EXHIBIT N

I certify that the following Japanese to English translation of the Japanese language document entitled, "JP-63167588-A" is an accurate and complete rendering of the contents of the source document to the best of my knowledge and ability. I further certify that I am a qualified professional translator familiar with both languages with more than twenty years of experience in Japanese to English translation of various legal, technical or business documents.

Translation Date: June 30, 2011

Robert M. Ginns

Translator’s Signature Date: June 30, 2011
Robert Ginns

(19) Japanese Patent Office (JP)

(12) Publication of Unexamined Patent Application (A)

(11) Unexamined PatentApplication (*Kokai*)
S63-167588

(43) Laid-Open Publication Date: July 11, 1988

(51) Int. Cl^4	Classification	JPO File No.
H04N 7/167		8321-5C
H 04 L 9/02		Z-7240-5K

Request for Examination: No Number of Inventions: 1 Total pages: 14

(54) Title of the Invention
Cryptographic Information Transmission System

(21) Application No.: S61-313474

(22) Filing Date: December 27, 1986

(72) Inventor Ishiyama, Tomoo
c/o Toshiba Yokohama Kinzoku Factory
8 DAIKOKU-FUTO TSURUMI-KU
YOKOHAMA-SHI **KANAGAWA**

(71) Applicant Toshiba Corp.
72, Horikawa-cho, Saiwai- ku
Kawasaki-shi, **Kanagawa**

(74) Agent, Attorney, Patent Agent Ito, Susumu

SPECIFICATION

1. Title of the Invention

Cryptographic Information Transmission System

2. What is claimed is:

A cryptographic information transmission system having a random number generating and initial value generating means for scrambling and descrambling transmission information on respectively an encoder side and a decoder side comprising:

original initial value generating means for generating original initial value data for a random number generator on the encoder side;

key data generating means for encrypting using key data temporally changed original initial value data generated by the source initial value generating means;

means for generating drive information for driving the key data generating means;

transmission means for transmitting to the decoder side scrambled transmission information from random numbers generated by the random number generator with, as initial value data, original initial value data encrypted using drive information generated by the drive information generating means, original initial value data, original initial value related data as well as original initial value data encrypted by key data;

extraction means for extracting transmitted original initial value data or original initial value related data as well as drive information;

key data generating means for generating key data corresponding to the encoding side with drive information extracted from the extraction means added; and

a random number generator that obtains initial values of the random number generator on the encoding side using this key data generating means and generates random numbers for descrambling transmitted signals that have been scrambled.

3. Detailed Description of the Invention

[Object of the Invention]

(Field of the Invention)

This invention relates to a cryptographic information transmission system in a subscriber transmission system according to unidirectional communications that can know key information used for scramble deciphering that was added to toll broadcast signals. The scrambling is not directly deciphered using this key information. In addition, in this system, it is possible to suppress to a minimum period the descrambling read operation even when it is not normally possible to separate synchronizing signals due to noise in transmission systems.

(Description of Related Art)

In subscriber broadcast systems such as CATV systems, the broadcasting station charges according to specific programs, mixes (scrambles) the transmission signals, and prevents viewing by subscribers other than subscribers that have executed contracts with the broadcast station. In order to accomplish this restriction, the greater the scrambling (encryption), the higher the security against theft viewing, but on the other hand, proper timing becomes difficult for descrambling (making undeciphered text) for the contract subscriber.

Various scrambling methods exist. For example, using video signals, sychronization and compression are performed adding AM modulation to synchronous signals in baseband stages. If the synchronization and compression are performed in a regular manner, accurate descrambling can be obtained, but there are occasions when failure of this method can result in theft viewing. Because of this method’s failure, it is common to use systems that emphasize security, for example, using M serial pseudo random pulse generators (random number generators) to make random timing. The key data (random number initial value) for deciphering the scrambling, for example, in the case of video signals, is superimposed during specific horizontal scan periods during vertical blanking periods.

However, even with toll broadcasting signals made confidential by random timing and transmitted, theft viewing becomes comparatively easy as long as the initial value is transmitted. More particularly, in the case of a unidirectional system, errors in initial values occur on the receiving side and because it is not possible to obtain a response whether or not there was accurate reception, security against theft viewing is reduced because it is necessary to transmit any number of times the same initial value data.

Therefore, in the case of unidirectional systems, the transmitted initial value data is successively changed, and if the initial value data is not immediately deciphered for every change that has occurred, theft viewing is not possible.

FIG. 8 and FIG. 9 show one embodiment of a conventional cryptographic information transmission system that transmits initial value data as previously described. Moreover, FIG. 8 shows an encoder and FIG. 9 shows a decoder.

In FIG. 8, source video signals are introduced from a source such as VTR to the terminal 801. The source video signals are input to the scramble circuit 802. Horizontal synchronous signals are sometimes randomly compressed or not compressed by the random timing signal 803a from the random number generator 803 and are supplied to the data superimposing circuit 804. The data superimposing circuit 804 is a circuit that superimposes the necessary initial value data in the decoder during video signal transmission.

The source video signals are separated by the synchronous separation circuit 805 into the horizontal synchronous signal Hsy and the vertical synchronous signal Vsy. Every synchronous signal Hsy and Vsy is input to the timing generator 806 becoming every kind of timing signal that is, in turn, fed to specific circuits. The timing pulse generator 806, along with driving the random number generator 803 using the driving pulse 806a, feeds the vertical synchronous pulse P1 and respectively signals 807a and 807b from the transmission count control circuit 807 to the AND gates AN1 and AN2. The initial value load pulse 806b as the output of the AND gate AN1 is fed to the random number generator 803 and the initial value conversion pulse 806c as the output of the AND gate 2 is fed to the initial value generating circuit 808. The output of the initial value generating circuit 808, along with causing unidirectional input data to the superimposing data operation circuit 809, feeds the random number generator 803 through the delay circuit 811. The delay circuit 811 delays the initial value data 808a from the initial value generating circuit 808 only to the extent of n field periods (nV) transmitting identical initial value data. From this delay, the scrambled video signals, according to the initial value data currently transmitted are transmitted after n field periods.

The transmission count control circuit 807 counts to a specific count the vertical synchronous signals Vsy from the synchronous sepearting circuit 805, having a function that controls scrambling using identical intial value data and controls its transmission frequency. The initial value conversion pulse 806c that outputs from the AND gate AN2 is a latch pulse towards the (nV) delay circuit 811 and the signal 807a is a data replacement control signal towards the superimposing data operation circuit 809. This superimposing data operation circuit 809 is a circuit that selects the output of the initial value generating circuit 808 and the output of the synchronous pattern generating circuit 810. 809 also selects synchronous pattern signals using the timing of the signal 807a and selects the initial value data 808a for other periods.

