPTO, Institute for Infocomm Research, 1 Fusionopolis Way #21-01, Connexis South Tower, Singapore 138632 (SG). **HUANG, Haibin** [CN/SG]; c/o IPTO, Institute for Infocomm Research, 1 Fusionopolis Way #21-01, Connexis South Tower, Singapore 138632 (SG).

(74) Agent: **SCHIWECK, Wolfram**; Viering, Jentschura & Partner LLP, P.O. Box 1088, Rochor Post Office, Rochor Road, Singapore 911833 (SG).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

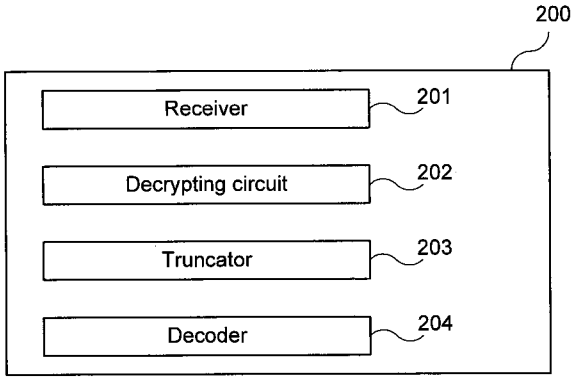
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

**Published**:

— *with international search report (Art. 21(3))*

(54) Title: TERMINAL DEVICE AND METHOD FOR PROCESSING AN ENCRYPTED BIT STREAM

FIG 2




(57) Abstract: A terminal device is described comprising a receiver configured to receive an encrypted bit stream which is decodable to a digital signal, a decrypting circuit configured to decrypt the encrypted bit stream, a truncator configured to receive a quality indication and configured to truncate the decrypted bit stream in accordance with the quality indication such that the truncated decrypted bit stream is decodable to a digital signal having a quality corresponding to the indicated by the quality indication, and a decoder configured to decode the truncated bit stream.

WO 2011/028175 A1

# TERMINAL DEVICE AND METHOD FOR PROCESSING AN ENCRYPTED BIT STREAM

Embodiments of the invention generally relate to a terminal device and a method for processing an encrypted bit stream.

Online music stores have shown the viability of online music sales. An existing limitation of online music sales is that the music files are only offered at fixed bitrates in lossy compressed form. However, with the proliferation of broadband access and continuous decline of memory storage prices, there is an increasing number of music lovers who wish to purchase their favorite music online at a high resolution which is as good as CD quality. On the other hand, some users may prefer to purchase songs that are cheaper but are encoded at a lower bit rate. This is because the perceptual audibility between, for example, an audio file encoded at 96kbps and an audio file encoded at 128kpbs is transparent or not important to such users, for example in case that the music is played on a mobile device.

In order to satisfy the various bit rate and quality requirements of their customers, music stores may archive different versions of the same piece of music at different bitrates on their file servers. This is a burden for the file servers since it increases the complexity of the data management and the amount of necessary storage space.

Alternatively, a music store may prefer to encode songs at a required bit rate only when a purchase order is received for the required bit rate. This, however, is both time consuming and computationally intensive.

Fine granular scalable audio coding, which has been extensively studied recently, provides the opportunity to address variable quality requirements. Released by the ISO in late 2006, MPEG-4 audio scalable lossless coding (SLS, cf. e.g. [1] and [2]) integrates the functions of lossless audio coding, perceptual audio coding and fine granular scalable audio coding in a single framework. It allows the scaling up of a perceptually coded representation such as a MPEG-4 AAC coded piece of audio to a lossless representation of the piece of audio with fine granular scalability.

Embodiments may be seen to be based on the problem to provide a user terminal with a digital signal having a pre-defined quality, e.g. a quality corresponding to a quality level for which the user has paid.

In one embodiment, a terminal device is provided including a receiver configured to receive an encrypted bit stream which is decodable to a digital signal, a decrypting circuit configured to decrypt the encrypted bit stream, a truncator configured to receive a quality indication and configured to truncate the decrypted bit stream in accordance with the quality indication such that the truncated decrypted bit stream is decodable to a digital signal having a quality corresponding to the indicated by the quality indication, and a decoder configured to decode the truncated bit stream.

According to other embodiments, a method for processing an encrypted bit stream and an computer readable medium in accordance with the terminal device described above are provided.

Illustrative embodiments of the invention are explained below with reference to the drawings.

FIG. 1 shows a communication system according to an embodiment.

FIG. 2 shows a terminal device according to an embodiment.

FIG. 3 shows a communication arrangement according to an embodiment.

FIG. 4 shows an encoder according to an embodiment.

FIG. 5 shows a decoder according to an embodiment.

FIG. 6 shows a bit plane diagram.

FIG. 7 shows an SLS enhancer.

FIG. 8 shows an illustration of file formats in accordance with an embodiment.

FIG. 9 illustrates an encryption process in accordance with an embodiment.

FIG. 10 illustrates a decryption process in accordance with an embodiment.

FIG. 11 shows a truncator according to an embodiment.

FIG. 12 shows a truncator according to an embodiment.

It should be noted that embodiments described in the following that are described in the context with the terminal device are analogously valid for the method for processing an encrypted bit stream and the computer readable medium.

FIG. 1 shows a communication system 100 according to an embodiment.

The communication system 100 includes a server (e.g. a server computer) 101 and a plurality of terminals 102. The terminals 102 are for example client units and may be (terminal) communication devices such as (radio) communication devices, e.g. mobile phones, or (personal) computers.

The server 101 may send a bit stream 103, for example an SLS (scalable-to-lossless coding) bit stream 103 to the terminals 102, for example by means of a communication network, indicated by arrow 104) such as the Internet or a radio communication network such as a cellular mobile radio communication network using broadcast or multicast. The bit stream 103 is for example decodable to a digital signal, e.g. an audio signal, of high quality. The bit stream 103 may thus be seen as a high or full quality bit stream including a high or full quality version of the digital signal.

The terminals 102 may generate from the bit stream 103 a digital signal of low quality 105, a digital signal of medium quality 106, or a digital signal of high quality 107, respectively. It should be noted that in other embodiments, more or less than three quality levels are used. For example it is possible to have two, five or any levels of quality. Similarly, in any of the examples described in the following where a plurality of quality levels is used, this plurality

of quality levels may include any number of quality levels, e.g. two, three, five or higher numbers of quality levels.

In other words, the terminals 102 may generate a low quality version of the digital signal, a medium quality version of the digital signal and a high quality version of the digital signal included in the bit stream 103. For example, the quality of the digital signal 105, 106, 107 that is generated from the bit stream 103 depends on the amount of money that the user of the respective terminal 102 has paid. For example, if a user of a terminal 102 has paid a low amount of money the digital signal with low quality 105 is generated from the bit stream 103. If a user of a terminal 102 has paid a medium amount of money the digital signal with medium quality 106 is generated from the bit stream 103 and if a user of a terminal 102 has paid a high amount of money the digital signal with high quality 107 is generated from the bit stream 103.

The bit stream 103 may for example be encrypted by the server 101 before broadcasting or multicasting.

A terminal 102 according to one embodiment is described in the following with reference to figure 2.

FIG. 2 shows a terminal device 200 according to an embodiment.

The terminal device 200 includes a receiver 201 configured to receive an encrypted bit stream which is decodable to a digital signal.

The terminal device 200 further includes a decrypting circuit 202 configured to decrypt the encrypted bit stream.

Additionally, the terminal device 200 includes a truncator 203 configured to receive a quality indication and configured to truncate the decrypted bit stream in accordance with the quality indication such that the truncated decrypted bit stream is decodable to a digital signal having a quality corresponding to the quality indicated by the quality indication.

Furthermore, the terminal device 200 includes a decoder 204 configured to decode the truncated bit stream.

In other words, illustratively, a bit stream is received which is decodable to a digital signal and the bit stream is truncated such that it is decodable to a version of the digital signal having an indicated quality. For example, the received bit stream would be decodable to a high (or full) quality but the user of the terminal device only has the right to receive medium quality and the received bit stream is therefore truncated to be only decodable to medium quality. The bit stream is for example received from a server device that transmits the bit stream corresponding to a fixed quality (e.g. a fixed bit rate). Embodiments may be seen to be based on the flexibility of the setting of the quality (e.g. bit rate) is moved from the server to the client or terminal.

The components such as the truncator 203 and the decoder 204 may be implemented using circuits. In an embodiment, a "circuit" may be understood as any kind of a logic implementing entity, which may be special purpose circuitry

or a processor executing software stored in a memory, firmware, or any combination thereof. Thus, in an embodiment, a "circuit" may be a hard-wired logic circuit or a programmable logic circuit such as a programmable processor, e.g. a microprocessor (e.g. a Complex Instruction Set Computer (CISC) processor or a Reduced Instruction Set Computer (RISC) processor). A "circuit" may also be a processor executing software, e.g. any kind of computer program, e.g. a computer program using a virtual machine code such as e.g. Java. Any other kind of implementation of the respective functions which will be described in more detail below may also be understood as a "circuit" in accordance with an alternative embodiment.

In one embodiment, the terminal device is a client device and the receiver is configured to receive the encrypted bit stream from a server device.

The digital signal is for example an audio signal or a video signal.

The quality indication may for example include the indication of a bit rate and the truncator is for example configured to truncate the decrypted bit stream such that the truncated decrypted bit stream is decodable to a digital signal having the indicated bit rate.

In one embodiment, the bit stream is an SLS bit stream.

For example, the bit stream includes the digital signal encoded in accordance with a scalable coding scheme.

In one embodiment, the bit stream includes the digital signal encoded in accordance with SLS. For example, the decoder is an SLS decoder.

In one embodiment, the terminal device is an electronic communication device. The terminal device is for example a mobile communication device such as a mobile phone.

In one embodiment, the truncator is configured to truncate the decrypted bit stream in accordance with the quality indication such that the truncated decrypted bit stream is not decodable to a version of the digital signal having a higher quality than the quality indicated by the quality indication.

In one embodiment, the encrypted bit stream is decodable to a digital signal of a plurality of digital signals wherein the digital signals are associated with different quality levels and wherein the truncator is configured to truncate the decrypted bit stream in accordance with the quality level indication such that the truncated decrypted bit stream is decodable to the digital signal of the plurality of digital signals that is associated with the quality level indicated by the quality level indication but is not decodable to a digital signal associated with a higher quality level than the quality level indicated by the quality level indication.

