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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
11 December 2003 (11.12.2003)

PCT

(10) International Publication Number
WO 03/103216 A2

(51) International Patent Classification[7]: H04L 9/08

(21) International Application Number: PCT/GB03/02381

(22) International Filing Date: 2 June 2003 (02.06.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

PCT/GB02/02512	31 May 2002 (31.05.2002)	GB
0228428.9	5 December 2002 (05.12.2002)	GB
0228434.7	5 December 2002 (05.12.2002)	GB

(71) Applicant *(for all designated States except US)*: **SCIENTIFIC GENERICS LIMITED** [GB/GB]; Harston Mill, Harston, Cambridgeshire CB2 5GG (GB).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **DUFFY, Dominic, Gavan** [GB/GB]; Scientific Generics Limited, Harston Mill, Harston, Cambridgeshire CB2 5GG (GB). **JONES, Aled, Wynne** [GB/GB]; Scientific Generics Limited, Harston Mill, Harston, Cambridgeshire CB2 5GG (GB).

(74) Agents: **BERESFORD, Keith, Denis, Lewis** et al.; Beresford & Co., 2-5 Warwick Court, High Holborn, London WC1R 5DH (GB).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

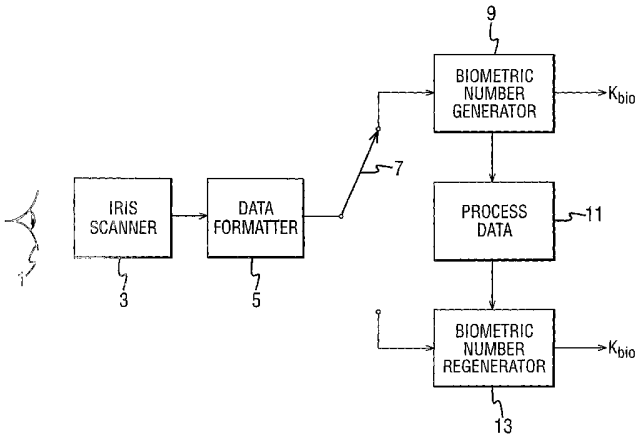
(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: DATA PROCESSING APPARATUS AND METHOD



(57) Abstract: There is described a process for generating a number representative of an analogue data source in which during enrolment a distinctive characteristic of the analogue data source is measured to obtain physical data. Part of the physical data is used to generate a physical value which is representative of the analogue source. An error correction algorithm is applied to the physical value to generate error correction data, which is then transformed, using another part of the physical data, to generate transform data. During subsequent regeneration of the physical value, the distinctive characteristic is re-measured to generate a new set of physical data, and a physical value is generated using the same part of the physical data as was used during enrolment. Error correction data is then generated by transforming the transform data, using an inverse transform to that used during enrolment, using the same part of the physical data as was used to transform the error correction data during enrolment. The regenerated error correction data is then used by the error correction algorithm to correct errors in the physical value representative of the analogue source. By using part of the physical data set to transform the error correction data and then storing the resulting transform data, the security of the original physical data is improved.

WO 03/103216 A2

DATA PROCESSING APPARATUS AND METHOD

This invention relates to the generation of a number representative of data from an analogue source. The invention has particular, but not exclusive, relevance to generating a number representative of an individual by processing biometric data obtained by measuring a distinctive characteristic of the individual.

Every individual has a number of distinctive characteristics (e.g. fingerprints, iris patterns and retinal patterns) having attributes which can be measured to generate biometric data representative of the individual, and these distinctive characteristics form the basis of many identification systems. Generally, during an enrolment process a reference set of biometric data is generated for an individual, and in a subsequent identification process a new set of biometric data is measured and compared with the reference set of biometric data. A positive identification is made if the new set of biometric data is sufficiently similar to, but not necessarily identical with, the reference set of biometric data. The reason why the newly measured set of biometric data need not be identical with the reference set of biometric data for a positive identification is that each time the same distinctive characteristic is measured, slightly different biometric data is generated due to the analogue nature (i.e. having values within a continuous range) of the measured attributes of the distinctive feature.

A paper entitled "On the relation of error correction and cryptography to an offline biometric based identification scheme", WCC99, Workshop on Coding and cryptography

January 1999,Paris, France, describes generating a biometric value which is exactly reproducible on a regular basis by employing error detection and correction techniques. In particular, this paper describes measuring the iris of an individual during enrolment to obtain an array of binary digits (bits), and applying conventional error correction algorithms, as are commonly used in forward error correction (FEC) encoding in digital data communication, to generate corresponding check bits. During a subsequent identification, the iris of the individual is re-measured to form a new array of data bits, and then the error correction algorithm corrects the new array of data bits using the check bits generated during enrolment. A disadvantage of this system is that the check bits generated during enrolment must be stored, and could therefore be used to aid fraudulent use of the biometric value for the individual.

An object of the present invention is to provide alternative schemes using error correction algorithms to enable a repeatable value to be derived from data obtained by measuring an analogue data source.

According to an aspect of the invention, there is provided a process for generating a number representative of an analogue data source in which during enrolment a distinctive characteristic of an analogue source is measured to obtain physical data, which is separated into parts. A first part is used to generate a physical value which is representative of the analogue source. An error correction algorithm is applied to the physical value to generate error correction data, which is then transformed by a binomial mapping operation, using a second part of the physical data, to generate transform data. During subsequent regeneration of the physical value, the

distinctive characteristic is re-measured to generate a new set of physical data, which is separated into parts in the same manner as during enrolment. A physical value is regenerated using a first part of the physical data in the same manner as during enrolment, and error correction data is generated by transforming the transform data, using an inverse transform to that used during enrolment, using a second part of the new set of physical data. The regenerated error correction data is then used by the error correction algorithm to correct errors in the physical value representative of the analogue source.

By using part of the physical data set to transform the error correction data and then storing the resultant transform data, the security of the original physical data is improved.

If the inherent randomness of the physical data is high, then in a preferred embodiment plural error correction operations are performed. In particular, during enrolment, the physical data is processed as described above to generate an intermediate data and a first set of transform data. The intermediate data is then split into two parts, the first part forming a physical value and the second part forming redundant data which is used to generate a second set of transform data. This process may continue iteratively until the repeatability of the physical value reaches an acceptable level, although each additional error correction operation reduces the size, and therefore the distinctiveness, of the final physical value.

According to another aspect of the invention, there is provided a process for generating a number representative

of an analogue data source in which during enrolment a distinctive characteristic of an analogue source is measured to obtain physical data having a plurality of data elements, with at least some of the data elements comprising plural binary digits. As the likelihood of errors occurring in the higher significant bits of the data elements is less than in the lower significant bits, the lower significant bits are processed using an error correction technique having a higher power of error correction than a different error correction technique which is used for the higher significant bits. In this way, the amount of error correction data required can be minimised.

Various embodiments of the invention will now be described with reference to the accompanying Figures in which:

Figure 1 schematically shows the main components of a number generation system according to the invention;

Figure 2 schematically shows the main components of a number generator and process data forming part of the number generation system illustrated in Figure 1;

Figure 3 schematically shows the main components of a source data splitter forming part of the number generator illustrated in Figure 2;

Figure 4 schematically shows the main components of an error correction data generator forming part of the number generator illustrated in Figure 2;

Figure 5 schematically shows the main components of a number regenerator forming part of the number generation system illustrated in Figure 1, together with the main components of the process data;

Figure 6 schematically shows the main components of a source data splitter forming part of the number regenerator illustrated in Figure 5;

Figure 7 schematically shows the main components of an error corrector forming part of the number regenerator system illustrated in Figure 5;

Figure 8 shows the main components of a number generator which forms part of a first alternative number generation system;

Figure 9 shows the main components of a number regenerator which forms part of the first alternative number generation system;

Figure 10 shows the main components of a number generator which forms part of a second alternative number generation system;

Figure 11 shows the main components of a number regenerator which forms part of the second alternative number generation system; and

Figure 12 shows the main components of an error corrector forming part of the number regenerator illustrated in Figure 11.

FIRST EMBODIMENT

OVERVIEW

Figure 1 schematically shows the main components of a system for generating a biometric number K_{bio} from the iris pattern of an eye 1 of a human being. As shown, an iris scanner 3 records an image of the eye 1 and outputs corresponding image data to a data formatter 5, which configures the image data into a standard format. In this embodiment, the data formatter 5 processes the image data using the image processing techniques described in US Patent No. 5,291,560, whose full content is hereby incorporated by reference, to form an iris code comprising four thousand and ninety-two bits arranged in a five hundred and twelve by eight array.

During enrolment, a switch 7 directs the iris code generated by the data formatter 5 to a biometric number generator 9, which processes the iris code to generate a biometric number K_{bio} and process data 11 which is stored for use in a subsequent biometric number regeneration operation. In particular, as will be described in more detail hereafter, the biometric number generator 9 splits the iris code into two parts, uses the first part to generate the biometric number K_{bio} and error correction data, and uses the second part to transform the error correction data to generate transform data which is stored as part of the process data 11.

During a biometric number regeneration operation, iris scanner 3 records a new image of the eye 1, and the data formatter 5 configures the resultant image data to produce a new iris code. The switch 7 directs the new iris code produced by the data formatter 5 to a biometric number regenerator 13 which, using the process data 11, regenerates the biometric K_{bio}.

The operation of the biometric number generator 9 during enrolment and the biometric number regenerator 13 during the regeneration of the biometric number K_{bio} will now be described in more detail.

ENROLMENT MODE

Figure 2 shows the main components of the biometric number generator 9 and the process data 11. As shown, the number generator 9 comprises a source data splitter 21 which splits the bit stream of data from the iris code, hereafter called S-data, into two bit streams in accordance with control signals from a controller 23. In particular, the source data splitter 21 outputs a first data bit stream conveying data, hereafter called

K-data, for forming the biometric number, and a second data bit stream conveying data, hereafter called R-data, for use in the generation of the transform data.

The relative proportions of S-data used for forming the K-data and the R-data are determined by the error correction algorithm applied by the biometric number generator 9. In this embodiment, the error correction algorithm simply receives a single data bit of K-data, and outputs a corresponding codeword comprising the data bit followed by four check bits each having the same value as the received data bit. Therefore, if the error correction algorithm unit receives a data bit having a value "0", the error correction algorithm unit outputs the codeword "00000". This algorithm will hereafter be referred to as the repetition/voting algorithm, and is applied by a repetition/voting algorithm unit 25.

In general, any error correction algorithm receives a block of k bits of data, generates p check bits, and outputs a codeword having k+p bits. Therefore, for the repetition/voting algorithm used in this embodiment, the k value is one and the p value is four.

One bit of R-data is required for each check bit in order to generate transform data. Therefore, in this embodiment only one-fifth of the S-data can be used to form K-data because the remaining four-fifths are required to form R-data. In order to ensure that the source data splitter 21 splits the S-data into K-data and R-data in the correct proportions, the controller interrogates the repetition/voting algorithm unit 25 to determine the k and p values, and sends a control signal to the source data splitter indicative of the determined k and p values.

The source data splitter 21 also outputs reference map data 27, which forms part of the process data 11, indicating for each bit of the K-data and the R-data the location of the corresponding bit of S-data. In this way, during a subsequent number regeneration operation, it can be ensured that the same bits of S-data are used to form the K-data and the R-data as the enrolment process.

As well as being output by the number generator 9 to form the biometric number K_{bio}, the K-data bit stream is input to an error correction data generator 29, which is connected to the repetition/voting algorithm unit 25. In this embodiment, the error correction data generator 29 sends each bit of K-data to the repetition/voting algorithm unit 25, extracts the check bits from the corresponding codewords returned by the repetition/voting algorithm unit 25, and outputs the extracted check bits as a stream of error correction data, hereafter called EC-data. The EC-data bit stream output by the error correction data generator 29 and the R-data bit stream output by the source data splitter 21 are input to a transform data generator 31, which applies a bitwise exclusive-OR operation to the EC-data bit stream and the R-data bit stream to generate transform data 33, which forms part of the process data 11.

As an example, for a sequence "100" of K-data, the corresponding EC-data bit stream is "111100000000". If the corresponding sequence of R-data is "101110100100", then the resulting transform data is "010010100100". It will be appreciated that, without knowledge of the corresponding R-data sequence, the EC-data cannot be recovered from the transform data and therefore the stored transform data 11 gives no information about the

K-data which forms the biometric value K_{bio}.

The source data splitter 21 will now be described in more detail with reference to Figure 3. As shown, the source data splitter 21 includes a reference word generator 41 which receives the number N of data elements in the iris code (in this embodiment four thousand and ninety-two) and the control signal from the controller 23 indicating a k value of one and a p value of 4. The reference word generator 41 then generates a reference data stream having N data elements, with each data element comprising a map code indicting the position of that data element within the reference data stream. In particular, in this embodiment the first data element of the reference data stream has a map code "0", the second data element has a map code "1", the third data element has a map code "2", and so on until the final data element which has a map code "4091".

The reference word generator 41 then partitions the reference data stream into a sequence of words, each word formed by k+p consecutive data elements, and discards any data elements at the end of the data stream which are not contained in a full word. Therefore, as in this embodiment k+p equals five, the reference word generator 41 separates the four thousand and ninety-two data elements into a sequence of eight hundred and eighteen words, each including five consecutive data elements, and discards the remaining two data elements.

The reference word generator 41 outputs the generated sequence of words to a data scrambler 43, which performs a pseudo-random scrambling of the data elements (i.e. a shuffling which appears random in nature but is in fact deterministic), and the shuffled data elements are output

to a reference map generator 45, which forms a reference map indicating the position in the S-data of each bit of K-data and R-data. The reference map generator 45 receives the k and p values from the controller 23 in order to ensure that the correct amounts of S-data are apportioned to K-data and R-data.

The source data splitter 21 also includes a data partitioner 47, which receives and caches the bit stream of S-data from the data formatter 5. The data partitioner 47 then uses the reference map generated by the reference map generator 45 for the K-data and R-data bit streams. In particular, to form the K-data bit stream the data partitioner 47 looks up in the reference map data the location of the bit of the S-data bit stream which forms the first bit of the K-data, and outputs the value of the located bit, and so on for the second and subsequent bits of the K-data bit stream. The R-data bit stream is formed by the data partitioner 47 using the reference map data in an analogous way to the K-data bit stream. Therefore, in this embodiment the data partitioner outputs a K-data bit stream comprising eight hundred and eighteen bits and a R-data bit stream comprising three thousand two hundred and seventy-two bits.

As stated previously, the data formatter 5 stores the iris code in the form of a bit array having eight rows and five hundred and twelve columns. Although there is a high level of randomness to the values of the bit array, in this embodiment the data in each column, which corresponds to a radial direction of the iris, shows a level of order. The data formatter 5 outputs the iris code column by column, and therefore neighbouring bits of the S-data bit stream show some measure of

correlation. However, the pseudo-random scrambling performed by the data scrambler 43 disperses the data elements in each column and therefore increases the randomness of the K-data and R-data bit streams. A further advantage of dispersing the data elements in each column is that if there is a localised group of errors in the iris code, then it is easier to correct the group of errors after dispersion.