FIG. 10 shows a timing chart for performing control operation of the transmission frequency control circuit 807. FIG. 10(a) shows transmission initial value data, FIG. 10(b) shows transmission video signals, and FIG. 10(c) shows the load pulse towards the random number generator. As shown in the drawing, it is understood that the initial value data X newly generated by the timing of the initial value conversion pulse 806c superimposes and transmits the video signals scrambled by old initial value data generated before the nV period.

Next, a description is given of the formation of the decoder.

Transmission signals from the data lines appear at the terminal 901 in FIG. 9.Signals at this terminal 901 are baseband scrambled video signals that have passed through a tuner, not illustrated, and a 1F detector circuit and are input to the descrambler circuit 902. The descrambler circuit 902 descrambles the video signals synchronously compressed using random signal timing from the random number generator 903 that generates random numbers that match with those found at the encoder side. The following formation is a circuit that generates random numbers that match the timing on the encoder side from the random number generator 903.

Signals from the terminal 901 are input to the data extraction circuit 904 and the synchronous separator circuit 907. The synchronous separator circuit 907 separates from the scrambled video signal the horizontal synchronous signal Hsy and the vertical synchronous signal Vsy and feeds these two signals to the timing pulse generator 908. The data extraction circuit 904 extracts superimposed data during the vertical blanking period of the scrambled video signal according to the timing pulse 908 from the timing pulse genertaor 908. The output from the data extraction circuit 904 is supplied to the synchronous pattern detector 906 and the data discriminator 905.

In addition, the vertical synchronous signal from the synchronous separator circuit 907 is frequency input to the transmission circuit counter 909. This transmission circuit counter 909 has a counter function that matches the transmission circuit of the transmission count control circuit 807 on the encoder side and is reset by the logical product output of the reset signal 906a and the non-illustrated carry output from the synchronous pattern detector 906.

The synchronous pattern detector 906 detects synchronous patterns among data from the data extraction circuit 904 according to the detection timing signal 908c from the timing pulse generator 908. The reset signal 906 is output when the detected data is a synchronous pattern.

The data discriminator 905 is a circuit that discriminates, using bit units, the contents of the initial value data transmitted n (n is an integer equal to or greater than 1) times. An example of this circuit is a majority decision circuit. In the data discriminator 905 a bit comparison clock (not shown) for comparing the contents with each bit of the initial value data is obtained by the n count decode output 909a from the transmission frequency counter 909 and the bit synchronous output 908d of the timing pulse generator 908. In addition, when the data discriminator 905 feeds to the random number generator 903 the output 905a, having determined the data contents, the discriminator clears the counter of the majority decision circuit according to a clear pulse (not shown) formed using the pulse 908e generated by the synchronous pattern timing and formed using the output 909a. The random number generator 903 generates random numbers based on data determined as initial value data using the data discriminator 905.

Moreover, the random number generator 903 loads data from the data discriminator 905 according to the output 910a of the AND gate 910 that inputs the final count data output 909a and a specific timing pulse 910a from the timing generator 908.

A subscriber transmission system that employs conventional unidirectional communications in this way continuously multicycles initial value data and prevents a reduction in theft viewing security by periodically changing the initial value data. Because the initial value data determines the correct data by majority decision, having compared the contents for every bit of the mutliple received data, it is understood that practically, the decoder can only obtain once in multiple fields the initial value data.

At the same time, because the pulse 903a that drives the random number generator 903 on the decoder side is formed by the timing pulse generator 908 based on synchronous signals from the synchronous separator circuit 907, noise is generated by the data circuits and as synchronous signals fall and rise, proper driving pulses cannot be obtained. The random numbers end up out of sync with the encoder side and it is not possible to accurately perform descrambling. Furthermore, because practically the initial value data is only obtained one time in multiple fields, when the synchronous signals are not properly separated using any one of the segments of the scrambled video signals according to some initial value data, the video signal of the entire segment is unavoidably received on the screen according to the descrambling operation.

(Problems that the Invention is to Solve)

A conventional CATV system that uses unidirectional communication periodically modifies the initial value data used for descrambling that is transmitted multiple times. Using the data determined from the transmitted data of this multiple part as the initial value, because the same random number as on the encoder side can be obtained using the timing of specific timing signals generated based on the transmitted synchronous signals, noise is generated by the transmission system. When synchronous signals of this periodicity cannot be correctly obtained, at least the next initial value data is transmitted and there are circuit defects that prevent being able to properly perform descrambling up to the point where data contents can be determined. Because of this inability, the contract subscriber cannot obtain the correct information and because of countermeasures in place against theft viewing, the contract subscriber bears some inconvenience.

This invention solves the previously described problems, providing a cryptographic information transmission system that provides extremely high quality information for the contract subscriber even in the presence of noise from the transmission system and transmits toll broadcast signals with high security against theft viewing by the non-contract subscriber.

(Constitution of the Invention)

(Means of Solving the Problems)

This invention comprises original initial value generating means for generating original initial value data for a random number generator on the encoder side;

key data generating means for encrypting using key data temporally changed original initial value data generated by this source initial value generating means;

means for generating drive information for driving this key data generating means;

transmission means for transmitting to the decoder side scrambled transmission information from random numbers generated by the random number generator with, as initial value data, original initial value data encrypted using drive information generated by the drive information generating means, original initial value data, original initial value related data as well as original initial value data encrypted by key data;

extraction means for extracting transmitted original initial value data or original initial value related data as well as drive information;

key data generating means for generating key data corresponding to the encoding side with drive information extracted from this extraction means impressed; and

a random number generator that obtains initial values of the random number generator on the encoding side using this key data generating means and generates random numbers for descrambling transmitted signals that have been scrambled and wherein it is not possible to illegally view using only initial value data.

(Use)

According to this invention, because the scrambling actually performed on the transmitted information is performed according to converted data that has logically converted transmitted initial value data according to key data on the encoder side, it is not possible to obtain proper descrambling timing by only deciphered transmitted initial value data.

In addition, because on the decoder side it is possible to reproduce the key data without a transmission path having matched the encoder side and the timing, even when the timing of the random number generation is not in sync because of missing amplification of the synchronous signals and when it is not possible to properly descramble information of this information’s unit period, it is possible to perform correct descrambling from the period if the contents of the original initial value data are altered.

Conventionally, the timing of the random number generator until the change segment of the initial value data has elapsed remains out of sync, but by converting the actual initial value by key data, it becomes possible to contract to a minimum period the descrambling operation.

(Embodiments)

Below, a description is given of this invention for the embodiments shown in the drawings.

FIG. 1 is a block diagram showing one

embodiment of an information transmission system related to this invention. FIG. 2 and 3 show the embodiment's formation in detail.