The quality indication is for example a key (e.g. in a form of a sequence of bits) corresponding to a quality level.

The truncator may be configured to determine the quality level from the user key and to truncate the decrypted bit stream in accordance with the quality level.

In one embodiment, the receiver is configured to receive the encrypted bit stream via streaming.

In one embodiment, the receiver is configured to receive the encrypted bit stream via broadcast or multicast.

In the following, a communication arrangement is described that may for example include a terminal device as described above with reference to figure 2.

FIG. 3 shows a communication arrangement 300 according to an embodiment.

The communication arrangement 300 includes a server communication device 301 and a terminal device 302, e.g. a client device. The server communication device 301 may be seen as the encoding side and the terminal device 302 may be seen as the decoding side.

The server communication device 301 includes a bit stream generating circuit 303 which may for example be an SLS encoder or an SLS enhancer as explained below. The bit stream generating circuit 303 for example outputs a bit stream which is decodable to a digital signal such as a video signal or an audio signal.

The server communication device 301 further includes an encrypting circuit 304 which for example receives a cipher bit stream for encrypting the bit stream output by the bit stream generating circuit 303. The cipher bit stream may for example be seen as or may be based on a shared key of the server communication device 301 and the terminal device 302,

i.e. a key both known to the server communication device 301 and the terminal device 302. The encrypting circuit 304 generates an encrypted bit stream 304 which is supplied to an error protection circuit 305 of the server communication device 301. The error protection circuit 305 processes the encrypted bit stream 305 to allow error correction and detection at the receiver side, i.e. by the terminal device 302. For example, the error protection circuit 304 includes additional bits for error correction into the encrypted bit stream, such as bits in accordance with CRC (cyclic redundancy check).

The encrypted bit stream that has been processed by the error protection circuit 305 is then transmitted by the server communication device 301 to the terminal device 302 by means of a communication channel 306, e.g. by means of broadcasting it, e.g. using a radio communication network, or by streaming it via the Internet.

The terminal device 302 includes an error detection and correction circuit 307 which applies error detection and, possibly, error correction on the encrypted bit stream as received by the terminal device 302. The encrypted bit stream is then supplied to a decryption circuit 308 of the terminal device 302 which decrypts the encrypted bit stream, e.g. in accordance with the cipher bit stream that has been used by the encrypting circuit 304 for encrypting the bit stream. The decryption circuit 308 outputs a (received) bit stream which corresponds to the bit stream generating circuit 303 except for, for example, differences which may arise, for example, due to the transmission errors that could not be corrected by the error detection and correction circuit 307.

The terminal device 302 further includes a truncator (e.g. a truncating circuit) that truncates the bit stream such that the truncated bit stream is decodable to digital signal having a quality indicated by a quality indication 310. The quality for example corresponds to an amount of money the user of the terminal device 302 has paid for the digital signal (e.g. a piece of music or a video clip). For example, the quality corresponds to a type of subscription of the user of the terminal device 302.

The truncator 309 supplies the truncated bit stream to a decoding circuit 311, e.g. an SLS decoder, of the terminal device 302 which generates the digital signal having the quality indicated by the quality indication 310. For example, the decoding circuit 311 generates and outputs an audio signal that is a lower quality version (as specified by the quality indication 310) of an original audio signal (e.g. a PCM (pulse code modulation) audio signal) supplied to the bit stream generating circuit 303. The original audio signal can for example be seen as a full quality audio signal. The bit stream that is supplied to the truncator 309 is in this case in one embodiment decodable to the full quality audio signal (except for, e.g., transmission errors that could not be corrected by the error detection and correction circuit 307, i.e. the bit stream supplied to the truncator may be seen as a full quality bit stream which is truncated by the truncator to a bit stream of lower quality, i.e. to a bit stream that is only decodable to a digital signal of lower quality than the original digital signal. In other words, this can be seen as the truncator removing parts of the decrypted bit stream that would be need for a certain quality. For example, the truncator removes SLS enhancement layers included in the decrypted bit stream such that the decrypted bit stream can

only be decoded to a version of the digital signal with a certain maximum quality.

The server communication device is for example a streaming server or a broadcasting station.

The bit stream generating circuit 303 is for example an encoder as explained in the following with reference to figure 4.

FIG. 4 shows an encoder 400 according to an embodiment.

The encoder 400 receives an audio signal 401 as input, which is for example an original uncompressed audio signal which should be encoded to an encoded bit stream 402.

The audio signal 401 is for example in integer PCM (Pulse Code Modulation) format and is losslessly transformed into the frequency domain by a domain transforming circuit 406 which for example carries out an integer modified discrete Cosine transform (IntMDCT).

The resulting frequency coefficients (e.g. IntMDCT coefficients) are passed to a lossy encoding circuit 403 (e.g. an AAC encoder) which generates the core layer bit stream, e.g. an AAC bit stream, in other words a core audio signal portion. The lossy encoding circuit 403 for example groups the frequency coefficients grouped into scale factor bands (sfbs) and quantizes them for example with a non-uniform quantizer. In order to efficiently utilize the information of the spectral data that has been coded in the core layer bit stream, an error-mapping procedure is employed by an error mapping circuit 404 which receives the frequency

coefficients and the core layer bit stream as input to generate an residual spectrum (e.g. a lossless enhancement layer, LLE), in other words a residual audio signal portion, by subtracting the quantized frequency coefficients generated by the lossy encoder (e.g. the AAC quantized spectral data) from the original frequency coefficients. The encoder 400 may thus be seen to include a core layer and a (lossless) enhancement layer.

The residual spectrum is then encoded by a bit stream encoding circuit 405, for example according to the bit plane Golomb code (BPGC), context-based arithmetic code (CBAC) and low energy mode coding (LEMC) to generate a scalable enhancement layer bit stream (e.g. a scalable LLE layer bit stream).

Finally, the scalable enhancement layer bit stream is multiplexed by a multiplexer 407 with the core layer bit stream to produce the encoded bit stream 402, e.g. the SLS bit stream.

The decoding circuit 311 of the terminal device for example corresponds to the encoder 400 as explained in the following with reference to figure 5.

FIG. 5 shows a decoder 500 according to an embodiment.

The decoder 500 receives an encoded bit stream 501 as input. A bit stream parsing circuit 502 extracts the core layer bit stream 503 and the enhancement layer bit stream 504 from the encoded bit stream. The enhancement layer bit stream 504 is decoded by a bit stream decoding circuit 505 corresponding to the bit stream encoding circuit 405 to reconstruct the

residual spectrum as exact as it is possible from the transmitted encoded bit stream 501.

The core layer bit stream 503 is decoded by a lossy decoding circuit 506 (e.g. an AAC decoder) and is combined with the reconstructed residual spectrum by an inverse error mapping circuit 507 to generate the reconstructed frequency coefficients.

The reconstructed frequency coefficients are transformed into the time domain by a domain transforming circuit 508 corresponding to the domain transforming circuit 406 (e.g. an integer inverse MDCT) to generate a reconstructed audio signal 509.

By selecting how much of the residual spectrum generated by the error mapping circuit 404 is supplied to the decoder 500, the reconstructed audio signal 509 is scalable from lossy to lossless. For example, the quality of the audio signal 509 depends on the amount of the residual spectrum that is left from the full residual spectrum after the truncation by the truncator 309.

In SLS (MPEG-4 scalable lossless) coding, the bit stream encoding circuit 405 carries out a bit plane scanning scheme for encoding the residual spectrum. SLS, using this bit plane scanning scheme, allows the scaling up of a perceptually coded representation such as MPEG-4 AAC to a lossless representation with a wide range of intermediate bit rate representations.

The bit plane scanning scheme in SLS that is used according to one embodiment is illustrated in figure 6.

FIG. 6 shows a bit plane diagram 600.

In the bit plane diagram 600, the residual spectrum values are represented as bit words (i.e. words of bits), wherein each bit word is written as a column and the bits of each bit word are ordered according to their significance from most significant bit to least significant bit.

The significance of the bits in their respective bit word increases along a first axis 601 (y-axis). Each residual spectrum value for example corresponds to a frequency and belongs to a scale factor band. The scale factor band (sfb) number increases from left to right (from 0 to s-1) along a second axis 602 (x-axis).

The scanning process carried out by the bit stream encoding circuit 405 starts from the most significant bit of spectral data (i.e. of the residual spectrum values) for all scale factor bands. It then progresses to the following bit planes until it reaches the least significant bit (LSB) for all scale factor bands. Starting from the fifth bit plane or in this example the seventh bit plane (for CBAC), the bit plane scanning process enters the Lazy-mode coding for the lazy bit planes where the probability of a bit to be 0 or 1 is assumed to be equal.

As the frequency assignment rule of BPGC is derived from the Laplacian probability density function, BPGC only delivers excellent compression performance when the sources are near-Laplacian distributed. However, for some music items, there exist some "silence" time/frequency regions where the spectral data are in fact dominated by the rounding errors of

IntMDCT. In order to improve the coding efficiency, low energy mode coding may be adopted for coding signals from low energy regions.

It is possible to improve the coding efficiency of BPGC by further incorporating more sophisticated probability assignment rules that take into account the dependencies of the distribution of IntMDCT spectral data to several contexts such as their frequency locations or the amplitudes of adjacent spectral lines, which can be effectively captured by using CBAC. For CBAC coding, the seventh and below bit planes are set as absolute lazy bit planes in SLS reference codec.

In one embodiment, the bit stream generating circuit 303 is an SLS enhancer as described in the following with reference to figure 7.

FIG. 7 shows an SLS enhancer 700.

The SLS enhancer 700 can operate in two modes. In the core mode, there are two inputs including the original audio signal, which is in this embodiment an original uncompressed PCM audio file 701 and a compressed version of the original audio signal, in this embodiment in the form of a perceptually compressed file 702 e.g. in accordance with AAC (Advanced Audio Coding), scalable AAC, or BSAC (Bit Sliced Arithmetic Coding). The compressed version of the original audio signal is for example a low quality version of the original audio signal.