In this embodiment, the data scrambler 43 performs two data scrambling operations. Firstly, the data scrambler 43 shuffles the words received by the reference word generator 41. The data scrambler 43 then forms an array by sequentially stacking the shuffled words. Therefore, in this embodiment, the array is formed by eight hundred and eighteen rows each having five data elements. The data scrambler 43 then performs a rotational shifting operation of the data elements in each column. In this embodiment, in the rotational shifting operation: the data elements of the first column remain in the same locations within the array; the data elements of the second column are shifted down the column one hundred and sixty-four places (i.e. are shifted by approximately one fifth of the size of the column) so that the first data element in the column becomes the one hundred and sixty-fifth data element in the column, and the bottom one hundred and sixty-four data element are shifted to the top of te column; in the same manner, the data elements of the third, fourth and fifth columns are shifted by three hundred and twenty-eight, four hundred and ninety-two and six hundred and fifty-six places respectively.

The data scrambler 43 outputs the array formed by the shuffling operation to the reference map generator 45, which separates the first k columns (i.e. in this

embodiment the first column) to provide the locations of the data elements in the S-data bit stream to form the K-data bit stream, and then uses the remaining p columns to provide the locations of the data elements in the S-data bit stream to form the R-data bit stream.

The error correction data generator 29 will now be described in more detail with reference to Figure 4. As shown, the K-data bit stream is input to a data block generator 51, together with a control signal from the controller 23 indicating the value of the number k of data bits to be included in each block of data bits sent to the repetition/voting algorithm unit 25. The data block generator 51 partitions the K-data bit stream into a sequence of data blocks having k (i.e. in this embodiment one) bit, and outputs the sequence of data blocks to a data block transmitter 53, which sequentially transmits the data blocks to the repetition/voting algorithm unit 25. For each data block transmitted, the repetition/voting algorithm unit 25 returns a codeword comprising the k data bits and p check bits. Each codeword is received by a codeword receiver 55, which forwards each received codeword to a check bits pass filter 57 which removes the k data bits and outputs the p check bits to form the EC-data bit stream.

REGENERATION MODE

Figure 5 schematically shows the main components of the biometric number regenerator 13. As described previously, during regeneration a new image is formed of the eye 1 and the corresponding image data processed by the data formatter 5 to form a new iris code. As shown, a S'-data bit stream output by the data formatter 5 during enrolment is input to a source data splitter 61, which splits the S'-data bit stream into a K'-data bit

stream and a R'-data bit stream in accordance with a control signal from a controller 63 and using the reference map data 27 forming part of the process data 11 generated during enrolment. The control signal from the controller 63 conveys the values of k and p associated with a repetition/voting error correction algorithm unit 65 (i.e. a k value of one and a p value of four), which is connected to the controller 63.

The K'-data bit stream and the R'-data bit stream are input to an error corrector 67 and an error correction data generator 69 respectively. The error correction data generator 69 applies a bitwise exclusive-OR operation to the R'-data bit stream and the transform data 33 generated during enrolment, to form an EC'-data bit stream, which is input to the error corrector 67. The error corrector 67 forms a sequence of codewords using the K'-data bit stream and the EC'-data bit stream and outputs each codeword to the repetition/voting algorithm unit 65. In this embodiment, each codeword is formed by one bit from the K'-data bit stream followed by four bits from the EC'-data bit stream. For each received codeword, the repetition/voting algorithm unit 65 performs a voting operation to determine which bit value appears more often (hereafter called the majority bit value), converts all of the bits of the codeword to the determined majority bit value to form a converted codeword, and outputs the converted codeword.

For example, as described above if during enrolment the K-data bit stream has a sequence 100 and the corresponding sequence of the R-data bit stream is "101110100100", then the stored transform data is "010010100100". In a subsequent regeneration operation, the generated K'-data and R'-data bit streams normally

exhibit a number of differences from those generated during enrolment, and a typical example of corresponding bit sequences for the K'-bit stream and the R'-bit stream would be "101" and "100110001100" respectively. The error correction data generator 69 applies a bitwise exclusive-OR operation on the R'-data bit stream and the corresponding stored transform data to generate the EC'-data sequence "110100101000".

The error corrector 67 combines each bit of the K'-data bit sequence with the corresponding four bits of the EC'-data bit stream to form the following three codewords:

codeword 1 - 11101
codeword 2 - 00010
codeword 3 - 11000

The codewords are then sequentially sent to the repetition/voting algorithm unit 65, which sets all the bits of each codeword to the majority bit value for the codeword, and returns the corrected codewords:

corrected codeword 1 - 11111
corrected codeword 2 - 00000
corrected codeword 3 - 00000

From the corrected codewords, the error corrector 67 retrieves the data bits to form the corrected K'-data bit sequence "100", which is identical with the corresponding K-bit sequence generated during enrolment.

Figure 6 shows the main components of the source data splitter 61. The control signal from the controller 63 indicating the values of k and p, which as described

above are one and four respectively in this embodiment, are input to a reference map generator 75 together with the reference map data 27. The reference map generator 75 generates a reference map indicating for each bit of the K'-data and R'-data bit streams the location of the corresponding bit of the S'-data bit stream.

The S'-data bit stream is input to a data partitioner 77 which caches the S'-data bit stream, and then outputs the K'-data bit stream and the R'-data bit stream using the reference map provided by the reference map generator 75. In particular, for each bit of the K'-data and the R'-data bit streams, the data partitioner 77 identifies and outputs the corresponding bit of the S'-data bit stream using the reference map.

Figure 7 shows the main components of the error corrector 67. As shown the K'-data bit stream is input to a data bits block generator 81 which groups the K'-data into blocks of k bits, the value of k being provided by a control signal from the controller 63. Similarly, the EC'-data is input to a error correction bits block generator 83 which groups the EC'-data into blocks of p bits, with the value of p being provided by a control signal from the controller 63. The data bit blocks and the error correction bits blocks are sequentially input to a codeword generator 85, which concatenates each data bit block with the corresponding error correction bit block to form a codeword.

The codeword generator 85 sequentially outputs the generated codewords to a codeword transmitter 87, which transmits each codeword to the repetition/voting algorithm unit 65. The corrected codewords produced by the repetition/voting algorithm unit 65 are received by

a corrected codeword receiver 89 and forwarded to a data bits pass filter 91, which removes the check bits of the codeword and outputs the corrected data bits to form the biometric number K_{bio}.

SECOND EMBODIMENT

OVERVIEW

In the first embodiment, the iris code from the data formatter 5 is split into two parts. During enrolment, the first part is used to generate a biometric number K_{bio} and associated error correction data, and the second part is used to transform the error correction data to form transform data. During biometric number regeneration, the first part of the iris code is used to regenerate the biometric number, and the second part is used to revert the transform data back to error correction data. The error correction data is then used to correct errors in the regenerated biometric number.

The generated biometric number K_{bio} has eight hundred and eighteen bits. With this size of biometric number, there may still be a significant possibility of errors in one or more of the bits. A second embodiment will now be described, with reference to Figures 8 and 9, in which two passes of error correction are performed to reduce the likelihood of error in the biometric number K_{bio}. In Figures 8 and 9, components which are identical to corresponding components of the first embodiment have been referenced by the same numerals and will not be described in detail again.

ENROLMENT MODE

Figure 8 schematically shows the main components of a number generator 101 of the second embodiment, which

during enrolment receives S-data from a data formatter which is identical to the data formatter of the first embodiment. The S-data is input to a source data splitter 21, which is identical to the source data splitter 21 of the first embodiment. In this embodiment, the first pass of error correction uses a repetition/voting algorithm unit 25 which applies the same repetition/voting algorithm as described in the first embodiment. A controller 103 interrogates the repetition/voting algorithm unit 25 to determine the associated k value and p value, and sends a control signal to the source data splitter 21 indicated the determined k and p values. Therefore, in this embodiment the control signal received by the source data splitter 21 indicates that the value of k is one and the value of p is four.

The source data splitter 21 outputs a K_1-data stream and a R_1-data stream, together with reference map data 27 which forms part of process data 105, in the same manner as described in the first embodiment. The K_1-data stream output by the source data splitter 21 is processed by the first error correction data generator 29a, using the repetition/voting algorithm unit 25, in the same manner as described in the first embodiment to generate an EC_1-data stream. The R_1-data stream and the EC_1-data stream are then input into a first transform data generator 31a, which performs an exclusive-OR operation to generate a first set of transform data 33 which is stored as part of the process data 105.

In this embodiment, the eight hundred and eighteen bits of K_1-data form intermediate source data which is processed in a similar manner to the S-data to generate the biometric number K_{bio} and a second set of transform

data 105. In this embodiment, a Golay (23,12) error correction algorithm, which is a conventional error correction algorithm used for FEC encoding in digital data communications is used during the processing of the K_1-data. For the Golay (23,12) error correction algorithm, a block of twelve data bits are processed to generate a block of eleven check bits, and the data bits and check bits are then combined to form a twenty-three bit codeword. Therefore, for the Golay (23,12) algorithm the value of k is twelve and the value of p is eleven.

The Golay (23,12) error correction algorithm is applied by a Golay (23,12) algorithm unit 109, and the controller interrogates the Golay (23,12) algorithm unit 109 to determined the k value of twelve and the p value of eleven. As shown in Figure 8, the K_1-data bit stream is input to a data splitter 107 together with a control signal from the controller 103 indicating the determined k and p values for the Golay (23,12) algorithm unit. The data splitter 107 partitions the K_1-data bit stream into blocks of twenty-three bits, and for each block outputs the first twelve bits as a sequence of a K_2-data bit stream and the remaining eleven bits as a sequence of a R_2-data bit stream. In this way, the eight hundred and eighteen bits of K_1-data form a four hundred and twenty bit sequence of K_2-data, which forms the biometric number K_{bio}, and a three hundred and eighty-five bit sequence of R_2-data. The final eighteen bits of K_1-data are discarded.

The K_2-data bit stream is input to a second error correction data generator 29b, together with a third control signal from the controller 103 conveying a k value of eleven and a p value of twelve. The second error correction data generator 29b is functionally

identical to the error correction data generator of the first embodiment. In particular, in accordance with the control signal from the controller 103, the second error correction data generator 29b partitions the K_2-data bit stream into blocks of twelve data bits and sends each block to the Golay (23,12) algorithm unit 109, which applies the Golay (23,12) algorithm to generate a twenty-three bit codeword comprising the twelve data bits and eleven check bits. The Golay (23,12) algorithm unit 109 outputs each codeword to the second error correction data generator 29b, which extracts the check bits from each codeword and outputs the extracted check bits as an EC_2-data bit stream.

The EC_2-data stream is input, together with the R_2-data bit stream, to a second transform generator 31b which applies a bitwise exclusive-OR operation to the EC_2-data bit stream and the R_2-bit stream to form second transform data 111, which is stored as part of the process data 105.

REGENERATION MODE

Figure 9 schematically shows the main components of the number regenerator 121 of this embodiment. The S'-data from the data formatter 5 is input to a source data splitter 61, which is identical to the source data splitter of the number regenerator of the first embodiment. A controller 123 interrogates a repetition/voting algorithm unit 65 to determine the associated k and p values, and outputs a control signal to the data splitter 61 indicating a k value of one and a p value of 4. The source data splitter 61 converts the S'-data into a K_1'-data bit stream and a R_1'-data bit stream in accordance with the control signal from the controller 123, using the reference map 27 in the process

data 105 generated during enrolment.

The R_1'-data bit stream is input, together with the first set of transform data 33 of the process data 105 generated during enrolment, to a first error correction data generator 69a, which applies a bitwise exclusive-OR operation to generate an EC_1'-data bit stream. The K_1'-data and the EC_1'-data bit streams are input to an error corrector 67a which, in the same manner as in the first embodiment, outputs a corrected K_1'-data bit stream using the repetition/voting algorithm unit 65, which applies the same repetition/voting error correction algorithm as the first embodiment.

The eight hundred and eighteen bits of the corrected K_1'-data bit stream forms intermediate source data which is processed using a Golay (23,12) algorithm unit 127. The controller 123 interrogates the Golay (23,12) algorithm unit 127 and determines the associated k value of twelve and p value of eleven.

The K_1'-data bit stream is input to a data splitter 125 together with a control signal from the controller 123 indicating a k value of twelve and a p value of eleven. The data splitter 125 partitions the K_1'-data into a sequence of thirty five blocks of twenty-three bits, sequentially outputs the first twelve bits of each block as a K_2'-data bit stream, and sequentially outputs the remaining eleven bits of each block as a R_2'-data bit stream. The R_2'-data bit stream is input to a second error correction data generator 69b, together with the second set of transform data 111 stored in the process data 105 during enrolment. The second error correction data generator 69b applies a bitwise exclusive-OR operation to the R_2'-data bit stream and the second set

of transform data 111 to form an EC_2'-data bit stream, which is input to a second error corrector 67b together with the K_2'-data bit stream.

The second error corrector 67b is functionally identical to the first error corrector 67a, and receives a control signal from the controller 123 indicating a k value of twelve and a p value of eleven. Accordingly, the second error corrector 67b partitions the K_2'-data into blocks of twelve bits and the EC_2'-data into blocks of eleven bits, and combines each block of K_2'-data with a corresponding block of EC_2'-data to form a codeword. The second error corrector 67b then sequentially transmits the codewords to the Golay (23,12) algorithm unit 127, which applies the Golay (23,12) error correction algorithm on each received codeword to generate a corrected codeword which is transmitted back to the error corrector 67b. As each corrected codeword is received, the second error corrector 67b extracts the data bits and outputs the extracted data bits to form the biometric number K_{bio}.

As described above, in the second embodiment a second pass of error correction is applied to improve the repeatability of the biometric number K_{bio}, at the expense of reducing the number of bits of the biometric number K_{bio} because a larger proportion of the original S-data is effectively used to provide transform data for encoding the error correction data.

THIRD EMBODIMENT

OVERVIEW

In the first and second embodiments, an iris code is formed by the data formatter 5 having four thousand and

ninety-two data elements, with each data element comprising a single bit. An alternative type data formatter is described in International Patent Application WO 02/098053, the whole content of which is incorporated herein by reference. In particular, WO 02/098053 describes a feature template generator which extracts plural features from an image of an iris, with each feature having one or more attributes, and an attribute value stabiliser which uses data stored during enrolment to stabilise the respective values of the attributes. The resultant feature template is a forty-five by eighteen array of data elements, with each data element having a multi-bit value.

A third embodiment will now be described, with reference to Figures 10 to 12, in which the image data of the eye of an individual is configured by a data formatter as described in WO 02/098053 to produce a forty-five by eighteen array of data elements, with each data element having a multi-bit value. In figures 10 to 12, components which are identical to corresponding components of the first embodiment have been referenced by the same reference numerals and will not be described in detail again.

A consequence of the multi-bit nature of the data elements is that there is a greater likelihood of an error in the lower significant bits than the higher significant bits. Therefore, in this embodiment the lower significant bits and the higher significant bits are processed using different error correction algorithms with the aim of reducing the amount of error correction data required to achieve a desired level of repeatability.

ENROLMENT MODE

Figure 10 schematically illustrates the main components of a number generator 141 which in this embodiment processes the data array produced by the data formatter to generate a biometric number K_{bio} and process data 143 for use in a subsequent number regeneration operation.