In FIG. 1, the transmission data processing means 11 is a circuit that inputs source video signals 10 and performs scrambling. The output of the same processing means 11 is introduced to the transmission path 13 through the data superimposing means 12. The source video signal 10 is fed also to the transmission frequency control means 14. The transmission frequency control means 14 counts the vertical synchronous signals of the source video signal and outputs the signals 14a, 14b, and 14c. Among these, the signal 14a is a signal that increments for every vertical synchronous signal that is counted and this signal is input to the initial value conversion means 16. The output signals 14b and 14c of the transmission frequency control means 14 are signals that impart timing for converting the initial value data. For example, when converting initial value data for every n fields, a maximum count value for the transmission frequency control means 14 is set to n and at this time, the signal 14b is output corresponding to the count value n. The new initial value data is generated using the timing of the n count value output 14b. The superimposed data creation means 17 selects the output of the synchronous pattern generating means 18 during an n count output and selects the initial value data for other periods. Moreover, the initial value generating means 15 holds new initial value data from the count value n until n-1 of the next count period.

At the same time, the initial value conversion means 16 has the function of outputting n fields for latched initial value data (suitable for data X letting the current transmission data be data of X + 1 in FIG. 10) that was generated previously using timing when new initial value data is generated by the initial value generating means 15. The previous initial value data that was latched output receives specific logical conversion using each increment value of the signal 14 and generates the random number signal 16a based on this converted data. The source video signal input to the transmission data processing means 11 using the timing of this output random signal 16a is scrambled.

The scrambled video signal is transmitted in this way on the transmission path 13 with the converted data as the initial value.

The scrambled video signal 19 from the transmission path 13 is fed to the reception data processing means 20, the data extraction means 21 and the transmission frequency count means 22. The reception data processing means 20 is a circuit that performs processing converse to the transmission data processing means 11 on the encoder side and descrambles the scrambled video signal. In addition, the data extraction means 21 is a circuit that extracts for every field all the initial value data superimposed in a specific period.

The transmission frequency count means 22 counts the vertical synchronous signals in the scrambled video signal and feeds to the initial value conversion means 23 the count output 22a. In this case, for the transmission frequency count means 24, when the synchronous pattern detection means 24 that detects synchronous patterns detects a synchronous pattern, the count value is cleared by the signal 24a that shows the detection timing. From this operation, the initial value conversion means 23 outputs the random signal 23 that is identical to that of the encoder side. The descrambled video signal properly descrambled by the reception data processing means 20 is output.

FIG. 2 is a block diagram showing, among the structures, the encoder side. When comparing FIG.2 and FIG. 1, the transmission data processing means 11 corresponds to the scramble circuit 202, the data superimposing means 12 corresponds to the data superimposing circuit 204, the transmission frequency control means 14 corresponds to a structure comprised of the synchronous separation circuit 205, the field counter 213 and the n-stage decoder 212, the initial value generating means 15 corresponds to the initial value generating circuit 208, the initial value conversion means 16 corresponds to a structure comprised of the initial value latch circuit 214, the initial value conversion circuit 215 and the random number generator 203, the superimposing data creation means 17 corresponds to a structure comprised of the data exchange circuit 209 and the P/S (parallel/serial) converter 216, and the synchronous pattern generating means 18 corresponds to the synchronous pattern generating circuit 210. Moreover, the circuit 207 formed using the field counter 213 and the n-stage decoder 212 is compatible with the transmission frequency control circuit 807 in FIG. 8 and is explained in detail below.

The terminal 201 is an input terminal for source video signals and the signals from the same terminal 201 are fed to the data superimposition circuit 204 through the scramble circuit 202. Signals from the terminal 201 are input also towards the synchronous separator circuit 205 and the horizontal synchronous signal Hsy and the vertical synchronous signal Vsy are separated. The timing pulse generator 206 inputs the reference clock signal and the horizontal synchronous signal Hsy and furthermore is reset using pulses from the reset circuit 211 that generate output using the timing of the vertical synchronous signal Vsy.

The point where the timing pulse generator 206 differs from FIG. 8 is in outputting every field of the load pulse 206b towards the random number generator 203 (conventionally there was output only once for n fields). The reason for feeding every field of the load pulse 206b in this way is because the count output 207c from the transmission frequency control circuit 207 is fed to the initial value converter 215 newly established by this invention and because every field of the real initial value is converted to the random number generator 203. This count output 207c is compatible with FIG. 1's signal 14a. Moreover, the timing pulse generator 206 generates the P/S convertion clock 206c and the load pulse 206d for driving the P/S converter 216.

The field counter 213 for the circuit 207 self-resets using the carry output CR. In addition, the n-stage decoder 212 outputs the n-1 count value decode output 207b and the n count value decode output 207a, feeding respectively as one single input and the exchange control signal of the data exchange circuit 209 towards the AND gate 3. The pulse P2 is fed to the other input of the AND gate 3 and from this feeding, along with the AND gate AN3 generating new initial values from the initial value generating circuit 208 using the timing of the n-1 count value decode output 207b, the newly generated initial value data is latched to the initial value latch circuit 214.

The initial value data generated from the initial value generating circuit 208 is output from the data exchange circuit 209 using timing other than that of the n count value decode output 207a of the n-stage decoder 212. The data exchanged, selected, and output from this data exchange circuit 209 is parallel data, is converted to serial data by the P/S converter 216 and is input to the data superimposition circuit 204.

At the same time, the initial value latch circuit 214 directly latches the previous initial value data for which new initial value data is generated by the n-1 count timing. Until the next n-1 count output 207b arrives, this initial value data is held. In other words, initial value data generated up to just before each new initial value data is generated is held and is fed to the initial value conversion circuit 215. The initial value conversion circuit 215, from this feeding, directly corresponding to increment value of the signal 207 feed the random number generator 203 the conversion data 215a as data from the initial value latch circuit 214 that has been logically converted. It is possible for the random number generator 203 to output the random number signal 203a that randomly generated pulses following the converted data 215a and scrambled the source video signal.

FIG. 3 is a block diagram showing decoder formation. When comparing FIG.3 and FIG. 1, the reception data processing means 20 is compatible with a circuit comprised of the descramble circuit 302 and the random number generator 303, the data extraction means 21 is compatible with a circuit comprised of the data extraction circuit 304 and the S/P converter 313, the transmission frequency counter 22 is compatible with a circuit comprised of the synchronous separator circuit 307, the field counter 312, and the n-stage decoder 311, the synchronous pattern detection means 24 is compatible with the synchronous pattern detection circuit 306, and the initial value conversion means 23 is compatible with the circuit comprised of the initial value latch circuit 314 and the initial value conversion circuit 315.

The terminal 301 is a terminal for which the baseband scrambled video signal is introduced. The signal from the terminal 301, along with being fed to the descramble circuit 302, is input to the synchronous signal separator circuit 307 and separated into the horizontal and vertical synchronous signals Hsy and Vsy. The timing pulse generator 308, according to synchronous signals from this synchronous separator circuit 307, generates pulses Q1 and Q2 for outputting the drive pulse 308a towards the random number generator 303, the load pulse 308f, the data extraction pulse 308a towards the S/P converter 313, the detection timing signal 308c towards the synchronous pattern detection circuit 306, the respective bit comparison clock 308d from the AND gates AN4, AN5, and AN6, the clear pulse 308e, and the latch pulse 308g. The bit comparison clock 308d and the clear pulse 308e are fed to the data discriminator 305 and perform data comparisons from the S/P converter 313 during the period of count values “0”-“n-1.” Data clear is performed when the count value is “n.” In addition, the latch pulse 308g is a pulse for latching in the initial value latch circuit 314 for counter value “n” discriminated data.