The perceptually compressed file 702 is in this embodiment Huffman decoded by a Huffman decoder 703 of the SLS enhancer 700, and the quantized frequency coefficients corresponding

to the compressed audio signal are extracted from the bit stream corresponding to the Huffman decoded perceptually compressed file 702 by a de-quantization and data extraction circuit 704.

The uncompressed PCM audio file 701 is losslessly transformed into the frequency domain by an integer modified discrete Cosine transform (IntMDCT) circuit 705.

The resulting IntMDCT coefficients are passed to an error mapping circuit 706 which also receives the quantized frequency coefficients to generate a residual spectrum, in other words a residual audio signal portion, by subtracting the quantized frequency coefficients generated from the original frequency coefficients.

The residual spectrum is then encoded by a low energy mode encoding circuit 707 and a BPGC/CBAC encoding circuit 708 according to the bit plane Golomb code (BPGC) and the context-based arithmetic code (CBAC) and by a low energy mode encoding circuit 707 according to low energy mode coding (LEMC), e.g. for coding coefficients from low energy regions of the spectrum.

The outputs of the BPGC/CBAC encoding circuit 708 and the low energy mode encoding circuit 707 are multiplexed by a multiplexer 710 with the core layer bit stream to produce an SLS bit stream 709.

In the second mode, which is so called non-core mode, the Huffman decoder 703 and the de-quantization and data extraction circuit 704 are not used and the uncompressed PCM audio file 701 is the only input. In this case, the SLS

enhancer 700 operates as an SLS encoder as explained above with reference to figure 4. The output of the SLS enhancer 700 is, in both cases, a bit stream corresponding to a lossless SLS format as illustrated in figure 8

FIG. 8 shows an illustration of data formats in accordance with an embodiment.

Data in a first format 801 may be seen as the perceptually compressed file which includes an audio signal, for example, in a format in accordance with AAC.

Data in a second format 802 is the uncompressed PCM audio (file) which includes the original audio signal.

Data in a third format 803 includes the audio signal in SLS lossless format according to core mode and a data in a fourth format 804 includes the audio signal in SLS lossless format according to non-core mode. A difference between the third format 803 and the fourth format 804 may be seen in that in the fourth format 804, the data is fine granularly scalable over the whole range while the third format 803 includes the audio signal in a basic quality that is not scalable.

The drawing of the data size in figure 8 is not exact to scale but should only illustrate the relation of the data amounts corresponding to the formats 801, 802, 803, 804.

The perceptually compressed format in accordance with AAC for examples corresponds to a bit rate of the audio signal of 64kbps.

As explained above, the output of the bit stream generating circuit 303 is supplied to the encrypting circuit 304 for encryption. In one embodiment, this output is a bit stream corresponding to the data in the third format 803 or the data in the fourth format 804.

This bit stream is sent to the encrypting circuit 304 for encrypting using the cipher bit stream. The encryption may for example be any symmetric key encryption where plaintext bits are combined with a pseudorandom cipher bit stream (key stream), e.g. by an exclusive OR (XOR) operation. A possible implementation of the encryption is illustrated in figure 9.

FIG. 9 illustrates an encryption process in accordance with an embodiment.

According to the encryption process a bit stream 901, e.g. an SLS bit stream, is encrypted using a cipher bit stream 902 to generate an encrypted bit stream 903. For this, each bit of the bit stream 901 is combined in accordance with an XOR operation with a corresponding bit of the cipher bit stream 902 to generate a corresponding bit of the encrypted bit stream 903. The encryption may thus be seen as a bit-wise combination of the bit stream to be encrypted 901 with the cipher bit stream 902. The XOR operation is for example carried out by an XOR circuit of the encrypting circuit 304.

In one embodiment, for better efficiency, in which the bit stream contains as a part the basic AAC format the audio signal compressed in accordance with the perceptually compressed format in accordance with AAC, only the SLS part is encrypted, i.e. the basic AAC format is not encrypted. In one embodiment in which the bit stream generating circuit 303

is an SLS enhancer in non-core mode, only the enhancement bit stream above a pre-defined bit rate is encrypted. For example, the pre-defined bit rate can be set at 64kbps or 96kbps. This is illustrated in figure 8 where only first parts 805 of the data in the third format 803 and the data in the fourth format 804 are illustrated to be encrypted while second parts 806, which may be seen as containing the audio signal in a basic quality, are not encrypted in one embodiment.

The error protection circuit 305 for example adds error protection code to the encrypted bit stream. For broadcasting, any type of forward error correction (FEC), such as turbo coding can be applied. For streaming, both the FEC and automatic repeat-request (ARQ) can be applied.

As mentioned above, the error protected encrypted SLS lossless bit stream, e.g. the error protected encrypted SLS lossless bit stream, is transmitted via the communication channel 306 through wireless or Internet transmission or broadcasting.

In the terminal device 302, the received signal, i.e. the bit stream received from the communication device 301 is firstly checked, in one embodiment, with an error detection and correction scheme that corresponds to the encoder error protection scheme.

The (possibly) corrected bit stream is then decrypted using a decryption method corresponding to the encryption method used by the encrypting circuit 304. For example, the decryption circuit 308 decrypts the received encrypted bit stream using the cipher bit stream, which is in this example a shared key,

that has been used in the encryption process illustrated in figure 9. The decryption process in this case is illustrated in figure 10.

FIG. 10 illustrates a decryption process in accordance with an embodiment.

According to the decryption process, the received encrypted bit stream 1001 is decrypted using the cipher bit stream 1002 to generate the decrypted (received) bit stream 1003. For this, each bit of the encrypted bit stream 1001 is combined in accordance with an XOR operation with a corresponding bit of the cipher bit stream 1002 to generate a corresponding bit of the decrypted bit stream 1003. The decryption may thus be seen as a bit-wise combination of the bit stream to be decrypted 1001 with the cipher bit stream 1002.The XOR operation is for example carried out by an XOR circuit of the decrypting circuit 308.

The decrypted bit stream, e.g. the decrypted SLS lossless bit stream, is then passed to the (SLS) truncator 309. Another input of the truncator 309 is quality information, in one embodiment in the form of a quality indication 310. This quality information is for example extracted from payment information. For example, there are three subscription choices including the basic (64kbps, $20/month), intermediate (192kbps, $50/month) and premium (lossless, $70/month) subscription. If the user of the terminal device 302 chooses intermediate quality and pays $50/month then the quality information input to the truncator is for example the indication of the corresponding bit rate which is, for example, 192kbps.

The truncator 309 truncates the decrypted received bit stream, which may be seen to contain the original audio signal in lossless format, to, for example, the target bit rate as indicated by the quality indication 310.

In one embodiment, this is for example done in accordance with the following. Let the total target bit rate after truncation be $B^T$ (in kbps) and the perceptually coded bit rate (i.e. the bit rate corresponding to the second parts 806, be $B^C$ (in kbps). The new total LLE bit stream length $L^T$ (in byte) for each frame may be determined by

$$L^T = F \cdot \frac{(B^T - B^C)}{8 \cdot S} \cdot 1000 \,(1) \qquad (1)$$

where F is the frame size and S is the sampling rate.

Let the lossless bit stream length for each frame be $L^L$. It is assumed that there are a total of N channels and for each channel n, n = 0,1,…,N-1, the bit stream length per frame is denoted as $L_n^L$. Then the target per frame LLE stream length for channel n, $L_n^T$, may be computed as

$$L_n^T = L^T \cdot \frac{L_n^L}{L^L} \qquad (2)$$

The received lossless bit stream for each channel is for example truncated according to equation (2). The truncated bit stream may then be input to the decoding circuit 311,

e.g. a standard SLS decoder to achieve the subscribed quality.

In another embodiment, the target per frame LLE stream length is evenly distributed over the channels such that $L_n^T$ is equal for all n, i.e. for all channels.

The operation of the truncator 309 according to one embodiment is illustrated in figure 11.

FIG. 11 shows a truncator 1100 according to an embodiment.

The truncator 1100 receives a high quality bit stream 1101 including a high quality audio signal, i.e. decodable to an audio signal with high quality, as input. For example, the high quality bit stream 1101 is a lossless SLS bit stream corresponding to the third file 803 or the fourth file 804. For example, the high quality bit stream 1101 includes a first part 1102, a second part 1103, and a third part 1104, wherein the first part 1102 corresponds to a basic quality, i.e. is decodable to an audio signal of low quality, e.g. includes an audio signal encoded according to AAC, and the second part 1103 and the third part 1104 include a lossless enhancement bit stream (LLE) for the first part 1102. For example, the second part 1103 may be used to enhance the low quality audio signal decodable from the first part 1102 to generate a medium quality version of the audio signal and the third part 1103 may be used to enhance the medium quality audio signal to generate a high quality version of the audio signal.

The truncator 1100 truncates the high quality bit stream 1102 in accordance with a quality indication which for example

indicates that the third part 1104 should be removed from the high quality bit stream 1102 or the third part 1104 and the second part 1103 should be removed from the high quality bit stream 1102. It should be noted that "truncation" a part from a bit stream may refer to the removal of any parts of the bit stream that do not have to be necessarily be arranged at the end of the bit stream. Thus, data may be arranged in any way (e.g. in and order to form of a bit stream) while the removal of certain parts from the data is still referred to in this specification as a truncation of a bit stream corresponding to the data.

In one embodiment, the quality indication is based on a user key. For example, a first user key 1105 corresponds to low quality, a second user key 1106 corresponds to medium quality, and a third user key 1107 corresponds to high quality. In one embodiment, the truncator does not receive the quality indication itself but receives a user key 1105, 1106, 1107 and truncates the high quality bit stream 1101 in accordance with the quality corresponding to the user key 1105, 1106, 1107. The user key 1105, 1106, 1107 is for example provided to the user of the terminal device 302 based on the subscription or the amount the user has paid for the audio signal.

The user key 1105, 1106, 1107 may be a software key provided (e.g. transmitted) to the user in course of the subscription or after having paid for the audio file. It may also be a hardware key that is provided for the terminal device of the user.