The data from the data formatter is input to a data element splitter 145, which for each data element directs the least significant bit of the associated value to a LSB data array 147 and directs the next least significant bit of the associated value to a HSB data array 149. In this embodiment, any bits of the value of a data element above the second least significant bit are discarded. Both of the LSB data array 147 and the HSB data array 149 are therefore in the format of a forty-five by eighteen array of data elements with each data element comprising a single data bit.

In this embodiment, error correction data for the LSB data array 147 and the HSB data array 149 are processed separately using different error correction algorithms. In particular, the LSB data array 147 is processed using the repetition/voting error correction algorithm, and the HSB data array is processed using the Golay (23,12) error correction algorithm. As shown, a first switch 151a is positioned with the LSB data array 147 and the HSB data array 149 on one side of the first switch 151a, and a source data splitter 21 which is identical to the source data splitter of the first embodiment on the other side of the first switch 151a. Further, a second switch 151b is positioned with an error correction data generator 29 on one side of the second switch 151b, and a repetition/voting error correction algorithm unit 25 and a Golay (23,12) error correction algorithm unit 109 on

the other side of the second switch 151b,.

Firstly, a controller 153 outputs control signals to set the first switch 151a so that the LSB data array 147 is connected to the source data splitter 21, and to set the second switch 151b so that the error correction data generator 29 is connected to the repetition/voting error correction algorithm unit 25. The controller 153 also extracts the k value of one and the p value of four from the repetition/voting algorithm unit 25, and sends corresponding control signals to the source data splitter 21 and the error correction data generator 29.

In the same manner as the first embodiment, the source data splitter 21 separates the eight hundred and ten data bits from the LSB-data array 147 into one hundred and sixty-two K_L-data bits and six hundred and forty-eight R_L-data bits in accordance with a generated LSB reference map, and stores LSB reference map data 155a as part of the process data 143. The K_L-data bit stream is output to form part of the biometric number K_{bio}, and is also input to the error correction data generator 29 which generates an EC_L-data bit stream using the repetition/voting algorithm unit 25 as described in the first embodiment. The EC_L-data bit stream is input, together with the R_L-data bit stream, to a transform data generator 31 which performs a bitwise exclusive-OR operation to generate six hundred and forty eight bits of LSB transform data 157a which are stored as part of the process data 147.

After the LSB data array 147 has been processed, the controller 153 switches the first switch 151a and the second switch 151b so that the HSB data array 149 is connected to the source data splitter 21 and the error

correction data generator 29 is connected to the Golay (23,12) algorithm unit 109. The controller 153 also extracts the k value of twelve and the p value of eleven from the Golay (23,12) algorithm unit, and sends corresponding control signals to the source data splitter 21 and the error correction data generator 29.

The source data splitter 21 separates the eight hundred and ten data bits from the HSB-data array 149 into four hundred and twenty K_H-data bits and three hundred and eighty-five R_H-data bits (the remaining five data bits being discarded) according to a generated HSB reference map, and stores HSB reference map data 155b as part of the process data 143. The K_H-data bit stream is output to form the remainder of the biometric number K_{bio}, and is also input to the error correction data generator 29, which generates an EC_H-data bit stream using the Golay (23,12) algorithm unit 109. The error correction data generator 29 outputs an EC_H-data bit stream which is input, together with the R_H-data bit stream, to the transform data generator 31, which performs a bitwise exclusive-OR operation to generate three hundred and eighty-five bits of HSB transform data 157b which are stored as part of the process data 143.

As described above, due to the lower likelihood of errors arising in the HSB data array 149 than in the LSB data array 147 during a subsequent number regeneration, the proportion of the data bits of the HSB data array 149 used to generate transform data is less than for the LSB data array 147.

REGENERATION MODE

Figure 11 schematically shows the main components of a number regenerator 161 which is used to regenerate the

biometric number K_{bio}, using the process data 143 generated during enrolment, from a data array produced by the data formatter from a scan of the eye of the individual.

In the same way as during enrolment, the data from the data formatter is input to a data element separator 145, which directs the lowest significant bit of each data element to a LSB data array 147, directs the next lowest significant bit to a HSB data array 149, and discards any remaining bits. As shown, a first switch 163a is positioned with the LSB data array 147 and the HSB data array 149 on one side, and a source data splitter 61 (which is identical to the source data splitter of the number regenerator of the first embodiment) on the other side. Further, a second switch 163b is positioned with an error corrector 165 on one side, and a repetition/voting error correction algorithm unit 65 and a Golay (23,12) error correction algorithm unit 127 on the other side.

Firstly, a controller 167 outputs control signals to set the first switch 163a so that the LSB data array 147 is connected to the source data splitter 21, and to set the second switch 163b so that the error corrector 29 is connected to the repetition/voting error correction algorithm unit 25. The controller 153 also extracts a k value of one and the p value of four from the repetition/voting algorithm unit 25, and sends corresponding control signals to the source data splitter 21 and the error corrector 165.

The source data splitter 61 separates the eight hundred and ten data bits from the LSB-data array 147 into one hundred and sixty-two K_L'-data bits and six hundred and

forty-eight R_L'-data bits in accordance with the LSB reference map data 155a stored in the process data 143. The K_L'-data bit stream and the R_1'-data bit stream are input to the error corrector 165 and an error correction data generator 69 respectively. The error correction data generator 69 applies a bitwise exclusive-OR operation to the R_L'-data bit stream and the LSB transform data 157a from the process data 143 generated during enrolment to generate an EC_L'-data bit stream which is input to the error corrector 165.

The error corrector 165 forms a sequence of codewords using the K_L'-data bit stream and the EC_L'-data bit stream and outputs corresponding codewords to the repetition/voting algorithm unit 65. When processing the LSB data array 147, each codeword is formed by one bit from the K_L'-data bit stream followed by four bits from the EC_L'-data bit stream. For each received codeword, the repetition/voting algorithm unit 65 generates and outputs a corrected codeword. The error corrector 165 sequentially receives the corrected codewords, removes the check bits, and outputs the remaining data bits to form part of the biometric number K_{bio}. As will be described in more detail hereafter, the error corrector 165 also compares each original codeword output to the repetition/voting algorithm unit 65 with the returned corrected codeword, and identifies which data bits have been changed. This information is subsequently used in the processing of the HSB data array 149.

After all the data bits of the LSB data array 147 have been processed, the controller 167 outputs control signals setting the first switch 163a to connect the HSB data array 149 and the source data splitter 21 and the second switch 163b to connect the error corrector 165 and

the Golay (23,12) algorithm unit 127. The controller 163 also interrogates the Golay (23,12) algorithm unit 127 to recover the k value of eleven and the p value of twelve, and sends corresponding control signals to the source data splitter 61 and the error corrector 165.

The source data splitter 61 separates the eight hundred and ten data bits from the HSB-data array 147 into four hundred and twenty K_H'-data bits and three hundred and eighty-five R_H'-data bits in accordance with the HSB reference map data 155b stored in the process data 143. The K_H'-data bit stream and the R_H'-data bit stream are input to the error corrector 165 and the error correction data generator 69 respectively. The error correction data generator 69 applies a bitwise exclusive-OR operation to the R_H'-data bit stream and the HSB transform data 157b from the process data 143 generated during enrolment to generate an EC_H'-data bit stream which is input to the error corrector 165.

The error corrector 165 forms a sequence of codewords using the K_H'-data bit stream and the EC_H'-data bit stream and outputs corresponding codewords to the Golay (23,12) algorithm unit 127. When processing the HSB data array 149, each codeword is formed by twelve bits from the K_H'-data bit stream followed by eleven bits from the EC_H'-data bit stream. For each received codeword, the Golay (23,12) algorithm unit 127 generates and outputs a corrected codeword. The error corrector 165 receives the corrected codewords, and uses the corrected codewords to form the remaining bits of the biometric number K_{bio}.

The operation of the error corrector 165 will now be described in more detail with reference to Figure 12. In this embodiment, the error corrector 165 includes a

suspect data elements identifier 171 which during the processing of the LSB data array 147 identifies the data bits whose values are corrected by the repetition/voting algorithm unit 25. If the lowest significant bit of a data element is incorrect, then there is a higher likelihood that the next lowest significant bit of that data element is also incorrect. The knowledge of the position of these suspect data elements is used during the processing of the HSB data array 149. This allows a reduced amount of error correction data to be generated and stored during enrolment, and consequently allows the biometric number K_{bio} to have an increased number of bits.

During processing of the LSB data array 147, the K_L'-data bit stream is input to a data bits block generator 173 which, in accordance with a control signal from the controller 167 indicating a k value of one, outputs the K_L'-data in blocks of one data bit to a codeword generator 85. The EC_L'-data is input to a check bits block generator 175 which, in accordance with a control signal from the controller 167 indicating a p value of four, outputs the R_L'-data to the codeword generator 85 in blocks of four check bits. The codeword generator 85 forms a codeword by concatenating each data bit with the corresponding block of four check bits, and outputs the generated codeword to a codeword transmitter 87 and to the suspect data elements identifier 171. The codeword transmitter 87 outputs each generated codeword to the repetition/voting algorithm unit 65, and a corrected codeword receiver 89 receives a returned corrected codeword. Each received corrected codeword is input to the suspect data elements identifier 171 and to a codeword selector 177, which during processing of the LSB data array 147 simply transmits each corrected codeword to a data bits pass filter 91 which removes the check

bits and outputs the remaining data bits to form part of the biometric number K_{bio}.

During processing of the LSB data array 147, each codeword is compared to the corresponding corrected codeword by the suspect data elements identifier 171 to identify which bits have been corrected. For each corrected bit identified, the suspect data elements identifier 171 identifies the corresponding data element of the LSB data array 147 using the LSB reference map data 155a, then identifies the location of the bit of the K_H'-data or EC_H'-data which corresponds to the identified data element using the HSB reference map data 155b, and then tags that data bit location as a suspect data bit.

During processing of the HSB data array 149, the K_H'-data bit stream is input to a data bits block generator 173 which, in accordance with a control signal from the controller 167 indicating a k value of twelve, partitions the K_H'-data into blocks of twelve data bits. Similarly, the EC_H'-data bit stream is input to a check bits block generator 175 which, in accordance with a control signal from the controller 167 indicating a p value of eleven, partitions the EC_H'-data into blocks of eleven bits.

For each block of K_H'-data and corresponding block of EC_H'-data, the suspect data elements identifier 171 determines the total number S of suspect bits. The suspect data elements identifier 171 then controls the data bits block generator 173 and the check bits block generator 175 to output data bit blocks and check bit blocks so that the codeword generator 85 outputs test codewords with every possible combination of values of the suspect bits, so that the codeword generator 85 generates 2^S different test codewords. The generated

test codewords are input to the codeword transmitter 87, and the 2^s corrected test codewords received from the Golay (23,12) algorithm unit 109 are input to the codeword selector 177, which compares the 2^s corrected codewords and outputs the codeword which appears most frequently to the data bits pass filter 91 which removes the check bits and outputs the remaining data bits to form part of the biometric number K_{bio}.

For example, if a data bits block and a check bits block contain between them three suspect bits, then eight (i.e. 2^s) test codewords are generated, with the values of the suspect bits in the eight test codewords being assigned the values 0-0-0, 0-0-1, 0-1-0, 0-1-1, 1-0-0, 1-0-1, 1-1-0 and 1-1-1 respectively. The Golay (23,12) algorithm is able to correct three incorrect data bits and therefore, if the only differences between the test codewords and the corresponding original codeword generated during enrolment are in the suspect data bits, the Golay (23,12) algorithm unit 109 corrects all the differences and returns eight identical corrected code words. If, however, in the eight test codewords one of the bits other than the suspect bits is different from the corresponding bit of the corresponding original codeword, then four of the corrected codewords are identical, corresponding to the four of the test codewords in which two or three of the suspect bits have been assigned the correct value, with the remaining four corrected codewords generally having differing values. The codeword selector 177 then identifies the value of the four identical codewords, and outputs the identified value.

It will be noted that in the above example, although the Golay (23,12) algorithm is only able to correct three

errors, potentially four errors were corrected (i.e. if all the received suspect data bits were incorrect). This is possible because of the processing of the LSB data array 147 provides additional information concerning the locations of possible errors.

MODIFICATIONS AND FURTHER EMBODIMENTS

In the third embodiment, during number regeneration the suspect data elements identifier generates a fault map identifying data elements of the source data which contain errors in the lowest significant bit. This fault map is used in the third embodiment during the processing of higher significant bits of the suspect data elements in order to allow a reduced amount of error correction data to be used. Such a fault map could be used in a number of other ways to improve the reliability of number regeneration.

If the fault map indicates a cluster of errors associated with a common portion of the iris, then this may indicate that the recorded image of that portion of the iris is unsound, for example due to reflected light or by being obscured by eyelids or eyelashes. In an alternative embodiment, if the fault map does indicate such a cluster of errors, then the suspect data elements identifier tags all the data elements associated with the corresponding portion of the iris, even those whose values were not corrected, suspect. The number regenerator then re-processes the lowest significant bit data, and in the same manner as the third embodiment process the suspect data bits by creating multiple test codewords containing all possible combinations of values of the suspect bits, applying the error correction algorithm to all the test codewords, and selecting from the resulting corrected

codewords the value which appears most frequently. In this way, the amount of error correction data needed to process the LSB data is reduced. It will be appreciated that such an arrangement may be applied to systems in which the data formatter configures the image data into data elements each having a single data bit, as in the first and second embodiments.

In another alternative embodiment, if the fault map indicates a cluster of errors corresponding to a common portion of the iris, then the number regenerator outputs a signal requesting that the eye is imaged again to generate new S-data. Preferably, the eye is imaged to provide replacement image data for just the suspect image portions, as the other image portions have already been judged sound.

The faults identified in the fault map could arise from a number of sources. As described above, the faults could be caused by a region of the iris being obscured during an image capture. Alternatively the faults could be caused by random measurement error. In both of these cases, the location of the faults on the fault map should vary in a random manner. Another source for the faults in the fault map is systemic error, and such faults are characterised by appearing in the same place within the fault map with high regularity.

In an embodiment, fault maps for a plurality of number regeneration operations are stored and compared to identify regularly occurring faults indicating systemic error. Preferably the fault maps are stored in an encrypted format. Further, in a preferred embodiment the biometric number K_{bio} is used as the cryptographic key of a symmetric encryption algorithm which is used to encrypt

the fault maps.

If stored fault maps do indicate systemic error, then this information can be exploited in a number of ways to improve performance of the number generation system. In one embodiment, data elements within the source data which are affected by systemic error are identified from the fault maps, and are labelled as suspect. The processing of the suspect data elements is then performed as described above. In an alternative embodiment, additional transform data is used to transform the data elements exhibiting systemic error back to their enrolment values. In another alternative embodiment, if the stored fault maps indicate systemic error, then a new enrolment process is performed.

In the third embodiment, the S-data comprises a plurality of data elements with each data element having a multi-bit value. The lowest significant bits of the data elements are initially processed, and suspect data elements identified. In this way, the error correction of the higher significant bit can be made more efficient. It will be appreciated that the same technique can be applied to data which is not in binary format. It will also be appreciated that instead of processing only the least significant bit and the secondly significant bit of each data element, alternatively, other combinations of significant bits of the data element could be processed. For example, if each data element has a four bit value, of which the least significant bit is found to vary randomly between captures of source data, then the least significant can be discarded and the biometric number generated using the second and third least significant bits.