Now, the timing pulse generator 308 represents a significant difference compared with conventional embodiments, namely that every field of the load pulse 308f of the random number generator 303 is generated. The output 312a from the field counter 312, in response, is fed to the initial value converter 315. From this feeding, it is possible for the initial value converter 315 to feed the converted data 315a where every field to the random number generator 303 as initial value data was converted. Conventionally, as described using FIG. 10, the initial value load pulse is only given once to the random number generator at the time that the initial value data is converted.

Moreover, the field counter 312 and the n-stage decoder 311 are circuits compatible with the conventional transmission frequency counter 909 and a reset for the field counter 312 becomes necessary according to the detector output 306a of the synchronous pattern detection circuit 306 and the carry (CR) output.

This invention is formed as previously described and FIG. 4 and 5 are circuit diagrams showing one example of concrete structures for the initial value conversion circuit 215 and the multiple decision data discriminator 305 that used the previously described structure.

FIG. 4 is a circuit diagram showing the initial value conversion circuit 215 that constructed the encoder side as an example. Moreover, it goes without saying that the decoder side also results in the same circuit. Using this example, the count output value for the field counter 213 is comprised of 4 bits, but the initial value data is 8-bits and the converted data that can be obtained 215a becomes 8 bits.

The random number generator 203 is formed using digital circuits with the main body being a shift register (random number generator 203) that also generates M series PN patterns within pseudo random patterns. The converted data from the initial value conversion circuit 215 is input in parallel to the same shift register using the timing of the load pulse 206b. The drive pulse 206a serially outputs in sequence, using the timing of the vertical synchronous signal, the converted data 213a as initial value data input in parallel in this way. This output 203a is a signal that promotes random pulses, and, for example, outputs proper synchronous signals when there is no pulse. When there is a pulse, it is also possible to compress, output and scramble synchronous signals.

FIG. 5 is a circuit diagram that shows one concrete example of the majority decision discriminator 305. This embodiment is formed using the up counter 401, the comparator 402 and the comparison value setup circuit 403. Each of these circuits has the same number setup as the bit count of the initial value data. The bit comparison clock signal 308d is compared by the AND gate AN7 with every parallel bit from the S/P converter 313 and the number of AND outputs during logical “1” is counted by the counter 401. The counter 401 performs a count for every data sent from the S/P converter 313 and outputs the count value A.This output A is compared with the comparison value B from the comparator 402. The comparator 402 determines that the bit data input to the counter 401 is “1” when B ≤ A, outputting the determination to the initial value latch circuit 314 as initial value data. Here A is an integer greater than integer B by 1 or more and B, with the transmission count of the initial value data on the encoder side assumed to be n-1 (odd number), is set to (n-2)/2 when the determined conditions are 1 or greater than 1. Concretely, when n = 10, B is set to 4 and when A becomes 5, the data is determined and output.

Next, a description is given for the operation of the embodiment by referencing the drawings of FIG. 6 and FIG. 7.

FIG. 6 is a timing chart of the encoder side. (a) shows the vertical synchronous signal Vsy separated using the synchronous separation circuit 205 and (b) shows the count value of the field counter 213. Using this example, the count value for every 10 counts of the vertical synchronous signal Vsy is reset. The field counter 213 is a 10-stage counter and corresponding to this counter, a 10-stage decoder is used also for the decoder 212.

After the counter 213 has been reset, when the 9th vertical synchronous signal is counted (field count value “8”), output appears at the n-1 decoder output terminal of the 10-stage decoder 212. The output P2 of the timing pulse generator 206 is generated by specific timing of every vertical scan period and from the generation of the n-1 count value decode output, the initial value conversion pulse 214a that is shown in FIG. 6(c) is generated from the AND gate AN3. The initial value generator circuit 208 generates new initial value data from the initial value modified pulse 214a. The initial value latch circuit 214 latches previously generated initial value data directly before new initial value data is generated. This latched previous initial value data is fed to the initial value conversion circuit 215.

In this way, the initial value conversion circuit 215 modifies initial value data using the timing when the field count value is “9.” Consequently, the random number generator 203 inputs in parallel, using every field load pulse 206b, the converted data 215a which is the logical converted output of the data modified for each 10 fields (initial value data) and the data (output of the field counter 213) modified for each field using the same pattern for each 10 field segment. The actual transmitted video signal is scrambled through the generation of random numbers using the drive pulse 206a. Using this example, the segment from the count value “9” until the count value “8” of the 10th field is a segment in which the initial value data is identical.

At the same time, the initial value data that was newly generated is fed to the data exchange circuit 209.

Because the n count value decode output is generated from the 10-stage decoder 212 during the period when the count value is “9”, the data exchange circuit 209, after selecting synchronous patterns, feeds the P/S conversion circuit 216. The P/S conversion circuit 216 captures this synchronous pattern using the timing of the load pulse 206d, converts to serial data using the timing of the conversion clock and sends out to the data superimposing circuit 204. The data exchange circuit 209, when the next vertical synchronous signal is counted, feeds newly generated initial value data from the count value “0”, using the stage of count value “9”, to the data superimposing circuit 204 through the P/S conversion circuit 216. In this way, for the scrambled video signal, information used for deciphering the scrambling that is performed on the next 10 field segment is transmitted from this segment to the decoder side in the previous 10 field segment. This procedure is the same as that which was described using FIG. 10.

Moreover, in FIG. 6, (d) shows the output of P/S converter 216, (e) shows the load pulse timing towards the random number generator 203, and (f) the drive pulse (shift pulse timing).

Next, FIG. 7 is a timing chart for the decoder side.

In FIG. 7, (a) is the data extraction pulse 308b that is imparted to the S/P converter 313. Data decisions are performed for the initial value data extracted by this pulse 308b according to the majority decision described by FIG. 5 by the majority data decision circuit 305. (e) and (g) are the necessary bit comparison clock 308d and clear pulse 308e using this data decision processing. It is understood that the bit comparison clock 308d is not generated during the insertion period for synchronous patterns, but that the clear pulse 308g is generated during the same period.

FIG. 7(b) is the detection timing signal 308c for the synchronous pattern detection circuit. The timing signal 308c, generated in the same way as the load pulse 308f towards the random number generator shown in FIG. 7(h) for every field is generated in the same period.