In one embodiment, the user key may be determined and issued by the provider of the audio file. In contrast, in one

embodiment, the shared key used for encrypting and decrypting by the encryption circuit 304 and decryption circuit 308 may be set by the operator of the communication network that is used for the transmission of the encrypted error protected bit stream from the server communication device 301 to the terminal device 302, i.e. by the operator who provides the communication channel 306. Thus, in one embodiment, the specification of what parts to be truncated may be carried out independently from the operator providing the communication channel 306. For example, the same shared key may be used for encrypting and decrypting for different users even if the users have paid for different quality levels of the digital (e.g. audio) signal (i.e. a common key may be used for different users). Furthermore, the number of different quality levels that are used (i.e. the number of different qualities according to which the received bit stream is truncated) may be set by the provider of the audio signal independently from the operator providing the communication channel 306 and independently from the encryption/decryption method used.

The truncator truncates the high quality bit stream 1101 in accordance with the quality corresponding to the user key 1105, 1106, 1107 such that a low quality bit stream 1108 (decodable to the audio signal in low quality), a medium quality bit stream 1109 (decodable to the audio signal in medium quality) or a high quality bit stream 1110 (decodable to the audio signal in high quality) are generated. The low quality bit stream 1108 for example corresponds to the first part 1102 of the high quality bit stream 1101, the medium quality bit stream 1109 for example corresponds to the first part 1102 and the second part 1103 of the of the high quality bit stream 1101 and the high quality bit stream 1110 for

example corresponds to the first part 1102, the second part 1103, and the third part 1104 of the high quality bit stream 1101, i.e. to the whole high quality bit stream 1101.

It should be noted that "low", "medium", and "high" are only used as examples and may refer to any quality levels. Furthermore, any number of different quality levels (and correspondingly truncation levels) may be defined and used.

In one embodiment, the truncator 309 receives as input the target bit rate of the audio signal decodable from the truncated bit stream. This is illustrated in figure 12.

FIG. 12 shows a truncator 1200 according to an embodiment.

In this embodiment, the full (or high) quality bit stream includes an AAC core layer 1201 and a lossless enhancement layer 1202 as for example generated by the encoder 400 described with reference to figure 4 or the SLS enhancer 700 described with reference to figure 7.

The truncator 1200 receives one of the target bit rates $B_1$, $B_2$, …, $B_{N-1}$ as input and truncates the full quality bit stream such that the resulting truncated bit stream 1203 is decodable to an audio signal with the specified target bit rate. For example, if the bit rate $B_1$ is input to the truncator 1200, the full quality bit stream is truncated such that the resulting truncated bit stream 1203 includes the AAC core layer 1201 and a first part 1204 of the lossless enhancement layer. Similarly, if the bit rate $B_2$ is input to the truncator 1200, the full quality bit stream is truncated such that the resulting truncated bit stream 1203 includes the AC core layer 1201, the first part 1204, and a second

part 1205 of the lossless enhancement layer. Analogously, if higher bit rates are input to the truncator 1200, further parts of the lossless enhancement layer remain in the resulting truncated bit stream 1203. For example, bit rate $B_N$ is the highest bit rate and corresponds to the full lossless enhancement layer, i.e. can be achieved if the truncated bit stream includes the full lossless enhancement layer.

The quality indication may, as mentioned above, for example be received from the provider of the digital signal. Thus, according to one embodiment, a terminal device is provided including a receiver configured to receive a quality indication and a bit stream, and including a truncator configured to truncate the received bit stream in accordance with the quality indication.

Embodiments may for example be used with a Digital Audio Broadcast (DAB) network such that single-quality audio data is broadcast and the users are provided with multi-quality audio signals according to their individual subscription. Thus, only one version of the audio data needs to be transmitted which may for example lead to less audio broadcast stations being necessary compared to a scenario where an audio signal is broadcast in a plurality of qualities. Embodiments may also be used, for example, for an Internet radio service.

The following documents are cited in the specification:

[1] Scalable Lossless Coding (SLS), ISO/IEC 14496-3:2005/Amd 3, 2006.

[2] R. Yu, S. Rahardja, X. Lin, and C. C. Koh, "A fine granular scalable to lossless audio coder," IEEE Trans. Audio, Speech, Lang. Process., vol. 14, no. 4, pp. 1352-1363, Jul. 2006.

Claims

1. A terminal device comprising
a receiver configured to receive an encrypted bit stream which is decodable to a digital signal;
a decrypting circuit configured to decrypt the encrypted bit stream;
a truncator configured to receive a quality indication and configured to truncate the decrypted bit stream in accordance with the quality indication such that the truncated decrypted bit stream is decodable to a digital signal having a quality corresponding to the indicated by the quality indication; and
a decoder configured to decode the truncated bit stream.

2. The terminal device of claim 1, wherein the terminal device is a client device and the receiver is configured to receive the encrypted bit stream from a server device.

3. The terminal device of claim 1 or 2, wherein the digital signal is an audio signal or a video signal.

4. The terminal device of any one of claims 1 to 3, wherein the quality indication comprises the indication of a bit rate and the truncator is configured to truncate the decrypted bit stream such that the truncated decrypted bit stream is decodable to a digital signal having the indicated bit rate.

5. The terminal device of any one of claims 1 to 4, wherein the bit stream is an SLS bit stream.

6. The terminal device of any one of claims 1 to 5, wherein the bit stream includes the digital signal encoded in accordance with a scalable coding scheme.

7. The terminal device of claim 6, wherein the bit stream includes the digital signal encoded in accordance with SLS.

8. The terminal device of claim 7, wherein the decoder is an SLS decoder.

9. The terminal device of any one of claims 1 to 8, wherein the terminal device is an electronic communication device.

10. The terminal device of claim 9, wherein the terminal device is a mobile communication device.

11. The terminal device of any one of claims 1 to 10, wherein the truncator is configured to truncate the decrypted bit stream in accordance with the quality indication such that the truncated decrypted bit stream is not decodable to a version of the digital signal having a higher quality than the quality indicated by the quality indication.

12. The terminal device of any one of claims 1 to 11, wherein the encrypted bit stream is decodable to a digital signal of a plurality of digital signals wherein the digital signals are associated with different quality levels and wherein the truncator is configured to truncate the decrypted bit stream in accordance with the quality level indication such that the truncated

decrypted bit stream is decodable to the digital signal of the plurality of digital signals that is associated with the quality level indicated by the quality level indication but is not decodable to a digital signal associated with a higher quality level than the quality level indicated by the quality level indication.

13. The terminal device of any one of claims 1 to 12, wherein the quality indication is a key corresponding to a quality level.

14. The terminal device of claim 13, wherein the truncator is configured to determine the quality level from the user key and to truncate the decrypted bit stream in accordance with the quality level.

15. The terminal device of any one of claims 1 to 14, wherein the receiver is configured to receive the encrypted bit stream via streaming.

16. The terminal device of any one of claims 1 to 15, wherein the receiver is configured to receive the encrypted bit stream via broadcast or multicast.

17. A terminal device comprising
a receiver configured to receive a quality indication and a bit stream, and
a truncator configured to truncate the received bit stream in accordance with the quality indication.

18. A method for processing an encrypted bit stream comprising

receiving, in a terminal device, an encrypted bit stream which is decodable to a digital signal;
decrypting, in the terminal device, the encrypted bit stream;
truncating, in the terminal device, the decrypted bit stream in accordance with a quality indication such that the truncated decrypted bit stream is decodable to a digital signal having a quality corresponding to the indicated by the quality indication; and
decoding, in the terminal device the truncated bit stream.

19. A computer readable medium having computer instructions recorded thereon, which, when executed by a computer, make the computer perform a method for processing an encrypted bit stream comprising
receiving, in a terminal device, an encrypted bit stream which is decodable to a digital signal;
decrypting, in the terminal device, the encrypted bit stream;
truncating, in the terminal device, the decrypted bit stream in accordance with a quality indication such that the truncated decrypted bit stream is decodable to a digital signal having a quality corresponding to the indicated by the quality indication; and
decoding, in the terminal device the truncated bit stream.

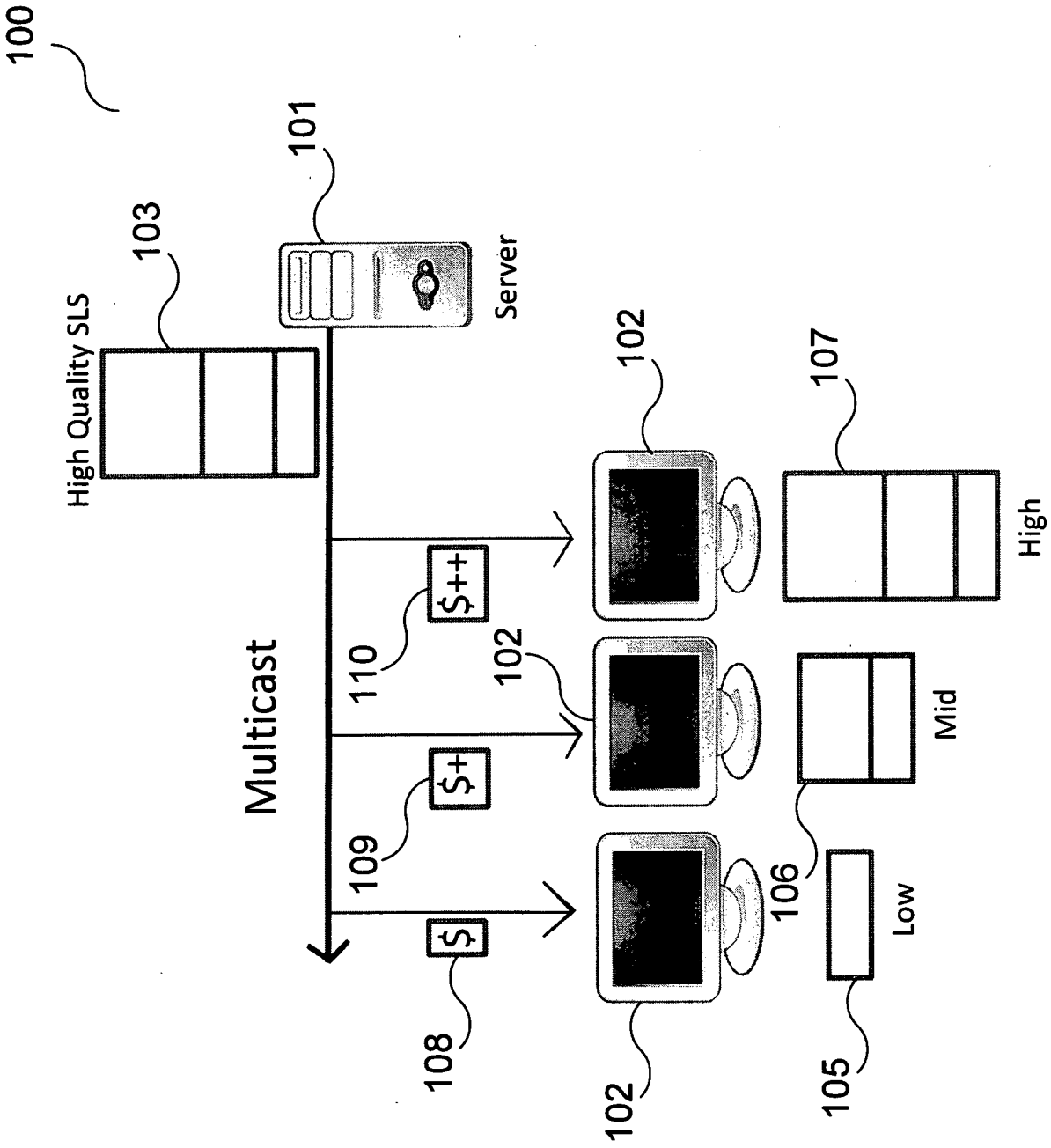

100
101
Server
103
High Quality SLS
102
107
High
Multicast
110
$++
102
Mid
109
$+
106
Low
108
$
102
105