It will be appreciated that more than two bits of a multi-bit data element can be processed to generate the repeatable number. In general, the lowest significant bits are first processed and a first fault map generated, the second least significant bits are then processed using the first fault map and a second fault map generated indicating errors in the second significant bits, the third significant bits are then processed using the second fault map and a third fault map generated indicating errors in the third significant bit, and so on to the most significant bit which is processed.

In the second embodiment, the first pass of error correction is performed using a repetition/voting algorithm. This is generally preferred because the repetition/voting algorithm allows correction of a comparatively large number of errors, albeit at the expense of requiring a large amount of error correction data. A feature of the repetition/voting algorithm used is that each codeword includes a single data bit. This allows the K_1-data from the first pass of error correction to be separated into K_2-data and R_2-data without any data shuffling, because typically any errors in the K_1-data are randomly distributed.

A feature that is common to most error correction algorithms is that if the codeword contains more errors than the algorithm can correct, then the codeword generated by applying the algorithm includes at least as many errors as the original codeword. For example, if four errors are present in a twenty-three bit codeword for the Golay (23,12) algorithm, then the resultant codeword contains more than four errors. Such a concentration of errors is unlikely to be correctable in a second pass of error correction.

In an alternative to the second embodiment, the Golay (23,12) algorithm is used to perform the first pass of error correction, and the BCH (32,21) algorithm is used for the second pass of error correction. In the number generator of this alternative embodiment, the data splitter 107 of the number generator is replaced by a data splitter functionally identical to the source data splitter of the number generator of the first embodiment. The source data splitter shuffles the data bits of the K_1-data bit stream and stores corresponding reference map data. The data splitter of the number regenerator is replaced by a source data splitter which is functionally identical to the source data splitter of the number regenerator of the first embodiment. The source data splitter uses the stored reference map data to shuffle the data bits of the K_1'-data bit stream in the same manner as the data bits of the K_1-data bit stream were shuffled during enrolment. In this way, errors in the K_1-data bit stream are dispersed.

In the second embodiment, the K_1-data effectively forms a first biometric number representative of the iris and the K_2-data forms a second biometric number representative of the iris, with the second biometric number having a higher repeatability but less binary digits. In an alternative embodiment, the K_2-data is split into K_3-data and R_3-data, the K_3-data being used to form a third biometric number representative of the iris and the R_3-data being used to form redundant data for mapping error correction data corresponding to the third biometric number. In this way, three passes of error correction are performed. It will be appreciated that the only limit to the number of error correction passes performed is the amount of the original source data, as with each pass of error correction the resulting

biometric number will have less binary digits.

It will be appreciated that the multiple pass error correction technique of the second embodiment could also be applied to the multi-bit processing of the third embodiment. In particular, the biometric number generated from the LSB-data and/or the HSB-data could be split into new K-data and R-data for another pass of error correction. It will be appreciated that when multiple passes of error correction are performed, the same error correction algorithm could be used for each pass of error correction, or alternatively different error correction algorithms could be used for different passes of error correction.

In the illustrated embodiments, during enrolment a transform data generator applies a bitwise exclusive-OR operation to a stream of error correction data and a stream of redundant data (i.e, the R-data) to generate transform data, and during number regeneration an error correction data generator applies to bitwise exclusive-OR operation to a stream of redundant data (i.e. the R'-data) and the stored transform data to recover the error correction data. Alternative mapping operations could be performed to map between the error correction data and the transform data using redundant data without the transform data providing information on the biometric number K_{bio}. For example, a simple addition operation could be performed on the error correction data and the redundant data during enrolment, and a simple subtraction operation performed on the transform data and the redundant data during number regeneration. Such mapping operations are generically termed binomial mapping operations.

Generally, the redundant data and the error correction data is formed by a random distribution of approximately equal numbers of bits having a value "1" and bits having a value "0", in which case the randomness of the redundant data and error correction data is optimal. In some occasions, however, this may not be the case. For example, if the highest significant bit of a data element having multiple significant bits is processed, then it is possible that the majority of the redundant data will have a value "0". If this coincides with error correction data which predominantly has the value "0", then to improve security of the K-data and R-data the transform data may be generated by storing a series of instructions indicating how bits of redundant data can be inverted and/or re-ordered to form the error correction data. In this way, it is more difficult to extract useful information about the R-data and the error correction data from the transform data.

The multi-bit data element processing techniques described above could also be applied to a number generation system in which error correction data is directly stored (i.e. is not mapped into transform data).

In the illustrated embodiments, a repetition/voting error correction algorithm is applied in which four check bits are assigned to each data bit. It will be appreciated that an alternative number of check bits could be used, although it is preferred that an even number of check bits is used to prevent any ties in the voting operation during number regeneration (i.e. the same number of data bits having value "0" as having value "1").

In the previously described embodiments, the number generators and the number regenerators have been designed

so that the error correction algorithm used can be changed simply by replacing the existing error correction algorithm unit by the error correction algorithm unit for the new error correction algorithm. The controller determines the k value and the p value associated with the new error correction algorithm unit, and outputs control signals ensuring that the data splitters apportion the S-data into K-data and R-data correctly, that the error correction data generator outputs blocks of k data bits to the error correction algorithm unit during enrolment, and that the error corrector outputs codewords having k data bits and p check bits to the error correction algorithm unit during number regeneration.

Examples of other error correction algorithms which could be used include the BCH (32,21) algorithm and the Hamming (8,4) algorithm.

In the illustrated embodiments, when the source data is separated into K-data and R-data, in some embodiments some of the source data is discarded because the amount of source data does not correspond to an integer number of codewords. It will be appreciated that this discarded data could be constructively used. For example, error detection data could be generated for the biometric number K_{bio}, and the discarded source data used to map the error detection data into transform data.

In the illustrated embodiments, during enrolment a source data splitter 61 generates a reference map indicating for the K-data and the R-data, the corresponding elements of the S-data. The reference map is stored and used by a source data splitter in a subsequent number regeneration operation. Alternatively, the source data splitter

during enrolment could perform a predetermined shuffling operation, with the source data splitter being programmed to perform the same shuffling operation during number regeneration. In this way, there is no requirement to store the reference map. However, for embodiments in which a fault map identifying suspect data elements is formed during number regeneration, a reference map can be transiently formed during number regeneration to enable the suspect data elements to be tracked back to the original S-data locations.

In the previously described embodiments, the source data is formed by imaging the iris of a human being. Alternatively, the source data could be formed by measuring other distinctive characteristics of an individual. For example, the source data could be formed by imaging a fingerprint or a retina of the individual. Alternatively, the source data could be formed by recording a sequence of utterances by the individual. Details of techniques for formatting biometric data from fingerprints and retina patterns can be found in International Patent Application WO 02/098053.

The source data (S-data) could be formed from a number of source data pools relating to the same distinctive feature. For example, the S-data could be formed by the combination of formatted data provided by the iris image data processing techniques described in US Patent No. 5,291,560 and WO 02/098053. Alternatively, the S-data could be formed from a number of source data pools representing different distinctive characteristics (e.g. iris pattern and fingerprint) of an individual. As another alternative, if a particular region of a source data pool was found to have a higher susceptibility to errors than the rest of the source data pool, then the

data associated with this region could be separated off to form a separate source data pool.

Generally, each source data pool will have an associated error behaviour. For example, one source data pool may have an expected error rate of one bit in ten while another source data pool may have an expected error rate of one bit in six. In a preferred embodiment, a plurality of source data pools are processed by respective error correction algorithms, which generally will not be the same, to produce respective intermediate source data pools all having a substantially constant error performance. The intermediate source data pools are then combined, and an additional pass of error correction applied to the combined intermediate source data pool.

As described above, a wide variety of error correction algorithms can be used, in one or more passes of error correction, to process analogue data representative of an analogue data source to generate a number representative of the analogue data source. Preferably, the choice of error correction methodology is determined by predicting for a set of analogue data the fault rate for all possible error correction methodologies, and identifying the error correction methodology which provides the largest number with a predicted fault rate within a desired tolerance level. The error correction performance of each error correction methodology may be determined from the likelihood of errors in the source analogue data and the error correcting performance of the various error correction algorithms.

It will be appreciated that biometric data from other animals could be used to generate a biometric number.

Further, some inanimate objects have distinctive features from which a physical value representative of the inanimate object can be derived. For example, analogue data may be generated by imaging an engraving or a jewel with an image sensor. Alternatively, a purpose-defined object having sharply defined, but random, geometric properties can be probed using ultrasound to generate analogue data.

Although in the first to third embodiments, the same apparatus is used both to carry out the enrolment process and the subsequent number regeneration, alternatively the enrolment process and the number regeneration process could be performed by separate devices. However, if the number regeneration is performed by a separate device to the enrolment, then the process data must be transferred from the enrolment apparatus to the number regeneration apparatus. This could be performed, for example, by transferring the process vector to a storage device (e.g. a floppy disc or a CD-ROM) which is moved to the number regeneration apparatus where the process vector is downloaded into the regeneration apparatus, or alternatively the enrolment apparatus and the number regeneration apparatus could be connected via a computer network, in which the process vector is transmitted across the computer network as an electrical signal.

The processing of the analogue data can either be performed by a hardware device, software running on a computer, or the processing could be split between a hardware device and software running on a computer. The invention is well suited to being implemented in software using an object oriented programming language such as Java or C++. In particular, each error correction algorithm can be implemented by a respective different

one of a library of program objects which can be selectively addressed by an error correction data generator and an error corrector.

As described, as well as computer apparatus and processes performed in the computer apparatus, the invention also extends to computer programs, particularly computer programs on or in a carrier, adapted for putting the invention into practice. The computer program may be in the form of source code, object code, a code intermediate source and object code such as in partially compiled form, or in any other form suitable for use in the implementation of the processes according to the invention.

The carrier may be any entity or device capable of carrying the program. For example, the carrier may comprise a storage medium such as a ROM, for example a CD ROM or a semiconductor ROM, or a magnetic recording medium, for example a floppy disk or hard disk. Further, the carrier may be a transmissible carrier such as an electrical or optical signal which may be conveyed via electrical or optical cable or by radio or other means.

When the program is embodied in a signal which may be conveyed directly by a cable or other device or means, the carrier may be constituted by such cable or other device or means. Alternatively, the carrier may be an integrated circuit in which the program is embedded, the integrated circuit being adapted for performing, or for use in the performance of, the relevant processes.

Claims

1. A method of providing process information for a number generation process which is operable to generate a number representative of an analogue data source, the method comprising the steps of:

receiving analogue data representative of the analogue data source;

processing the received analogue data to form a first data set and a second data set;

generating error correction data associated with said first data set;

generating transform data for transforming said second data set into the error correction data; and

storing said transform data.

2. A method according to claim 1, wherein the analogue data source comprises a plurality of data elements, and said analogue data processing step comprises assigning a respective different data element of the analogue data to each data element of the first data set and the second data set.

3. A method according to claim 2, wherein the assigning step comprises the steps of:

generating map data associating each data element of the first data set and the second data set with a respective different data element of the received analogue data; and

assigning the analogue data to the first data set and the second data set in accordance with the generated map data.

4. A method according to any of claims 1 to 3, further comprising the steps of:

processing the first data set to form a third data set and a fourth data set;

generating additional error correction data associated with said third data set;

generating additional transform data for transforming said fourth data set into the additional error correction data; and

storing said additional transform data.

5. A method according to claim 4, wherein the error correction data associated with said first data set is generated using a first error correction algorithm, and the additional error correction data associated with said third data set is generated using a second error correction algorithm which is different from the first error correction algorithm.

6. A method according to any of claims 1 to 3, comprising repeating the generation and storage of transform data plural times, with the first data set of one time forming the analogue data for the next time.

7. A method according to claim 6, wherein at least two of said plural times of generation and storage of transform data use different error correction algorithms.

8. A method according to any of claims 1 to 3, wherein the received analogue data comprises a plurality of data elements, each data element having a multi-digit value,

wherein said processing step comprises extracting from each data element of the analogue data the value of the digit in a first predetermined digit position of the multi-digit value to form a first group of digits, and forming said first data set and said second data set by processing the first group of digits,

and wherein the method further comprises the steps of:

extracting from each data element of the analogue data the value of the digit in a second predetermined digit position of the multi-digit value to form a second group of digits;

processing the second group of digits to form a third data set and a fourth data set;

generating additional error correction data associated with said third data set;

generating additional transform data for transforming said fourth data set into said additional error correction data; and

storing said additional transform data.

9. A method according to claim 8, wherein the error correction data associated with said first data set is generated using a first error correction algorithm, and the additional error correction data associated with said third data set is generated using a second error correction algorithm which is different from the first error correction algorithm.

10. A method according to claim 8 or 9, wherein the first predetermined position is the least significant digit.

11. A method according to any of claims 8 to 10, wherein the second predetermined position is the second least significant digit.

12. A method according to any of claims 8 to 11, wherein each data element is represented by a plurality of binary digits.

13. A method according to any of claims 8 to 12, further comprising the steps of:

predicting a fault rate of the received analogue data; and

selecting an error correction methodology in accordance with the predicted fault rate.

14. A method of generating a number representative of an analogue data source, the method comprising the steps of:

receiving analogue data representative of the analogue data source;

processing the received analogue data to form a first data set and a second data set;

retrieving transform data from a data store;

generating an intermediate number using the first data set;

transforming the second data set into error correction data using the retrieved transform data; and

processing said intermediate number and said error correction data using an error correction algorithm to generate the number representative of the analogue source.

15. A method according to claim 14, wherein said error correction algorithm is a first error correction algorithm, and wherein the method further comprises the steps of:

forming a third data set and a fourth data set using said second number;

retrieving additional transform data from a data store;

generating a third number using the third data set;

transforming the fourth data set into additional error correction data using the retrieved additional

transform data; and

processing said number and said error correction data using a second error correction algorithm to generate a fourth number.

16. A method according to claim 15, wherein the second error correction algorithm is different from the first error correction algorithm.

17. A method according to claim 14, comprising generating plural numbers representative of the analogue data source by using each generated number as the analogue data from which another representative number is generated, and in each number generation operation retrieving associated transform data.

18. A method according to claim 17, wherein at least two of the representative numbers are generated using different error correction algorithms.

19. A method according to claim 14, wherein the received analogue data comprises a plurality of data elements, each data element having a value represented by a plurality of digits,

wherein said intermediate number is a first intermediate number;

wherein said analogue data processing step comprises the steps of:

processing the received analogue data to form a plurality of groups of digits, each group of digits being formed by extracting from each data element of the analogue data the value of the digit in a respective different digit position of the multi-digit value; and

processing a first group of digits to form the first data set and the second data set,

wherein the method further comprises the steps of:

processing a second group of digits, different from the first group of digits, to form a third data set and a fourth data set;

generating a second intermediate number using the third data set;

retrieving additional transform data from the data store; and

transforming said fourth data set into additional error correction data using the retrieved additional transform data,

and wherein said intermediate number processing step comprises processing the first intermediate number and the associated error correction data using a first error correction algorithm and processing the second intermediate number and the associated additional error correction data using a second error correction algorithm to generate the number representative of the analogue source.

20. A method according to claim 19, wherein the first predetermined position is one place less significant than the second predetermined position.