However, when the data detected by the detection timing signal 308c is a synchronous pattern, the signal 306a shown in FIG. 7(c) is generated by the synchronous pattern detection circuit 306. At this time, the timing of the count value of the field counter 312 is when the counter value is “9”, and is the same as the timing during which the synchronous pattern is inserted at the encoder side. In addition, the signal 306a is generated across 1 field period and because the field counter 312 uses a synchronous type reset counter and because the rise of the vertical synchronous signal when the signal 306a is “1” is cleared, from the rise time of the vertical synchronous signal with the signal 306a “1”, the count value becomes “0.” Moreover, also when a synchronous pattern is not received, the field counter 312 returns from a counter value of “9” to a value of “0” through a self reset function (reference FIG. 7(d)).

At the same time, the data decision circuit 305 determines data when the count value ranges from “4”-“8” in the previous initial value segment where the clear pulse 308e is generated. Because when this count value is “8” is the period when the count value decode output of n-1 of the field counter 312 appears, the determined data is latched directly to the initial value latch circuit 314. Because the next n-1 count value decode output appears after 10 fields, the latched data in the initial value latch circuit 314 is fed to the initial value converter 315 until the 8th field of the next initial value segment from the count value “9”th field. The count data that sequentially modifies every field (SIC: from) the count value “9” until “8” in the initial value converter 315 in response to this initial value data is fed.

The initial value converter 315 is a logic circuit of the same structure as that found in FIG. 4 and if, for initial value data identical to that on the encoder side, the count data that is modified using the same timing as that found on the encoder side is fed, it is clear that the converted data 215a on the encoder side and the same converted data 315a can be fed to the random number generator 303. Because of this feeding, the descramble circuit 302 can perform accurate descrambling.

The signal (i) shown in FIG. 7 is the pulse 308a that drives the random number generator 303. When noise is generated in conventional transmission paths, the pulse count for this drive pulse 308a increases/decreases because synchronous signals are not accurately transmitted, random number signals with misaligned timing with the encoder side are generated, the initial value data is modified and until the data is determined, it is not possible to correctly perform descrambling of the timing. However, using this invention, even when there are increases/decreases in the drive pulses for some fields and the output bits are misaligned, because the next field has the converted data 315a inserted, it is possible to suppress descrambling mislaignment within the field.

In addition, this invention transmits identical multiple initial value data continuously and using only this transmitted initial value data, it is not possible to perform correct descrambling. Thus, when attempting theft viewing, descrambling with criminal intent is not possible so long as there is no matching of the timing of the field counter that is managed by both the encoder side and decoder side.

Moreover, this embodiment is one example, and, for example, it is not necessary that the data for initial value conversion be the output of the field counter. The requirement is that it is permissible for the output pattern to be modified by sequential constant rules that are time dependent.

[Effect of the Invention]

According to the previously described invention, security is high against theft viewing and the period of descramble error operation due to missing synchronous signals is kept to a minimum.

4. Brief Description of the Drawings

FIG. 1 is a block diagram showing one embodiment of a cryptographic information transmission system related to this invention, FIG. 2 and FIG. 3 are block diagrams of the encoder and decoder whose structure is more concretely shown than that shown in FIG. 1, FIG. 4 and FIG. 5 are circuit diagrams showing one example of concrete circuits used for this invention, FIG. 6 and FIG. 7 are time charts for describing the operation of this invention, FIG. 8 and FIG. 9 are block diagrams showing conventional systems, and FIG. 10 is a time chart showing the transmission timing of the initial value data and video signals.

202-scramble circuit, 204-data superimposition circuit, 203-random number generator, 215-initial value converter, 207-transmission frequency control circuit, 213-field counter, 212- n-stage decoder, 302-descramble circuit, 303-random number generator, 309-transmission frequency counter, 312-field counter, 311-n-stage decoder, 315-initial value converter, 207c, 312a-field count value, 215a-converted data, 315a-converted data

Agent, Attorney, Patent Agent Ito, Susumu

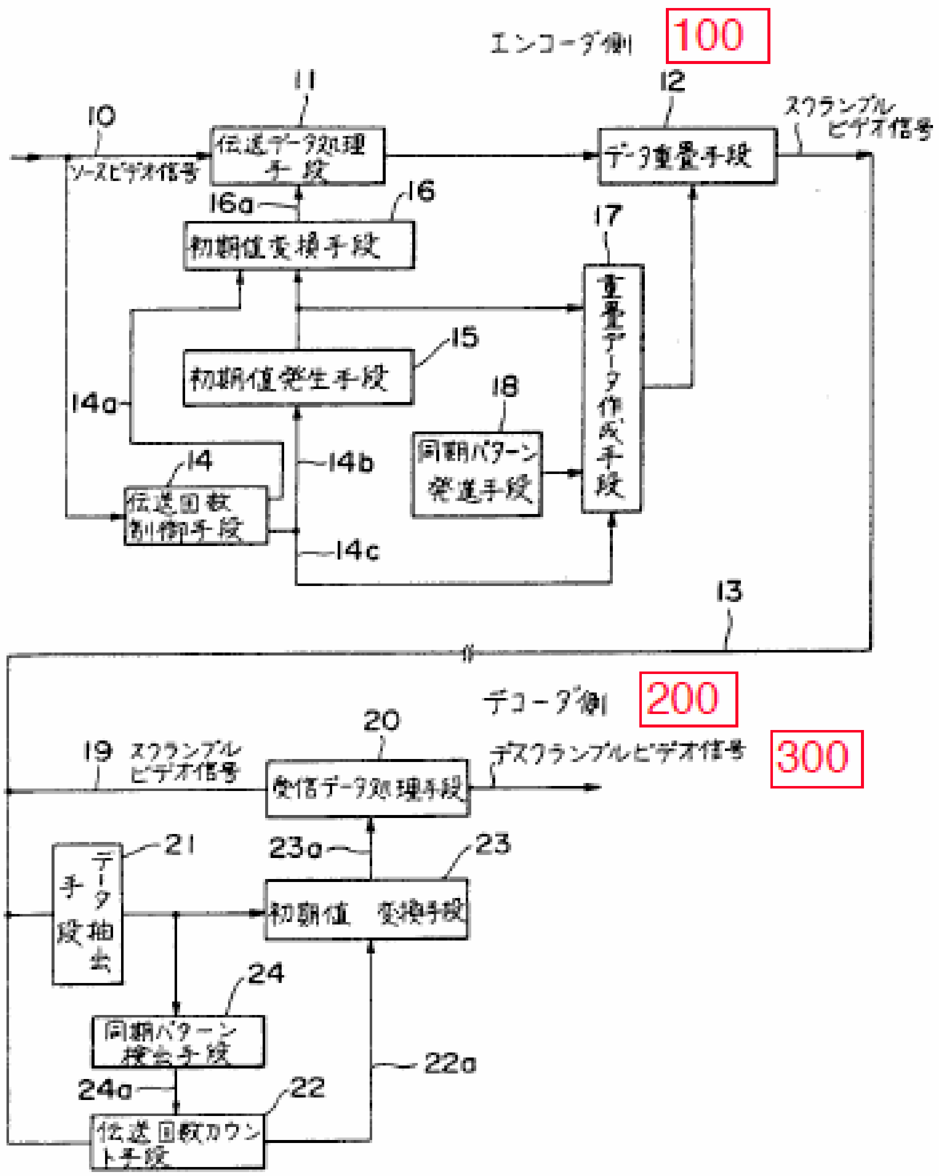

FIG. 1

10- source video signal, 11-transmission data processing means, 12-data superimposition means, 13-scrambled video signal, 14-transmission frequency control means, 15-initial value generating means, 16-initial value conversion means, 17-superimposition data creation means, 18-synchronous pattern generation means, 19-scrambled video signal, 20-received data processing means, 21- data extraction means, 22-transmission frequency count means, 23-initial value conversion means, 24-synchronous pattern detection means, 100-encoder side, 200-decoder side, 300-descrambled video signal