FIG 1

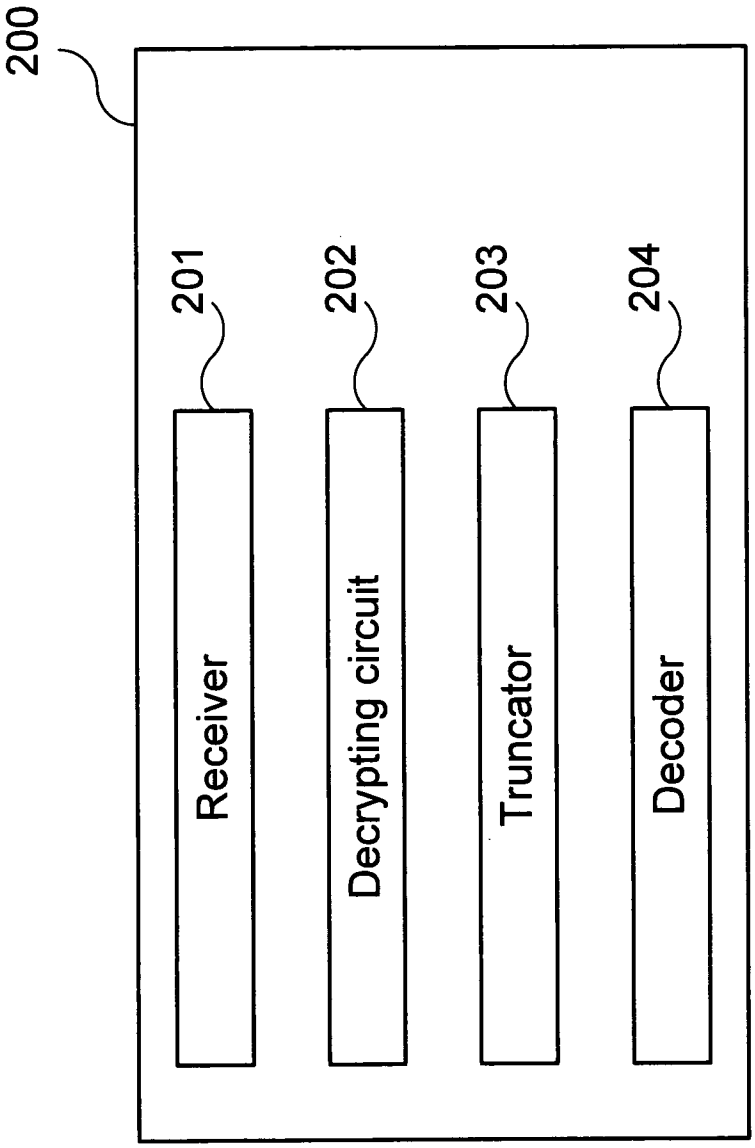

200
201
Receiver
202
Decrypting circuit
203
Truncator
204
Decoder

FIG 2

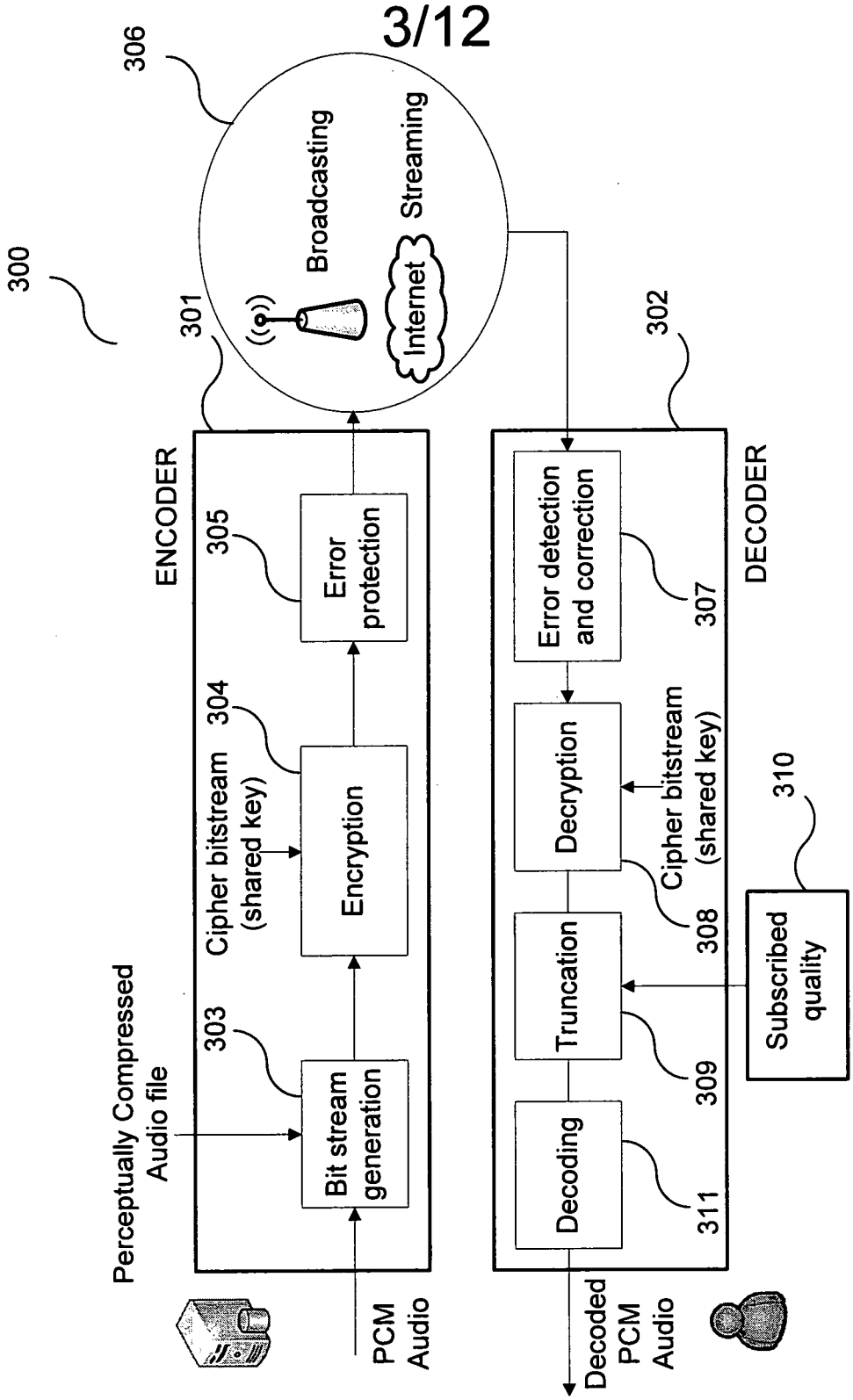

300
306
Broadcasting
Streaming
Internet
301
302
ENCODER
DECODER
305
Error protection
304
Cipher bitstream (shared key)
Encryption
303
Bit stream generation
Perceptually Compressed Audio file
PCM Audio
Error detection and correction
307
Decryption
Cipher bitstream (shared key)
308
Truncation
309
Decoding
311
Decoded PCM Audio
310
Subscribed quality