21. A method according to any of claims 14 to 20, further comprising the step of identifying the data elements of the analogue data which contain errors as suspect data elements.

22. A method according to claim 21, further comprising the steps of:

assigning all possible combinations of values to one or more digits of the suspect data elements;

for each combination of values, i) determining the resultant intermediate number and associated error

correction data, and ii) applying the error correction algorithm to the resultant intermediate number to generate a corrected number; and

using the most common value of the corrected number to generate the number representative of the analogue source.

23. A method according to claim 21 or 22, further comprising storing data identifying the suspect data elements in order to track errors in the analogue data.

24. A method of generating a number representative of an analogue data source together with error correction data for said number, the method comprising the steps of:

receiving analogue data representative of the analogue data source, said analogue data comprising a plurality of data elements each having a multi-digit value;

processing the received analogue data to form a plurality of groups of digits, each group of digits being formed by extracting from each data element of the analogue data the value of the digit in a respective different digit position of the multi-digit value;

forming a plurality of intermediate numbers, each intermediate number being formed by processing one or more of the groups of digits;

for each of the intermediate numbers, applying a respective error correction algorithm to form associated error correction data; and

generating said number representative of the analogue source by combining the plurality of intermediate numbers.

25. A method according to claim 24, wherein for at least two of the intermediate numbers, respective different

error correction algorithms are applied to generate the corresponding error correction data.

26. A method of generating a number representative of an analogue data source, the method comprising the steps of:

receiving analogue data representative of the analogue data source, said analogue data comprising a plurality of data elements each having a multi-digit value;

processing the received analogue data to form a plurality of groups of digits, each group of digits being formed by extracting from each data element of the analogue data the value of the digit in a respective different digit position of the multi-digit value;

forming a plurality of intermediate numbers, each intermediate number being formed by processing one or more of the groups of digits;

for each intermediate number, recovering corresponding error correction data, and applying an error correction algorithm to the intermediate number and the corresponding error correction data to form a corrected intermediate number; and

combining said corrected intermediate numbers to form the number representative of the analogue source.

27. A method according to claim 26, wherein for at least two of the intermediate numbers, respective different error correction algorithms are applied to the intermediate number an the corresponding error correction data to form corrected intermediate numbers.

28. A method according to any of claims 24 to 27, wherein each data element of the analogue data is represented by a plurality of binary digits.

29. A storage device storing instructions including instructions for causing a programmable apparatus to perform a method according to any preceding claim.

30. A signal conveying instructions including instructions for causing a programmable apparatus to perform a method according to any of claims 1 to 28.

31. An apparatus for providing process information for a number generation process which is operable to generate a number representative of an analogue data source, the apparatus comprising:

a receiver operable to receive analogue data representative of the analogue data source;

a processor operable to process the received analogue data to form a first data set and a second data set;

an error correction data generator operable to generate error correction data associated with said first data set;

a transform data generator operable to generate transform data for transforming said second data set into the error correction data; and

an outputter operable to output the transform data to a storage device

32. An apparatus according to claim 31, wherein the analogue data source comprises a plurality of data elements, and said processor is arranged to assign a respective different data element of the analogue data to each data element of the first data set and the second data set.

33. An apparatus according to claim 32, wherein the processor is arranged to i) generate map data associating

each data element of the first data set and the second data set with a respective different data element of the received analogue data, and ii) assign the analogue data to the first data set and the second data set in accordance with the generated map data.

34. An apparatus according to any of claims 31 to 33, further comprising:

means for processing the first data set to form a third data set and a fourth data set;

means for generating additional error correction data associated with said third data set;

means for generating additional transform data for transforming said fourth data set into the additional error correction data; and

means for storing said additional transform data.

35. An apparatus according to claim 34, wherein the error correction data associated with said first data set is generated using a first error correction algorithm, and the additional error correction data associated with said third data set is generated using a second error correction algorithm which is different from the first error correction algorithm.

36. An apparatus according to any of claims 31 to 33, comprising means for repeating the generation and storage of transform data plural times, with the first data set of one time forming the analogue data for the next time.

37. An apparatus according to claim 36, wherein said repeating means is operable to use different error correction algorithms for at least two of said plural times of generation and storage of transform data .

38. An apparatus according to any of claims 31 to 33, wherein the received analogue data comprises a plurality of data elements, each data element having a multi-digit value,

wherein said apparatus further comprises a data element slitter operable i) to extract from each data element of the analogue data the value of the digit in a first predetermined digit position of the multi-digit value to form a first group of digits, and ii) to extract from each data element of the analogue data the value of the digit in a second predetermined digit position of the multi-digit value to form a second group of digits, wherein said processor is operable to form said first data set and said second data set by processing the first group of digits,

and wherein the apparatus further comprises:

means for processing the second group of digits to form a third data set and a fourth data set;

means for generating additional error correction data associated with said third data set;

means for generating additional transform data for transforming said fourth data set into said additional error correction data; and

means for storing said additional transform data.

39. An apparatus according to claim 38, wherein the error correction data associated with said first data set is generated using a first error correction algorithm, and the additional error correction data associated with said third data set is generated using a second error correction algorithm which is different from the first error correction algorithm.

40. An apparatus according to claim 38 or 39, wherein the first predetermined position is the least significant

digit.

41. An apparatus according to any of claims 38 to 40, wherein the second predetermined position is the second least significant digit.

42. An apparatus according to any of claims 38 to 41, wherein each data element is represented by a plurality of binary digits.

43. An apparatus according to any of claims 38 to 42, further:

means for predicting a fault rate of the received analogue data; and

means for selecting an error correction methodology in accordance with the predicted fault rate.

44. An apparatus for of generating a number representative of an analogue data source, the apparatus comprising:

a receiver operable to receive analogue data representative of the analogue data source;

a processor operable to process the received analogue data to form a first data set and a second data set;

a data retriever operable to retrieve transform data from a data store;

a number generator operable to generate an intermediate number using the first data set;

a data transformer operable to transform the second data set into error correction data using the retrieved transform data; and

an error corrector operable to process said intermediate number and said error correction data using an error correction algorithm to generate the number

representative of the analogue source.

45. An apparatus according to claim 44 further comprising the means for forming a third data set and a fourth data set using said second number,

wherein said data retriever is operable to retrieve additional transform data from a data store

wherein said number generator is operable to generate a third number using the third data set,

wherein said data transformer is operable to transform the fourth data set into additional error correction data using the retrieved additional transform data, and

wherein said error corrector is operable to process said number and said error correction data using a second error correction algorithm to generate a fourth number.

46. An apparatus according to claim 45, wherein said error corrector comprises a selector operable to select one of a plurality of error correction algorithms.

47. An apparatus according to claim 44 wherein the data processor is operable to receive a generated number as a new set of analogue data in order to generate another representative number.

48. An apparatus according to claim 47, wherein at least two of the representative numbers are generated using different error correction algorithms.

49. An apparatus according to claim 44, wherein the received analogue data comprises a plurality of data elements, each data element having a value represented by a plurality of digits,

wherein said intermediate number is a first

intermediate number;

wherein said data processor comprises:

a data element splitter operable to process the received analogue data to form a plurality of groups of digits, each group of digits being formed by extracting from each data element of the analogue data the value of the digit in a respective different digit position of the multi-digit value,

wherein the data processor is operable to process a first group of digits to form the first data set and the second data set, and to process a second group of digits, different from the first group of digits, to form a third data set and a fourth data set,

wherein the number generator is operable to generate a second intermediate number using the third data set,

wherein the data retriever is operable to retrieve additional transform data from the data store,

wherein said data transformer is operable to transform said fourth data set into additional error correction data using the retrieved additional transform data, and

wherein said error corrector is operable to process the first intermediate number and the associated error correction data using a first error correction algorithm, and to process the second intermediate number and the associated additional error correction data using a second error correction algorithm to generate the number representative of the analogue source.

50. An apparatus according to claim 49, wherein the first predetermined position is one place less significant than the second predetermined position.

51. An apparatus according to any of claims 44 to 50, further comprising a suspect data element ientifier

operable to identify the data elements of the analogue data which contain errors as suspect data elements.

52. An apparatus according to claim 51, further comprising:

means for assigning all possible combinations of values to one or more digits of the suspect data elements;

wherein the error corrector is operable, for each combination of values, i) to determine the resultant intermediate number and associated error correction data, and ii) to apply the error correction algorithm to the resultant intermediate number to generate a corrected number, and iii) to select the most common value of the corrected number for generating the number representative of the analogue source.

53. An apparatus according to claim 51 or 52, further comprising a data store operable to store data identifying the suspect data elements in order to track errors in the analogue data.

54. An apparatus for generating a number representative of an analogue data source together with error correction data for said number, the apparatus comprising:

means for receiving analogue data representative of the analogue data source, said analogue data comprising a plurality of data elements each having a multi-digit value;

means for processing the received analogue data to form a plurality of groups of digits, each group of digits being formed by extracting from each data element of the analogue data the value of the digit in a respective different digit position of the multi-digit value;

means for forming a plurality of intermediate numbers, each intermediate number being formed by processing one or more of the groups of digits;

means for applying, for each of the intermediate numbers, a respective error correction algorithm to form associated error correction data; and

means for generating said number representative of the analogue source by combining the plurality of intermediate numbers.

55. An apparatus according to claim 54, wherein for at least two of the intermediate numbers, said applying means is operable to apply respective different error correction algorithms to generate the corresponding error correction data.

56. An apparatus for of generating a number representative of an analogue data source, the method comprising the steps of:

means for receiving analogue data representative of the analogue data source, said analogue data comprising a plurality of data elements each having a multi-digit value;

means for processing the received analogue data to form a plurality of groups of digits, each group of digits being formed by extracting from each data element of the analogue data the value of the digit in a respective different digit position of the multi-digit value;

means for forming a plurality of intermediate numbers, each intermediate number being formed by processing one or more of the groups of digits;

means for recovering, for each intermediate number, recovering corresponding error correction data;

means for correcting each intermediate number using

the corresponding error correction data and an error correction algorithm to form a corrected intermediate number; and

means for combining said corrected intermediate numbers to form the number representative of the analogue source.

57. An apparatus according to claim 56, wherein said correcting means is operable to apply respective different error correction algorithms for at least two of the intermediate numbers.

58. An apparatus according to any of claims 54 to 57, wherein each data element of the analogue data is represented by a plurality of binary digits.

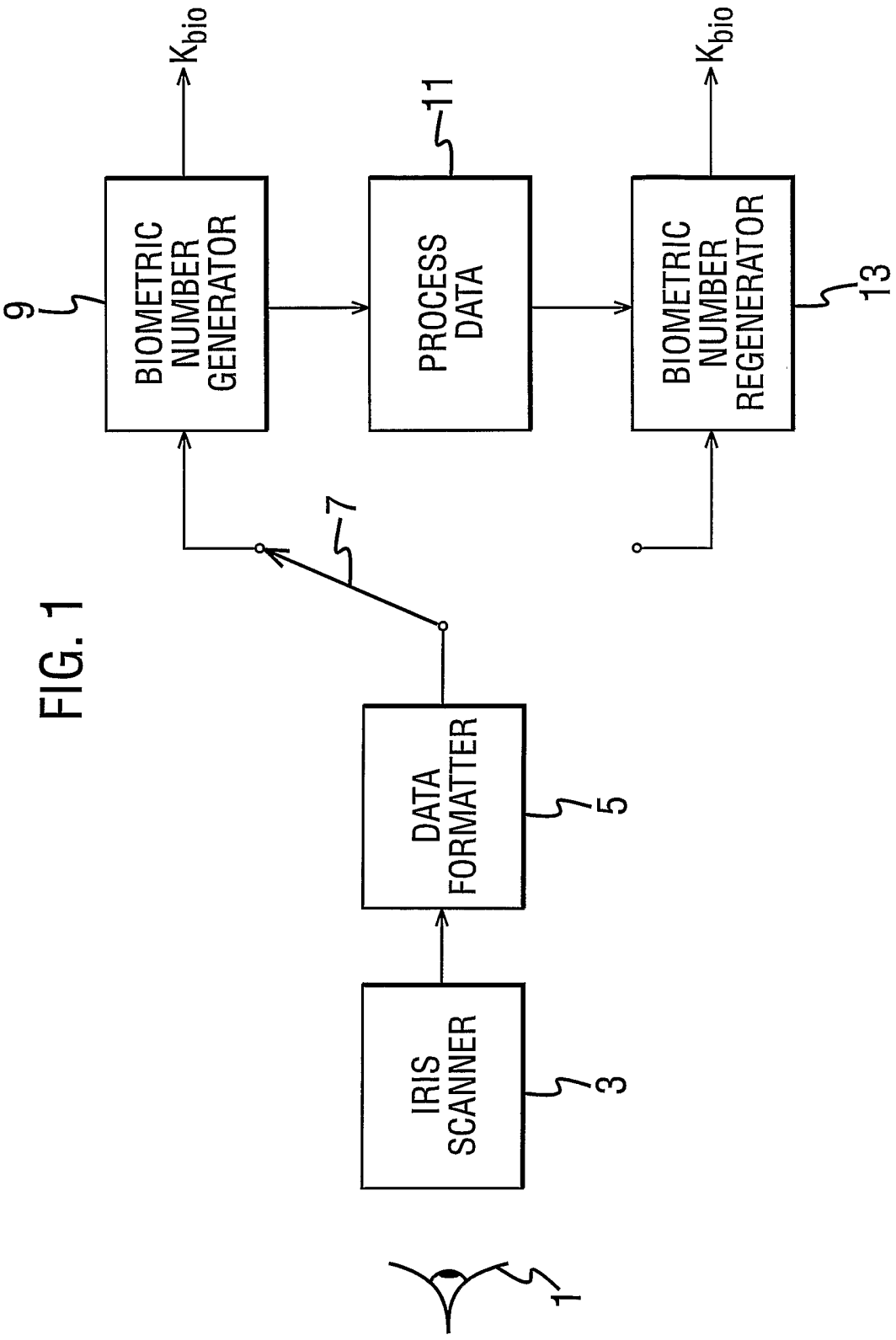

K_{bio}
11
K_{bio}
BIOMETRIC NUMBER GENERATOR
PROCESS DATA
BIOMETRIC NUMBER REGENERATOR
9
13
7
DATA FORMATTER
5
IRIS SCANNER
3
1