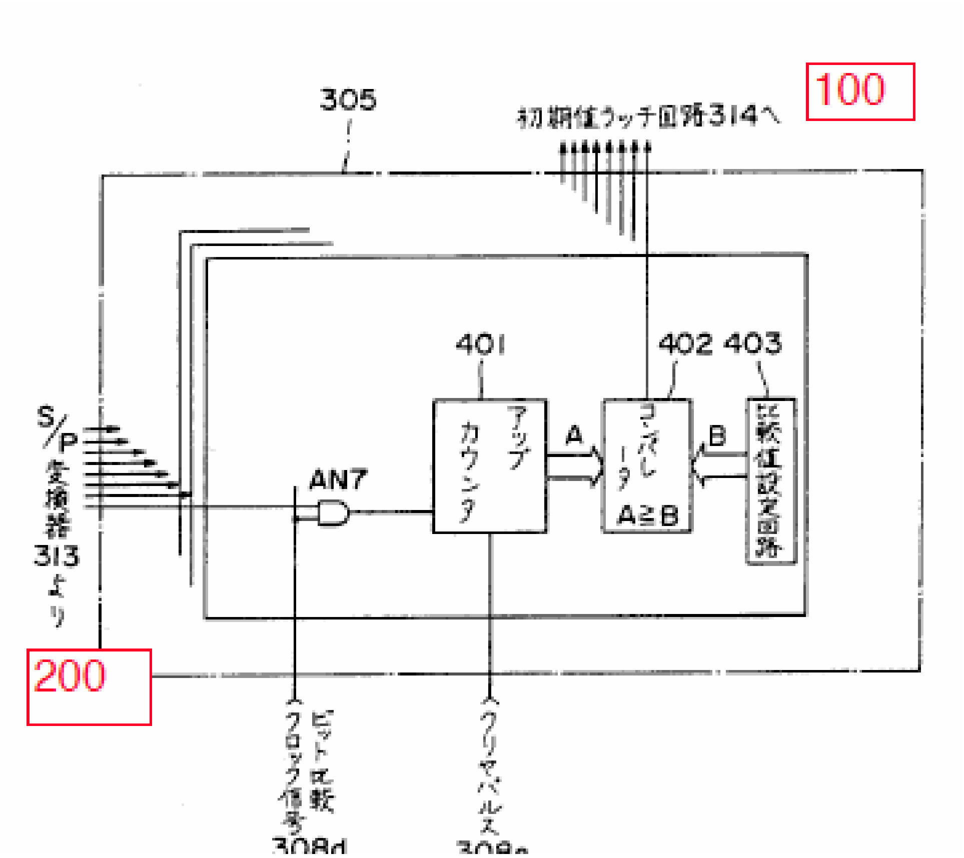

FIG. 5

100-to initial value latch circuit 314, 200-from S/P converter 313, 308d-bit comparison clock signal, 308e-clear pulse, 401-up counter, 402-comparator, 403-comparison value setup circuit

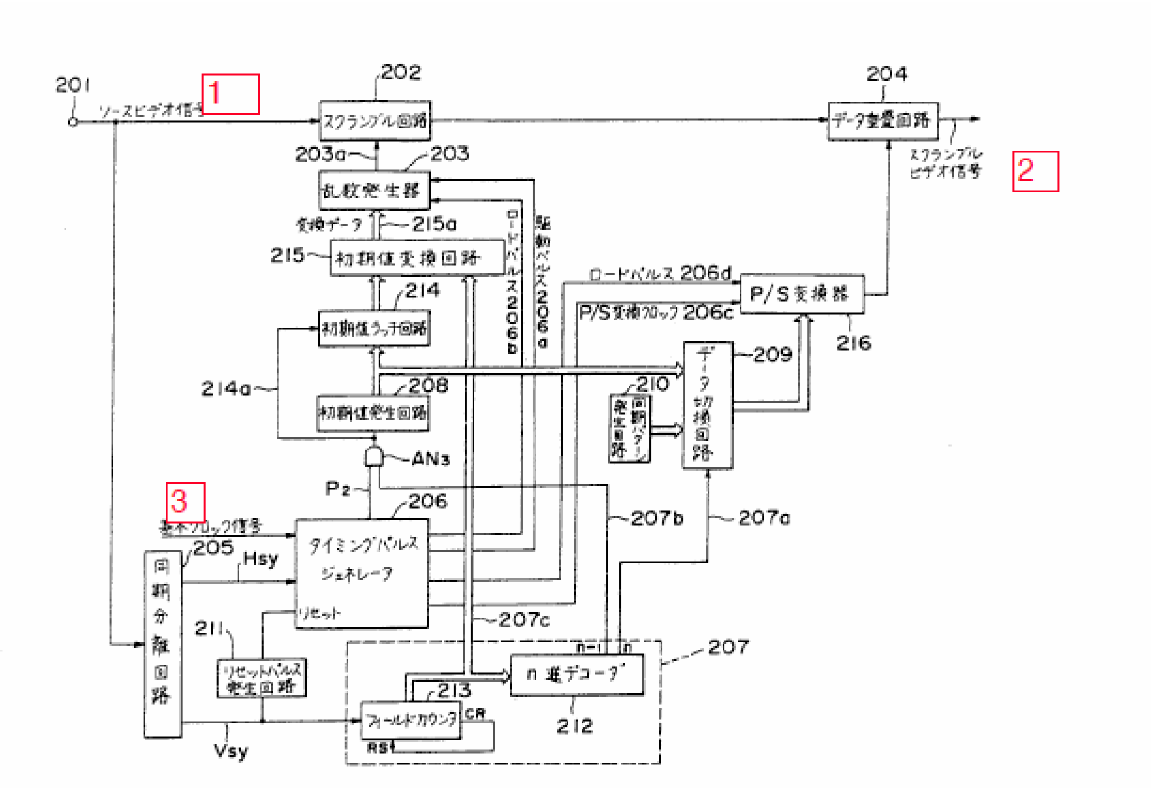

FIG. 2

1-source video signal, 2-scrambled video signal, 3-reference clock signal, 202-scramble circuit, 203-random number generator, 204-data superimposition circuit, 205-synchronous separator circuit, 206-timing pulse generator, 206a-drive pulse, 206b-load pulse, 206c-P/S conversion clock, 206d-load pulse, 207-n-stage decoder, 208-initial value generator circuit, 209-data exchange circuit, 210-synchronous pattern generating circuit, 211-reset pulse generator circuit, 212- n-stage decoder, 213-field counter, 214-

initial value latch circuit, 215a converted data, 215-initial value converter, 215a-converted data, 216-P/S converter