FIG 3

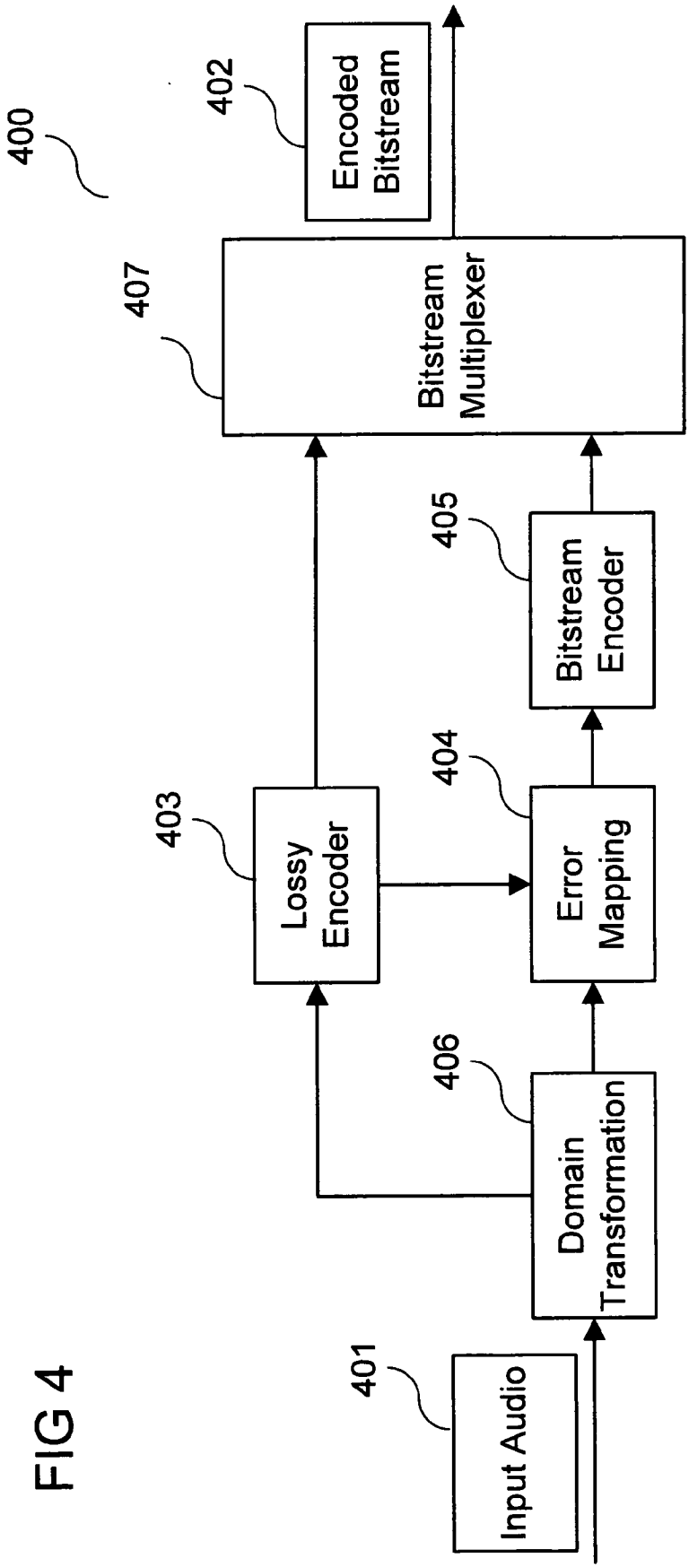

400
401
Input Audio
402
Encoded Bitstream
403
Lossy Encoder
404
Error Mapping
405
Bitstream Encoder
406
Domain Transformation
407
Bitstream Multiplexer

FIG 4

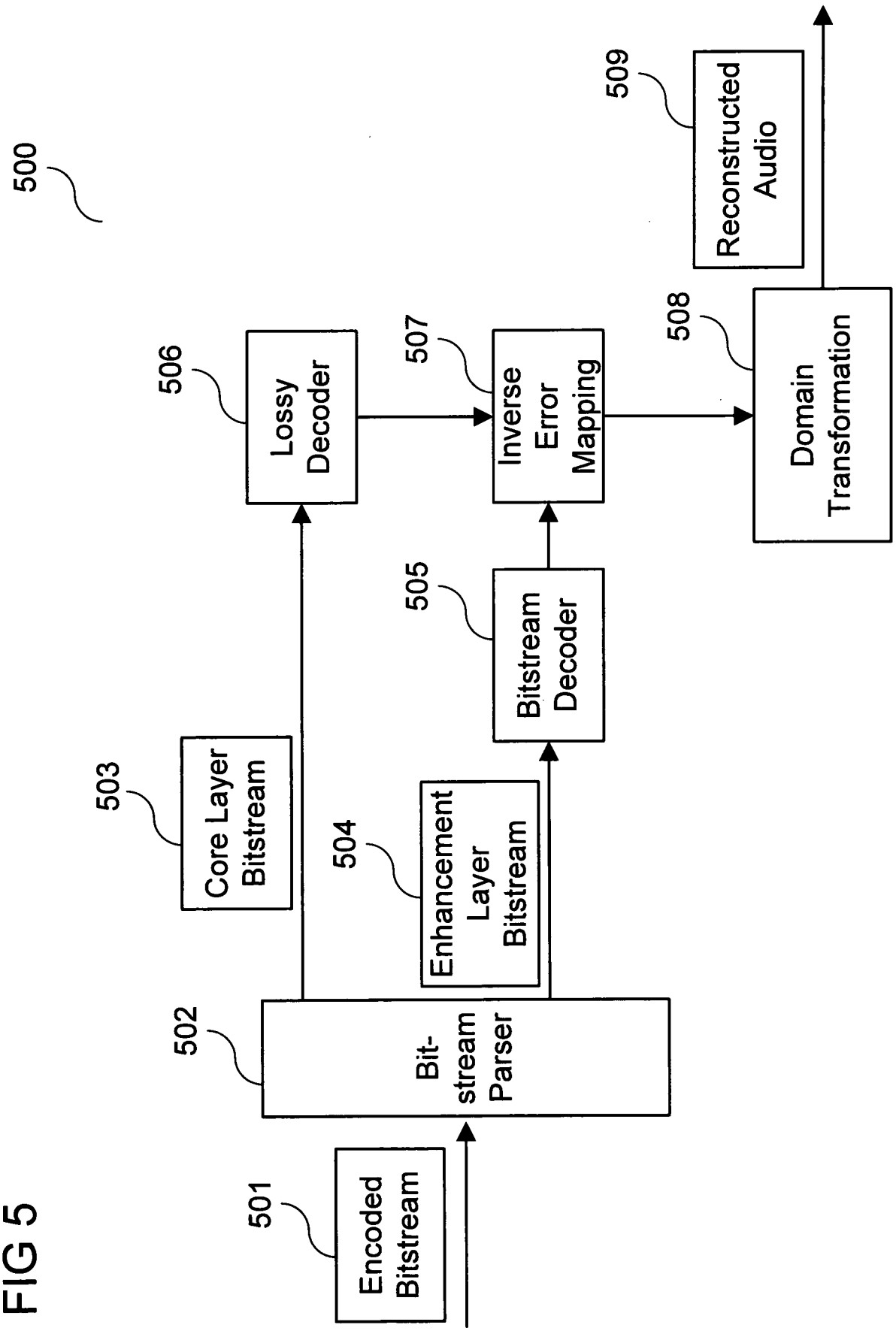
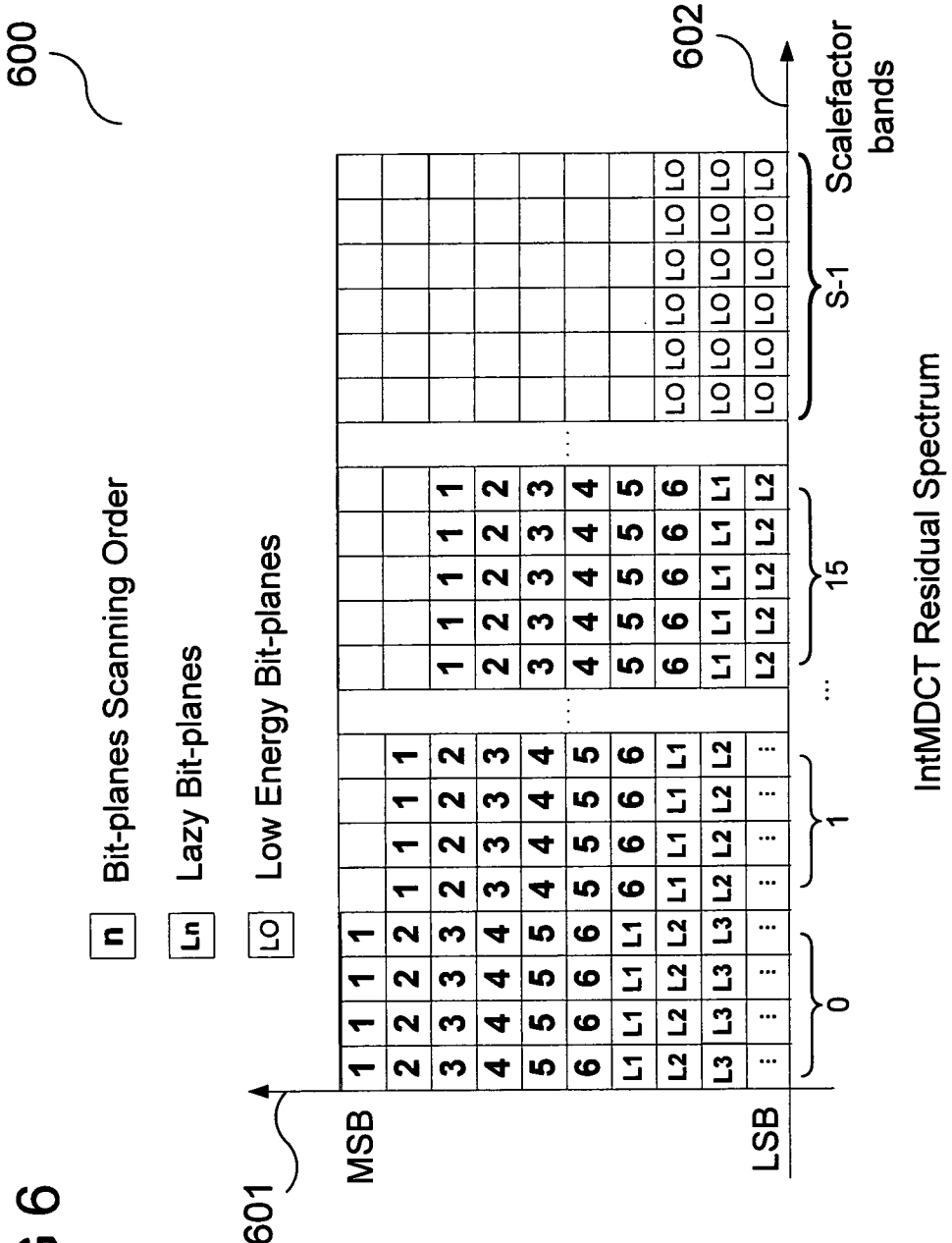

500
501
Encoded Bitstream
502
Bit-stream Parser
503
Core Layer Bitstream
504
Enhancement Layer Bitstream
505
Bitstream Decoder
506
Lossy Decoder
507
Inverse Error Mapping
508
Domain Transformation
509
Reconstructed Audio

FIG 5

FIG 6


600
n Bit-planes Scanning Order
Ln Lazy Bit-planes
LO Low Energy Bit-planes
601
MSB
LSB
602
0
1
15
S-1
Scalefactor bands
IntMDCT Residual Spectrum