FIG. 1

FIG. 2

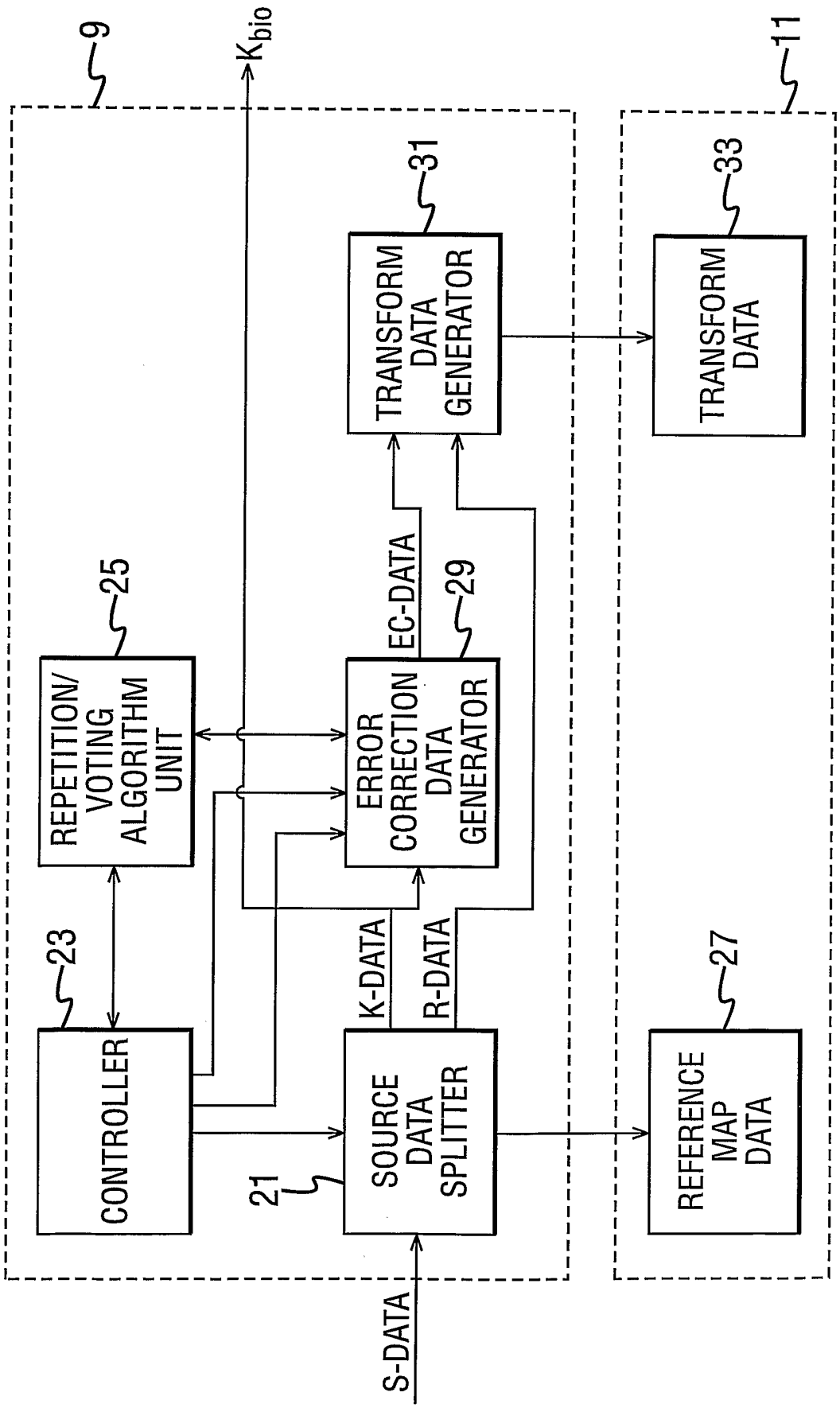

9
K_{bio}
11
31
33
TRANSFORM DATA GENERATOR
TRANSFORM DATA
25
EC-DATA
29
REPETITION/ VOTING ALGORITHM UNIT
ERROR CORRECTION DATA GENERATOR
23
K-DATA
R-DATA
27
CONTROLLER
SOURCE DATA SPLITTER
REFERENCE MAP DATA
21
S-DATA

FIG. 3

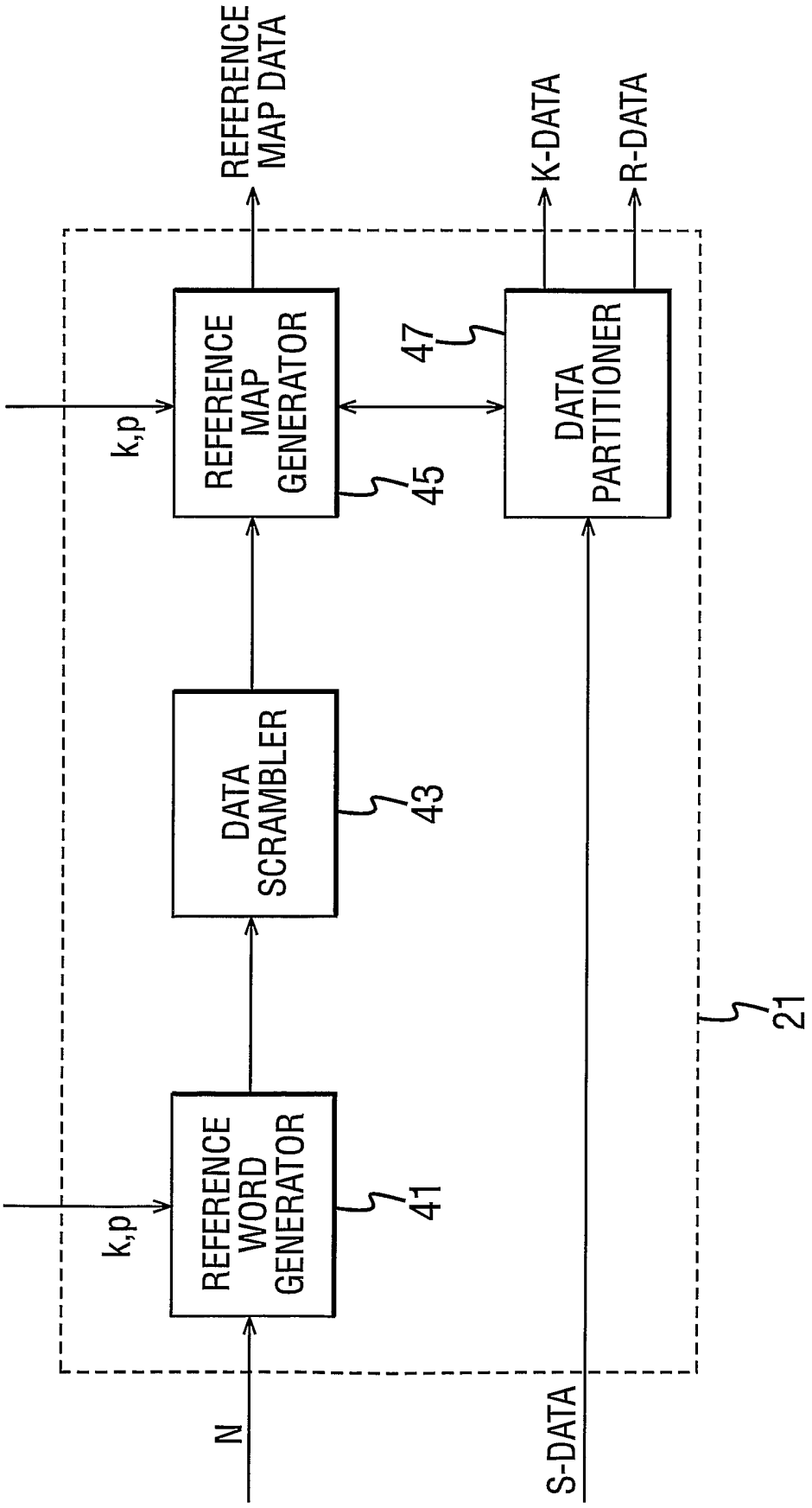

REFERENCE MAP DATA
K-DATA
R-DATA
REFERENCE MAP GENERATOR
DATA PARTITIONER
47
k,p
45
DATA SCRAMBLER
43
REFERENCE WORD GENERATOR
41
k,p
21
N
S-DATA

FIG. 4

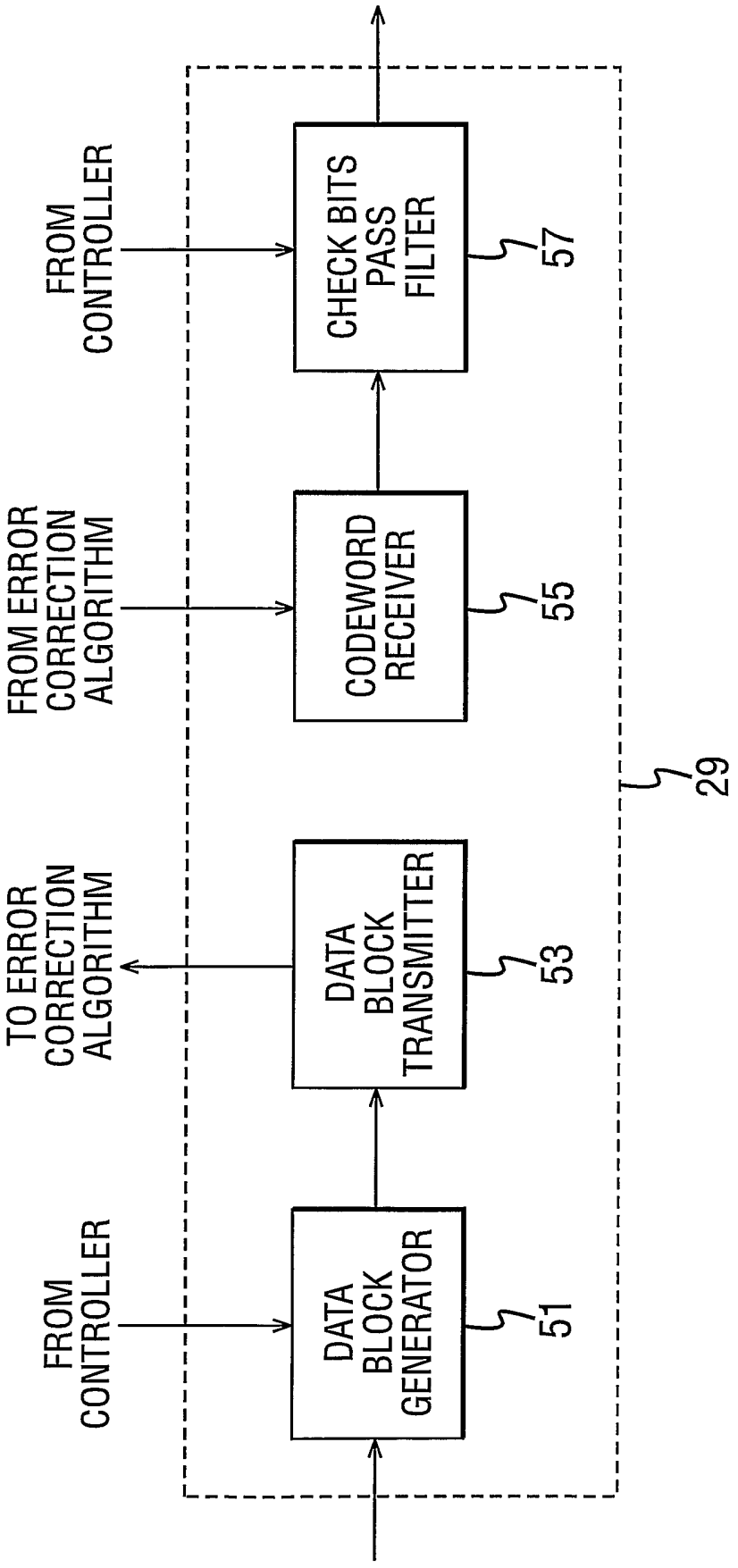

FROM CONTROLLER
DATA BLOCK GENERATOR
51
TO ERROR CORRECTION ALGORITHM
DATA BLOCK TRANSMITTER
53
FROM ERROR CORRECTION ALGORITHM
CODEWORD RECEIVER
55
FROM CONTROLLER
CHECK BITS PASS FILTER
57
29

FIG. 5

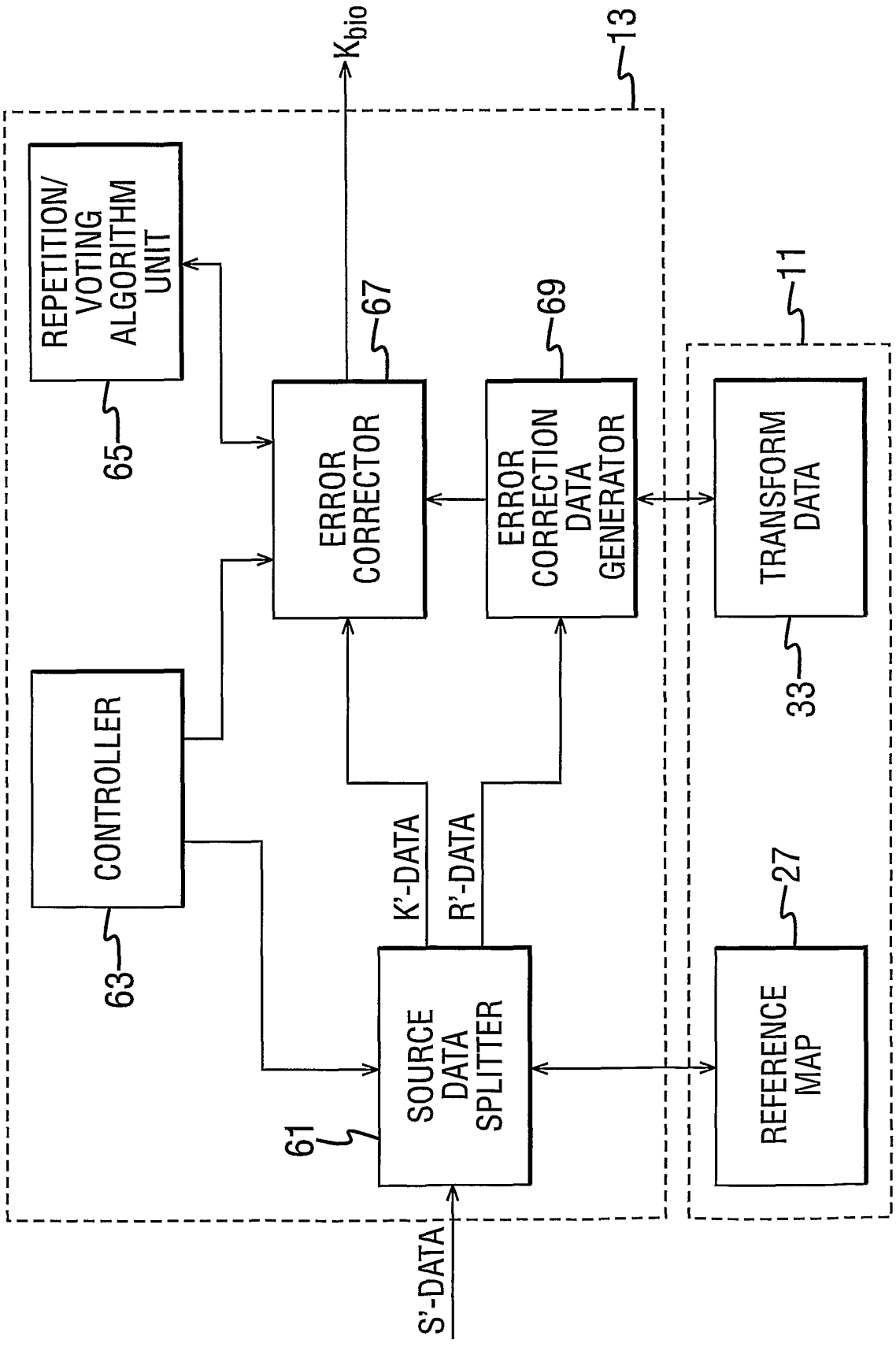

K_{bio}
13
REPETITION/ VOTING ALGORITHM UNIT
65
67
69
11
ERROR CORRECTOR
ERROR CORRECTION DATA GENERATOR
TRANSFORM DATA
33
CONTROLLER
63
K'-DATA
R'-DATA
27
61
SOURCE DATA SPLITTER
REFERENCE MAP
S'-DATA