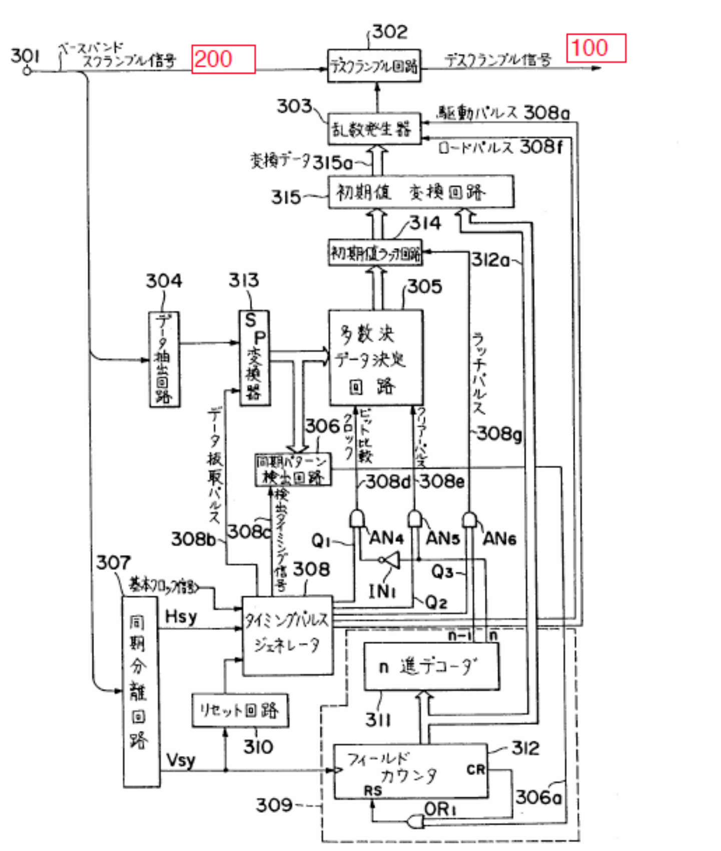

FIG. 3

100-descrmbled video signal, 200-baseband scrambled signal, 302-descramble circuit, 303-random number generator, 304-data extraction circuit, 305-majority decision data discriminator, 306-synchronous pattern detection circuit, 308a-drive pulse, 308b-data extraction pulse, 308c-detection timing signal, 308d-bit comparison clock, 308e-clear pulse, 308f-load pulse, 308g-latch pulse, 310-reset circuit, 311-n –stage decoder, 312-field counter, 313-S/P converter, 314- initial value latch circuit, 315a-converted data, , 315-initial value converter

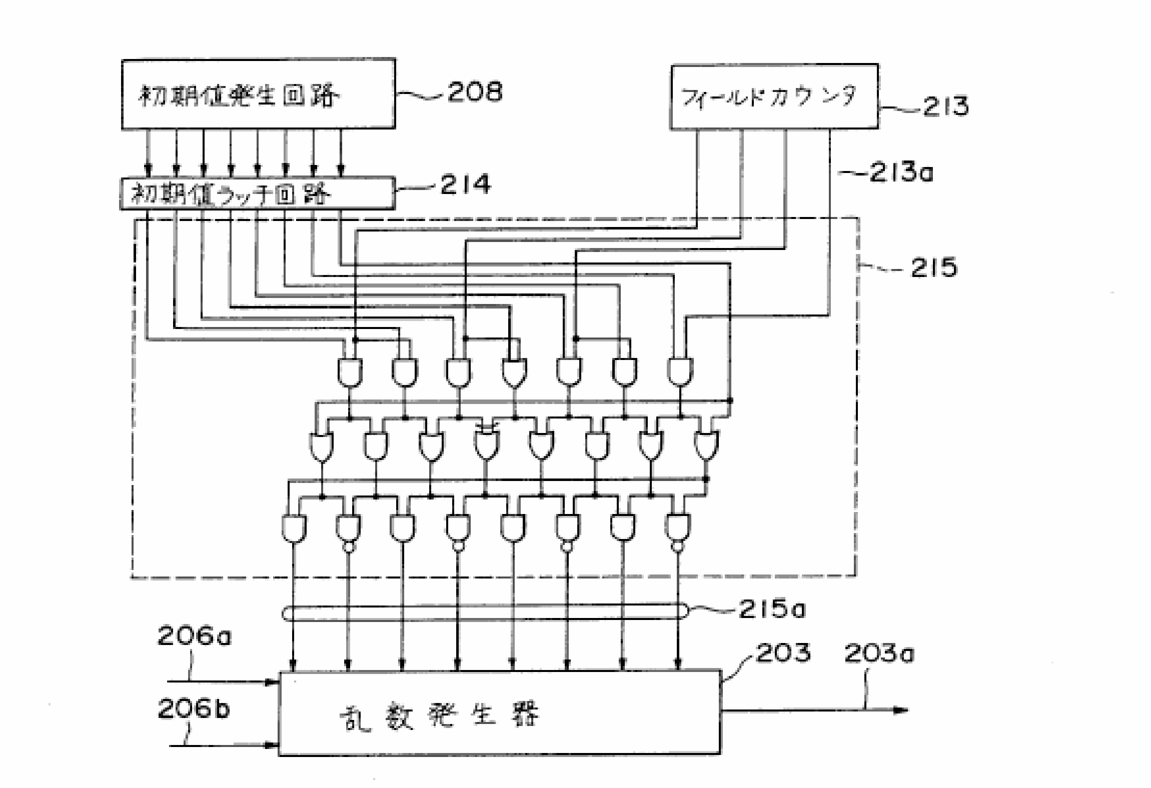

FIG. 4

203-random number generator, 208-initial value generator circuit, 213-field counter, 214-initial value latch circuit.