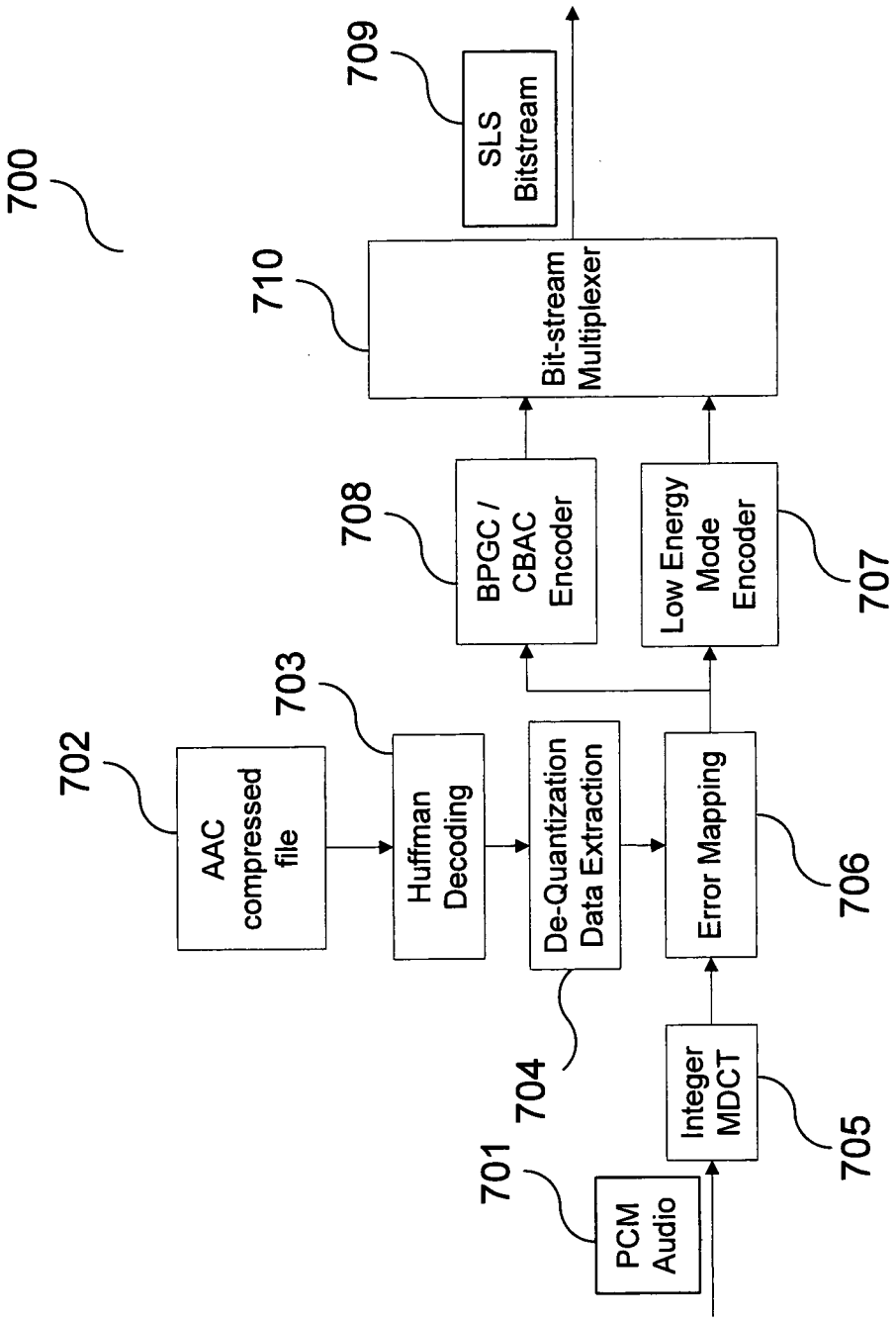

700
701
PCM Audio
702
AAC compressed file
703
Huffman Decoding
704
De-Quantization Data Extraction
705
Integer MDCT
706
Error Mapping
707
Low Energy Mode Encoder
708
BPGC / CBAC Encoder
709
SLS Bitstream
710
Bit-stream Multiplexer

FIG 7

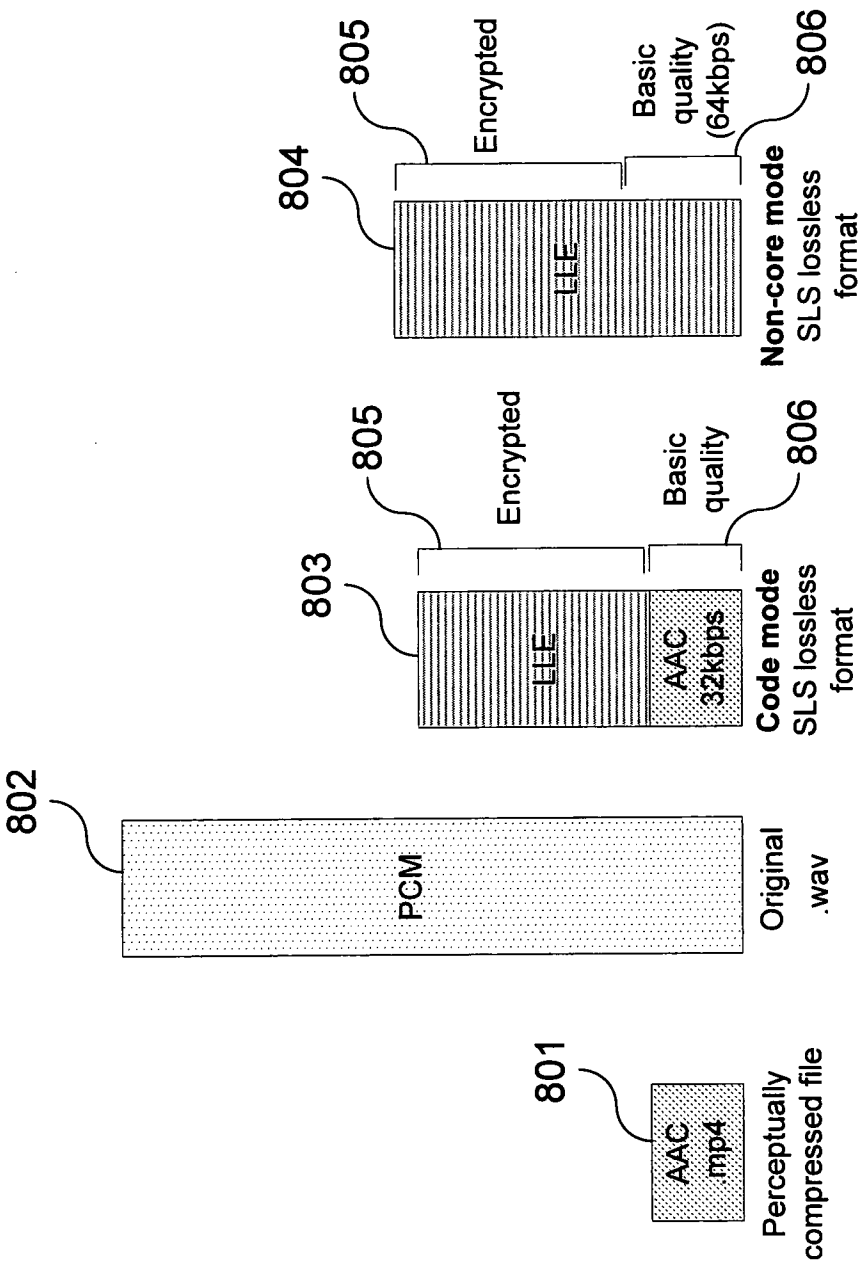

801
AAC
.mp4
Perceptually
compressed file
802
PCM
Original
.wav
803
LLE
AAC
32kbps
805
Encrypted
Basic
quality
806
Code mode
SLS lossless
format
804
LLE
805
Encrypted
Basic
quality
(64kbps)
806
Non-core mode
SLS lossless
format