FIG. 6

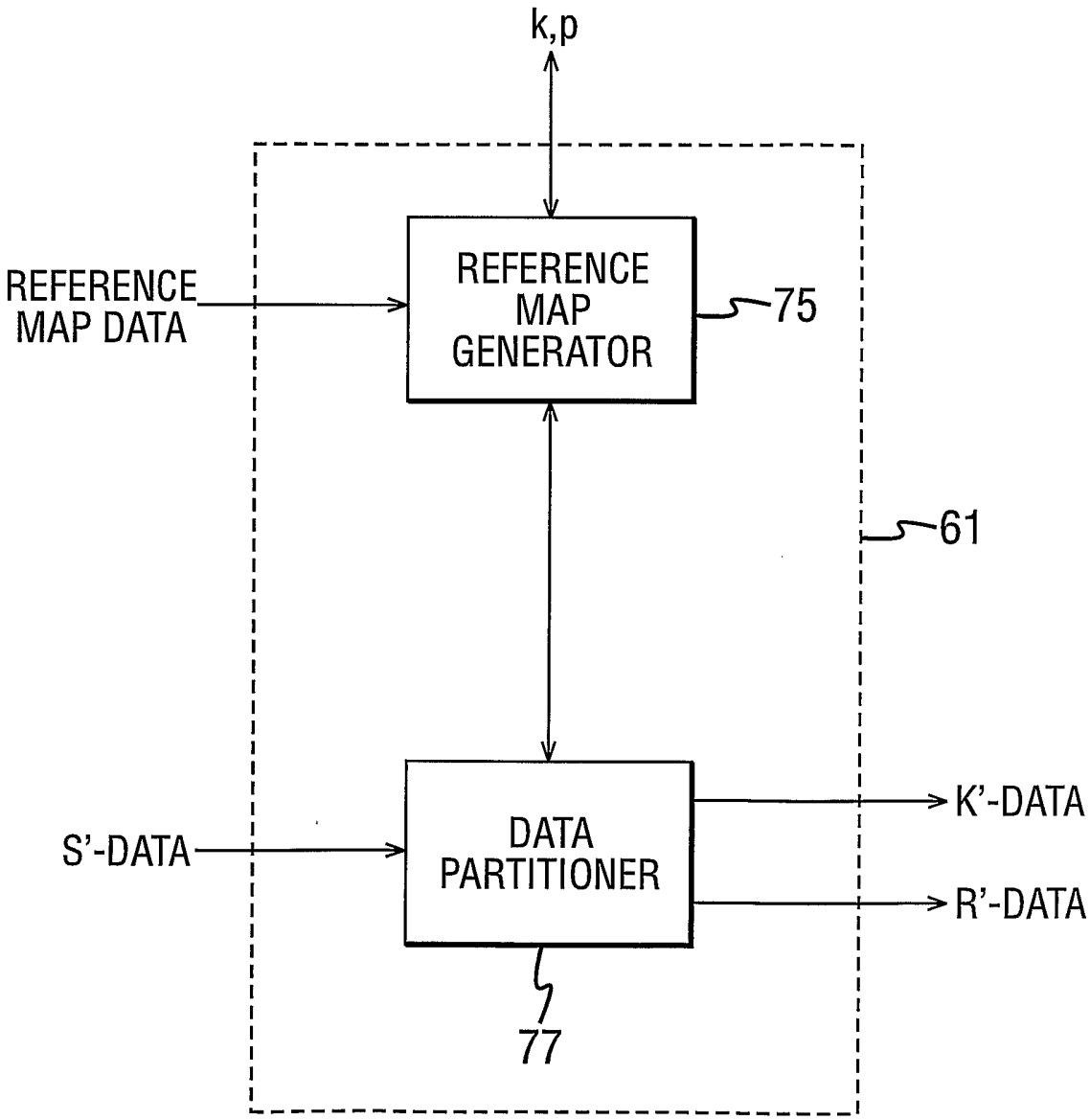

k,p
REFERENCE MAP DATA
REFERENCE MAP GENERATOR
75
61
S'-DATA
DATA PARTITIONER
K'-DATA
R'-DATA
77

FIG. 7

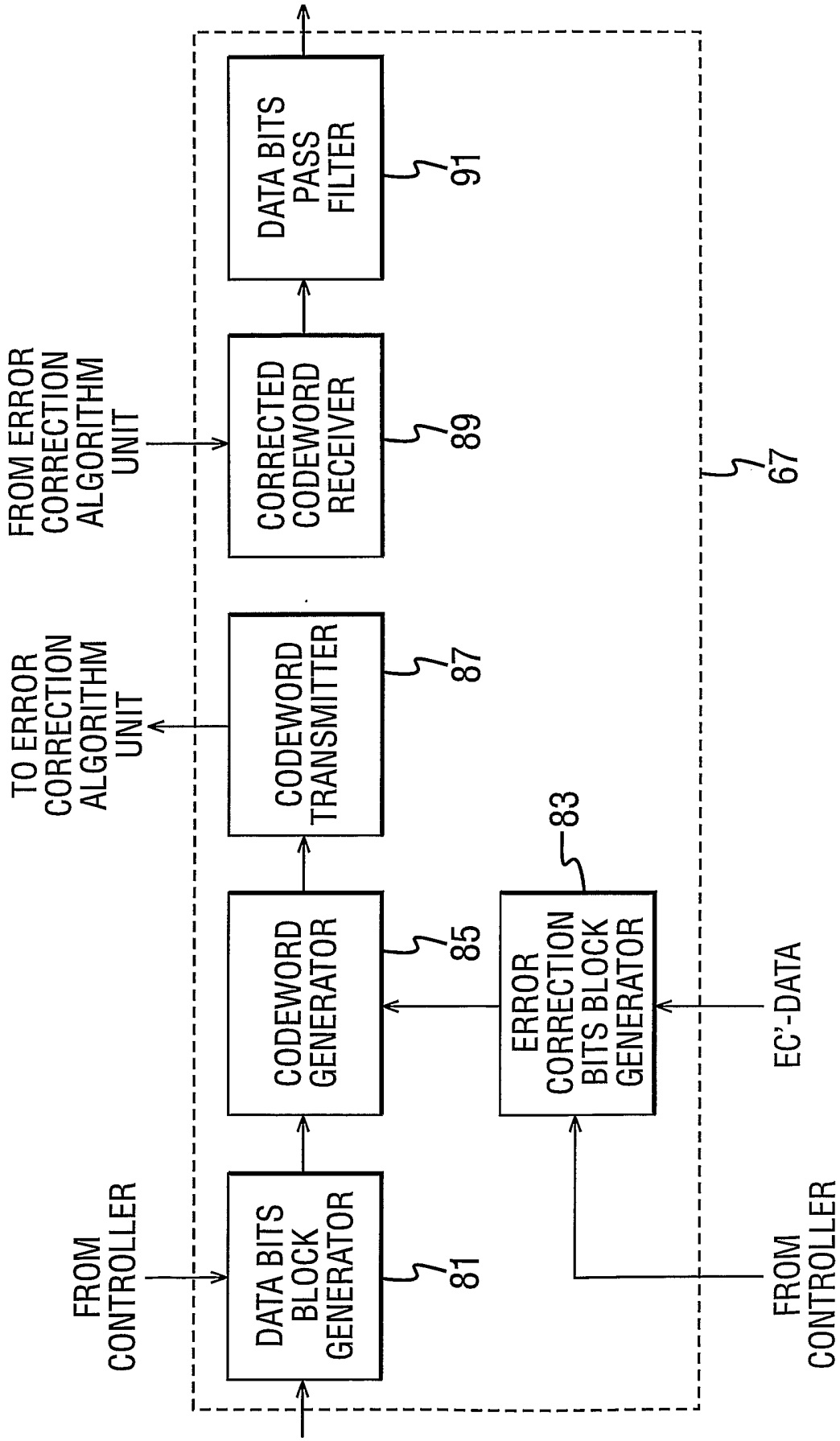

FROM CONTROLLER
DATA BITS BLOCK GENERATOR
81
CODEWORD GENERATOR
85
CODEWORD TRANSMITTER
87
TO ERROR CORRECTION ALGORITHM UNIT
FROM ERROR CORRECTION ALGORITHM UNIT
CORRECTED CODEWORD RECEIVER
89
DATA BITS PASS FILTER
91
67
ERROR CORRECTION BITS BLOCK GENERATOR
83
EC'-DATA
FROM CONTROLLER

FIG. 8

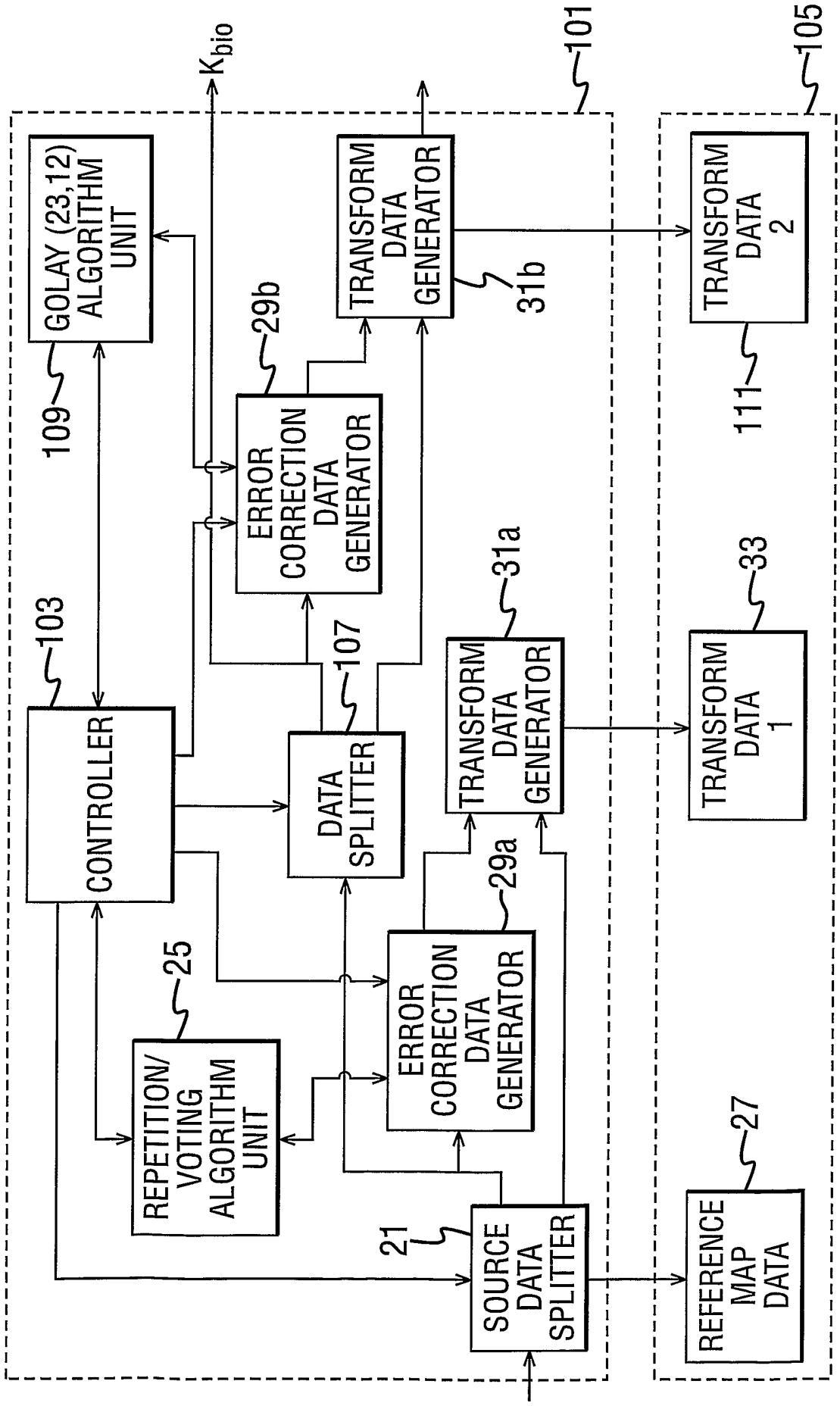

K_{bio}
101
105
GOLAY (23,12) ALGORITHM UNIT
109
TRANSFORM DATA GENERATOR
31b
TRANSFORM DATA 2
111
29b
ERROR CORRECTION DATA GENERATOR
103
CONTROLLER
107
DATA SPLITTER
31a
TRANSFORM DATA GENERATOR
33
TRANSFORM DATA 1
29a
ERROR CORRECTION DATA GENERATOR
25
REPETITION/ VOTING ALGORITHM UNIT
21
SOURCE DATA SPLITTER
27
REFERENCE MAP DATA