FIG 8

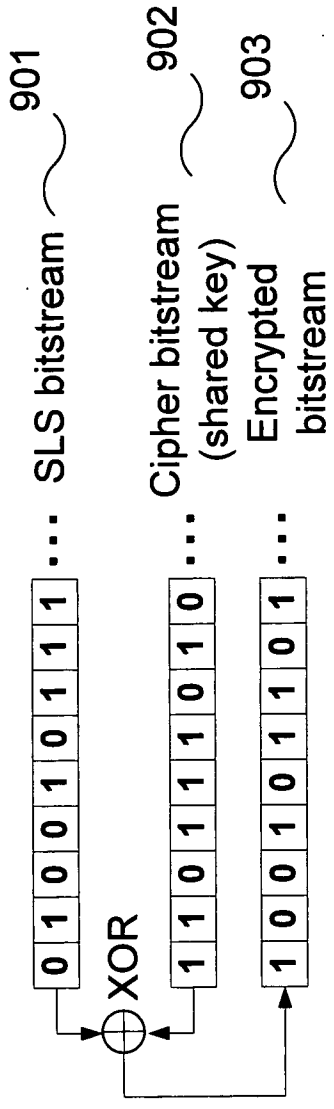

901
SLS bitstream
902
Cipher bitstream
(shared key)
903
Encrypted
bitstream
XOR

FIG 9

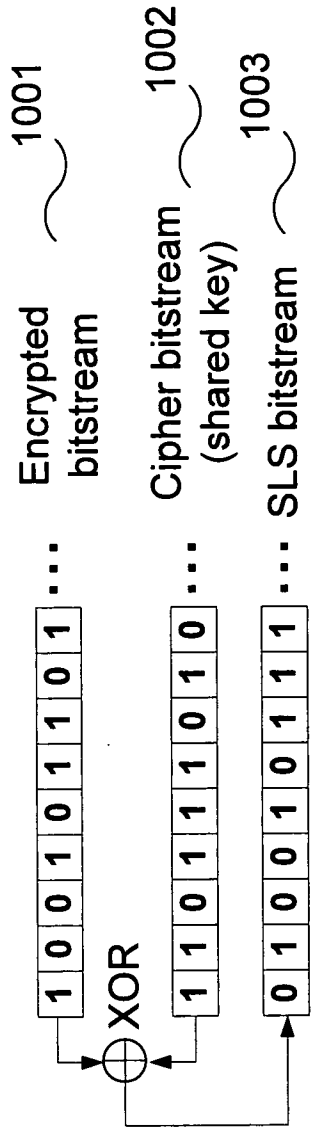

1001
Encrypted bitstream
1002
Cipher bitstream (shared key)
1003
SLS bitstream
XOR

FIG 10

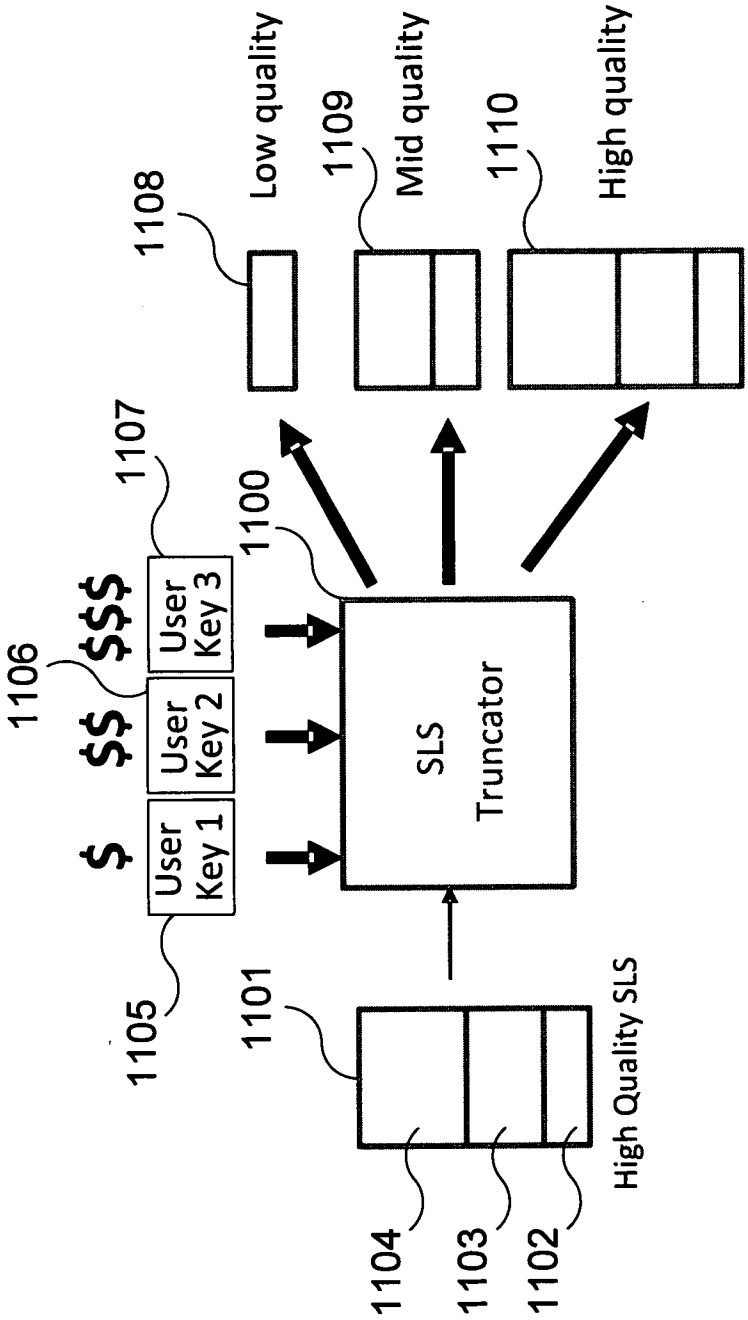

1108
Low quality
1109
Mid quality
1110
High quality
1107
1100
1106
$$$
$$
$
User Key 3
User Key 2
User Key 1
SLS Truncator
1105
1101
High Quality SLS
1104
1103
1102

FIG 11

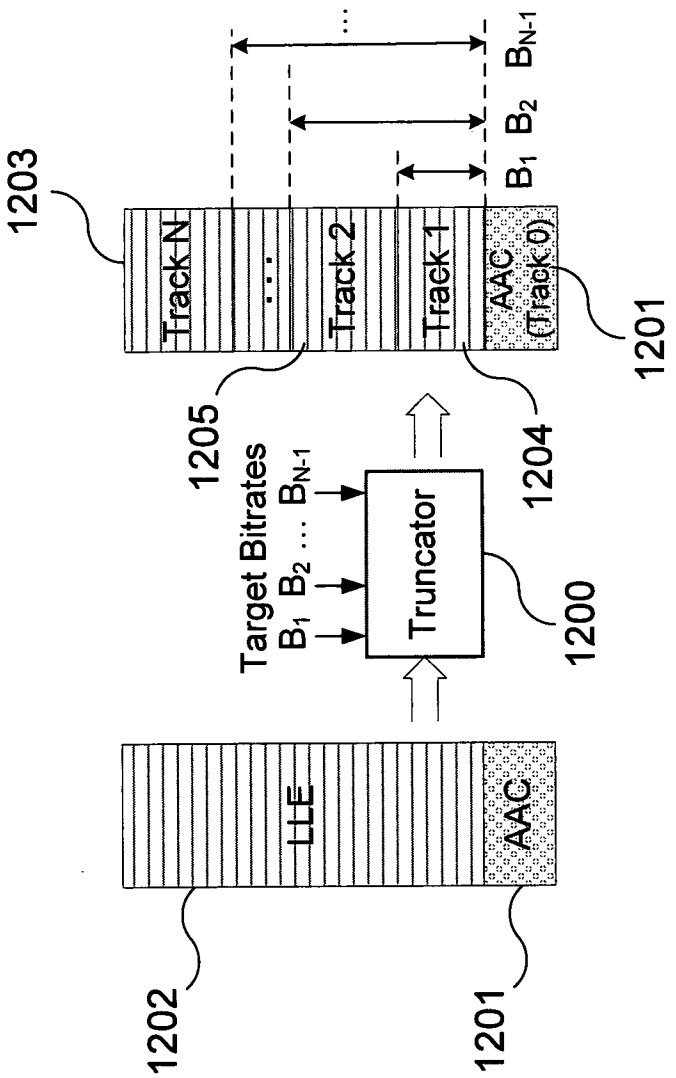

1203
Track N
Track 2
Track 1
AAC (Track 0)
1201
1205
1204
Target Bitrates
$B_1$ $B_2$ .... $B_{N-1}$
Truncator
1200
LLE
AAC
1202
1201

FIG 12

# INTERNATIONAL SEARCH REPORT

International application No.
PCT/SG2009/000307

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl. ***G06F 19/00*** (2006.01) ***H04L 9/18*** (2006.01) ***H04L 9/36*** (2006.01)

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
WPI, Patent Lens, Esp@cenet, WIPO & USPTO web patent database, internet "data stream, bit stream, decrypt etc."

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X | WO 2003/030542 A2 (HEWLETT-PACKARD COMPANY) 10 April 2003<br>Page 14 lines 24 to 36, page 17 line 5, page 17 lines 30 to 36, page 18 lines 31 to 39, page 19 lines 4 to 5, page 19 lines 12 to 14, figures 6, 11 and 20 in particular. | 1-4,6,9-12,15-19 |
| X | EP 1855436 A1 (DEUTSCHE THOMSON-BRANDT GMBH) 14 November 2007<br>Column 4 lines 40 to 46, column 5 lines 3 to 5, column 5 lines 19 to 42 and column 7 lines 16 to 22 in particular. | 1-3,5-19 |
| X | US 2005/0183118 A1 (WEE et al.) 18 August 2005<br>Paragraph 42 lines 9 to 11, paragraph 44, paragraph 53, paragraph 69, paragraph 73, paragraph 74 lines 1 to 3, paragraph 157 lines 10 to 13, paragraph 158 lines 1 to 4, paragraph 214 lines 9 to 18, paragraph 249, paragraph 251, paragraph 259 lines 6 to 10, Table 1, figures 23 and 26 in particular. | 1-12,15-19 |
| X | US 2002/0076043 A1 (VAN DER VLEUTEN et al.) 20 June 2002<br>Paragraph 6, paragraph 7 lines 5 to 9, paragraphs 15, 16 and 23 in particular. | 17 |
| A | WO 2009/096898 A1 (AGENCY FOR SCIENCE, TECHNOLOGY AND RESEARCH) 6 August 2009. Figures 8 and 9 in particular. | |
| A | WO 2007/004992 A1 (AGENCY FOR SCIENCE, TECHNOLOGY AND RESEARCH) 11 January 2007. Abstract in particular. | |

☐ Further documents are listed in the continuation of Box C ☒ See patent family annex

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| 20 October 2009 | 26 OCT 2009 |


Name and mailing address of the ISA/AU

AUSTRALIAN PATENT OFFICE
PO BOX 200, WODEN ACT 2606, AUSTRALIA
E-mail address: pct@ipaustralia.gov.au
Facsimile No. +61 2 6283 7999

Authorized officer
**PETER THONG**
AUSTRALIAN PATENT OFFICE
(ISO 9001 Quality Certified Service)
Telephone No : +61 2 6283 2128

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
**PCT/SG2009/000307**

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

| Patent Document Cited in Search Report | | Patent Family Member | | | | | |
|---|---|---|---|---|---|---|---|
| WO | 2003/030542 | EP | 1417834 | EP | 1436997 | EP | 1440577 |
| | | EP | 1446950 | US | 6983049 | US | 6990202 |
| | | US | 7136485 | US | 7184548 | US | 7349539 |
| | | US | 7409094 | US | 7463735 | US | 2002164018 |
| | | US | 2003012376 | US | 2003021296 | US | 2003041257 |
| | | US | 2003041258 | US | 2003068040 | US | 2003068041 |
| | | US | 2003070081 | US | 2005084132 | US | 2007036354 |
| | | WO | 02091743 | WO | 03030543 | WO | 03030544 |
| EP | 1855436 | CN | 101444065 | EP | 2018753 | US | 2009122992 |
| | | WO | 2007131885 | | | | |
| US | 2005/0183118 | EP | 1714496 | KR | 20060120257 | US | 7504968 |
| | | WO | 2005081536 | | | | |
| US | 2002/0076043 | AU | 20595/02 | BR | 0107307 | CN | 1398489 |
| | | EP | 1327360 | PL | 356718 | WO | 0232147 |
| WO | 2009/096898 | NONE | | | | | |
| WO | 2007/004992 | NONE | | | | | |

Due to data integration issues this family listing may not include 10 digit Australian applications filed since May 2001.

END OF ANNEX