FIG. 9

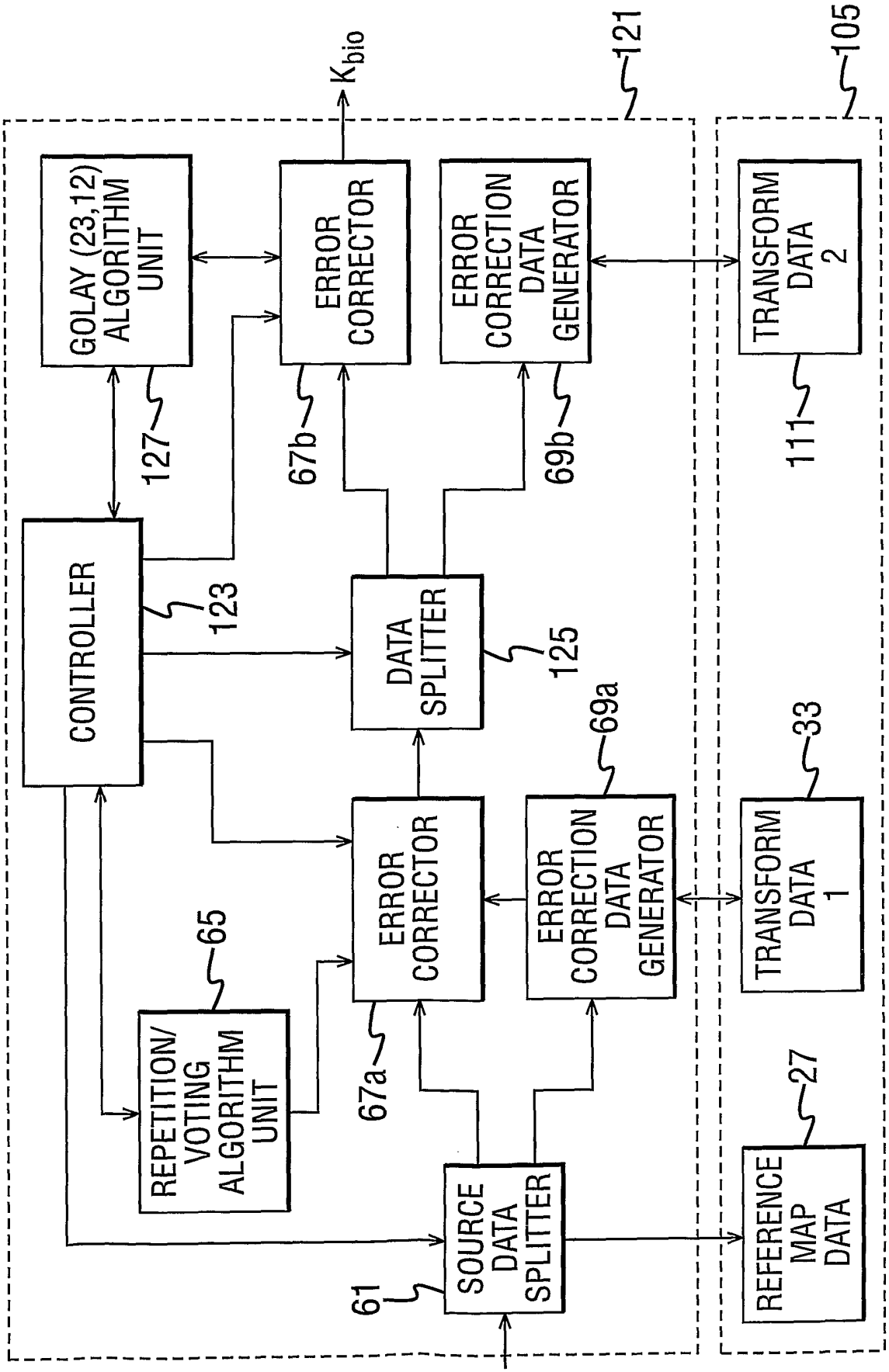

K_{bio}
121
105
GOLAY (23,12) ALGORITHM UNIT
ERROR CORRECTOR
ERROR CORRECTION DATA GENERATOR
TRANSFORM DATA 2
127
67b
69b
111
CONTROLLER
123
DATA SPLITTER
125
69a
33
ERROR CORRECTOR
ERROR CORRECTION DATA GENERATOR
TRANSFORM DATA 1
65
REPETITION/ VOTING ALGORITHM UNIT
67a
27
SOURCE DATA SPLITTER
REFERENCE MAP DATA
61

FIG. 10

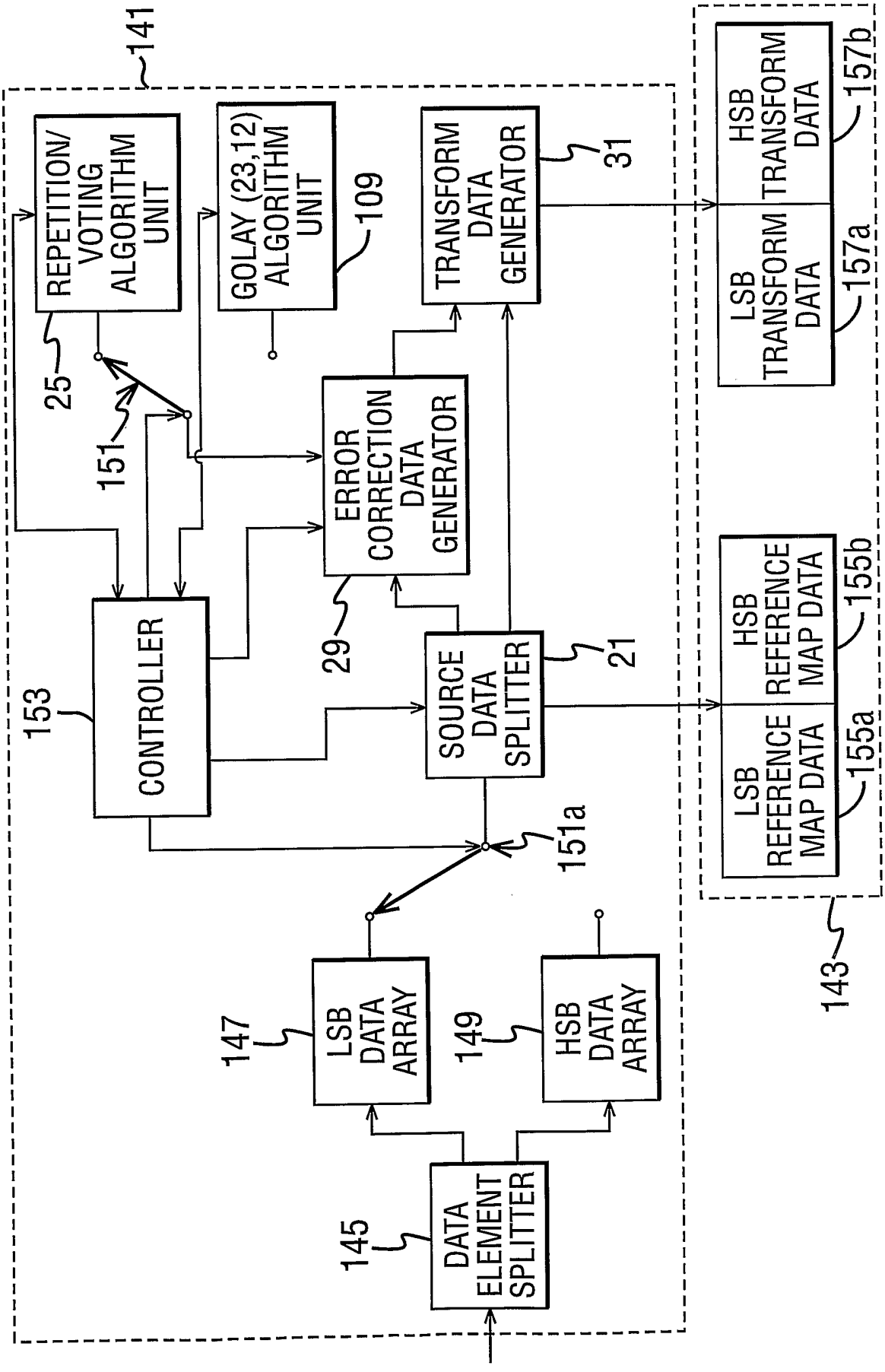

141
REPETITION/ VOTING ALGORITHM UNIT
GOLAY (23,12) ALGORITHM UNIT
109
TRANSFORM DATA GENERATOR
31
HSB TRANSFORM DATA
157b
LSB TRANSFORM DATA
157a
25
151
ERROR CORRECTION DATA GENERATOR
29
CONTROLLER
153
SOURCE DATA SPLITTER
21
HSB REFERENCE MAP DATA
155b
LSB REFERENCE MAP DATA
155a
151a
143
147
LSB DATA ARRAY
149
HSB DATA ARRAY
145
DATA ELEMENT SPLITTER

FIG. 11

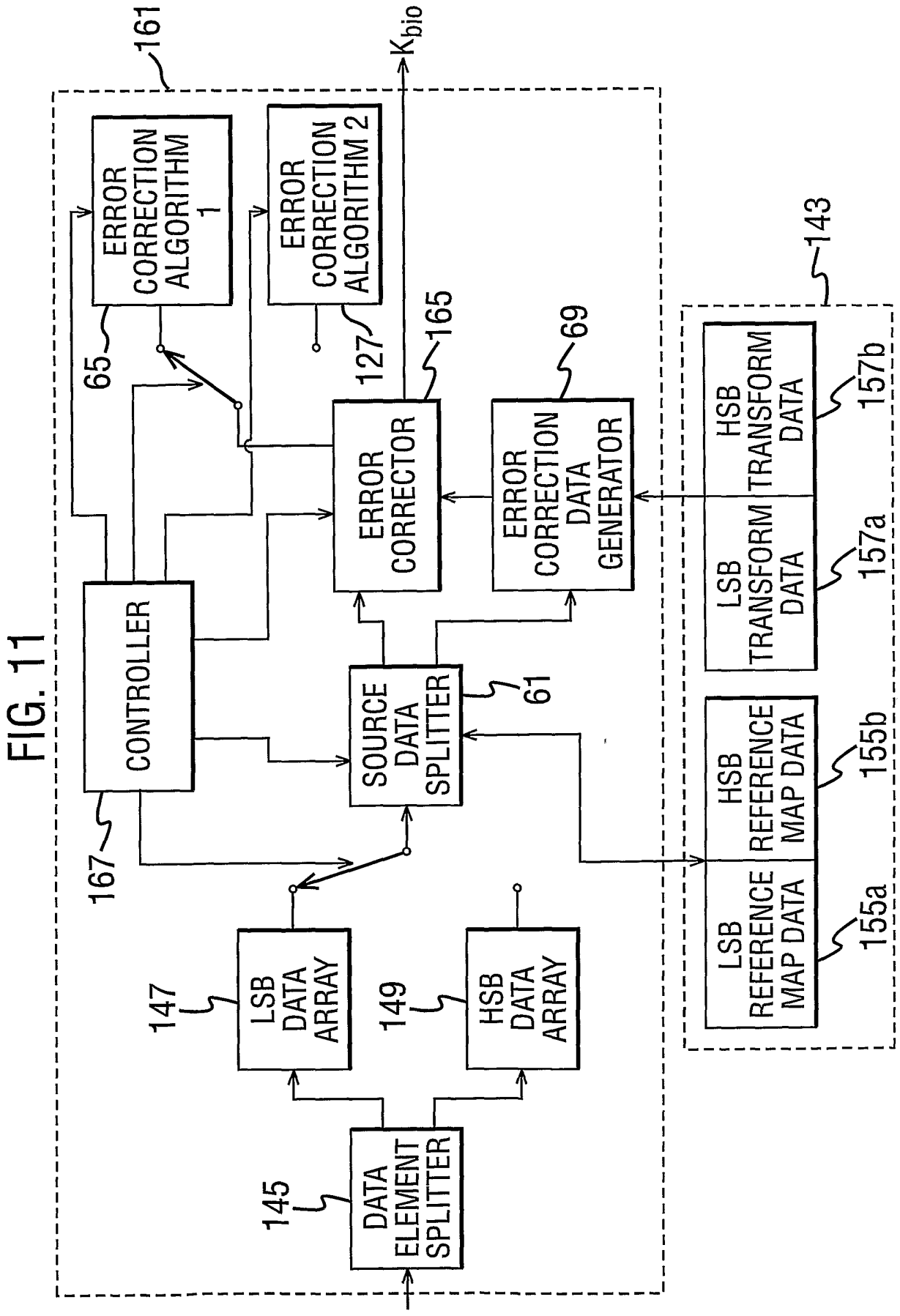
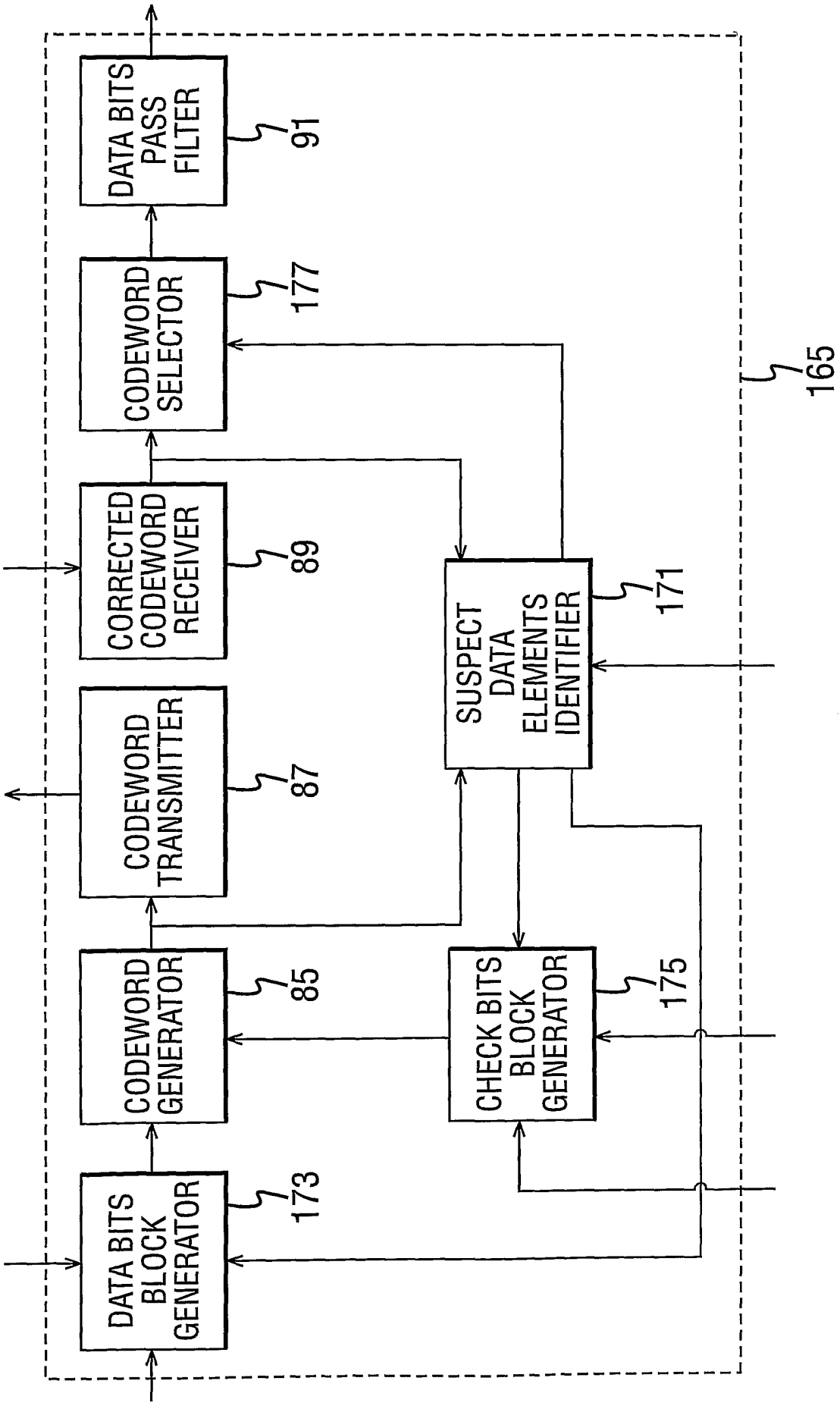

161
K_{bio}
ERROR CORRECTION ALGORITHM 1
ERROR CORRECTION ALGORITHM 2
65
127
165
69
143
ERROR CORRECTOR
ERROR CORRECTION DATA GENERATOR
HSB TRANSFORM DATA
157b
LSB TRANSFORM DATA
157a
CONTROLLER
SOURCE DATA SPLITTER
61
167
HSB REFERENCE MAP DATA
155b
LSB REFERENCE MAP DATA
155a
147
LSB DATA ARRAY
149
HSB DATA ARRAY
145
DATA ELEMENT SPLITTER

FIG. 12


DATA BITS PASS FILTER
91
CODEWORD SELECTOR
177
165
CORRECTED CODEWORD RECEIVER
89
SUSPECT DATA ELEMENTS IDENTIFIER
171
CODEWORD TRANSMITTER
87
CODEWORD GENERATOR
85
CHECK BITS BLOCK GENERATOR
175
DATA BITS BLOCK GENERATOR
173