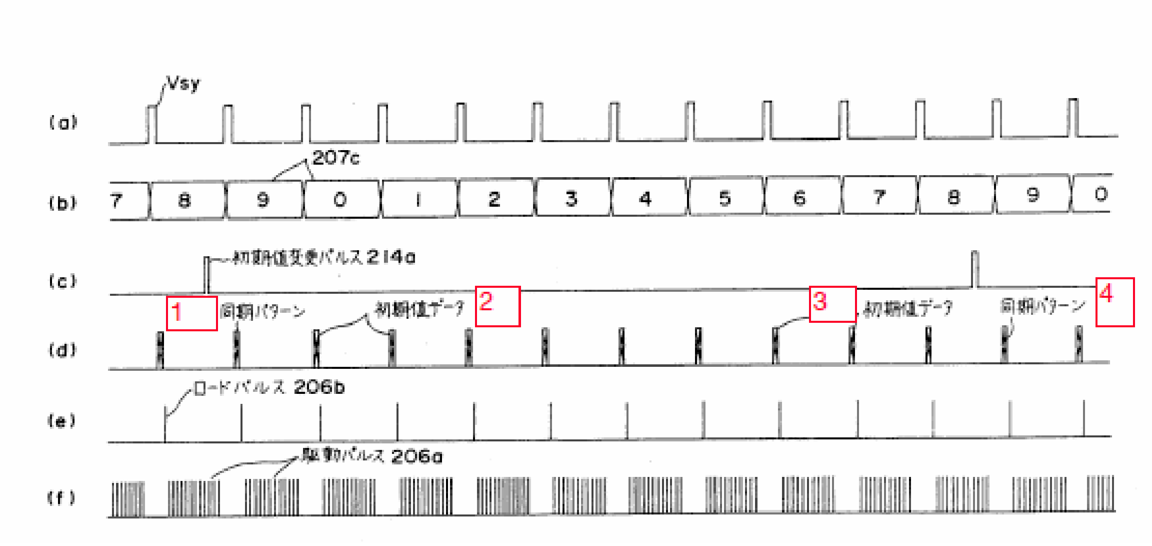

FIG. 6

1-synchronous pattern, 2-initial value data, 3-initial value data, 4-synchronous pattern, 206a-drive pulse, 206b-load pulse, 214a-initial value conversion pulse

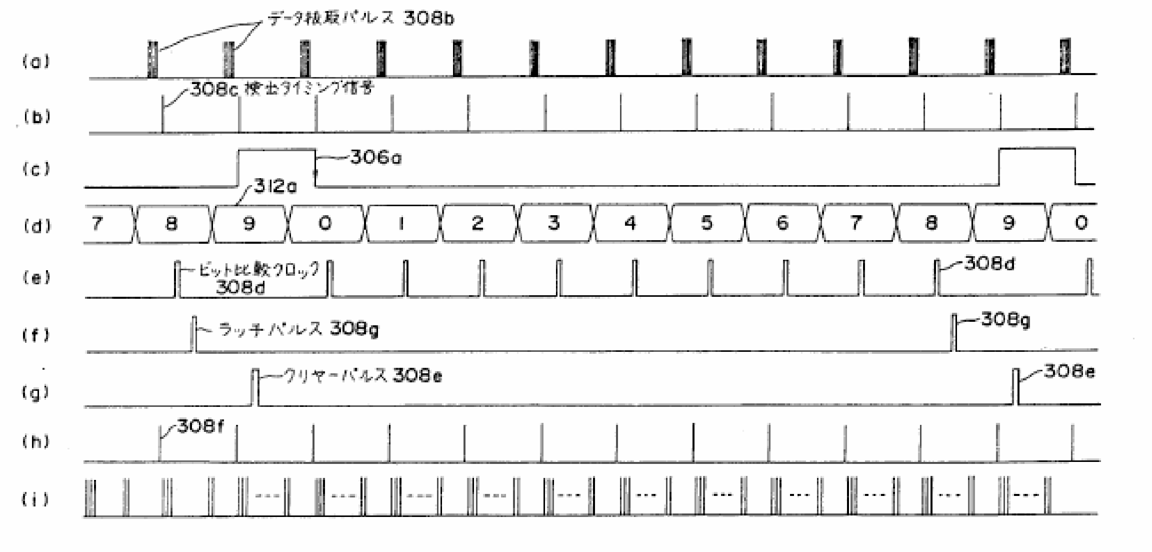

FIG. 7

308a-clear pulse, 308b-data detection pulse, 308c-detection timing signal, 308d-bit comparison clock, 308e-clear pulse, 308g-latch pulse.

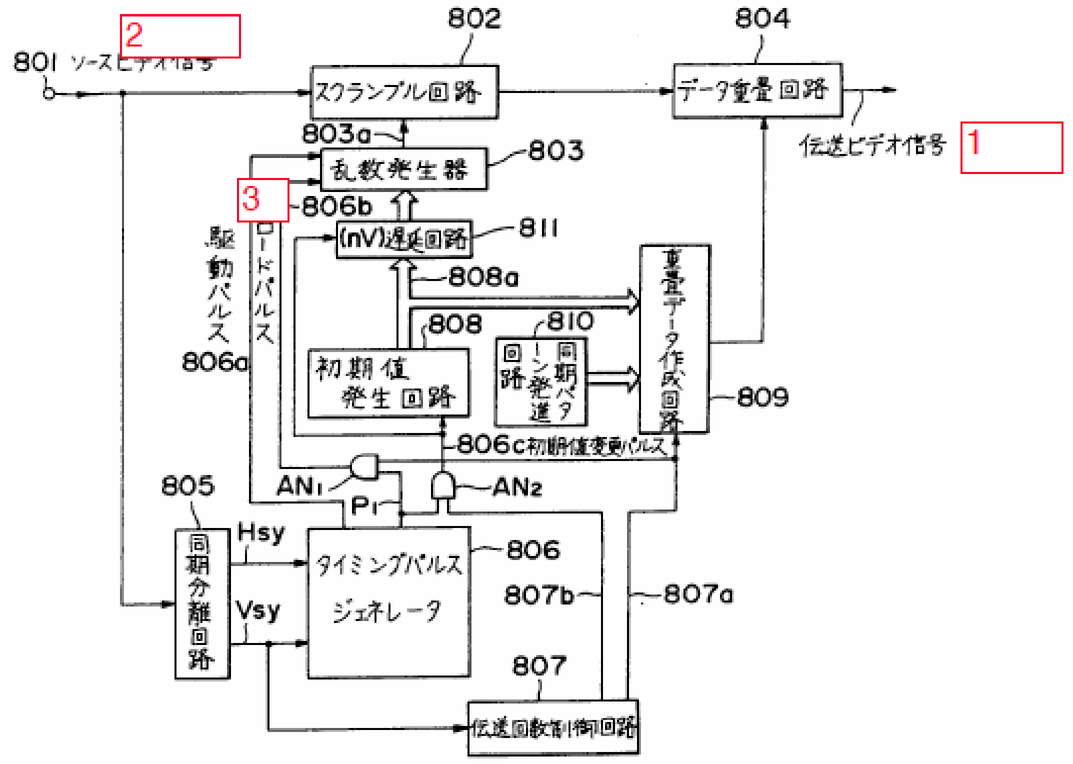

FIG. 8

1-transmitted video signal, 2-source video signal, 3-load pulse, 802-scramble circuit, 803-random number generator, 804-data superimposition circuit, 805-synchronous separator circuit, 806-timing pulse generator, 806a-drive pulse, 806c-initial value conversion pulse, 807-transmission frequency control circuit, 808-initial value generating circuit, 809-superposition data creation circuit, 810-synchronous pattern generating circuit, 811- (nV) delay circuit

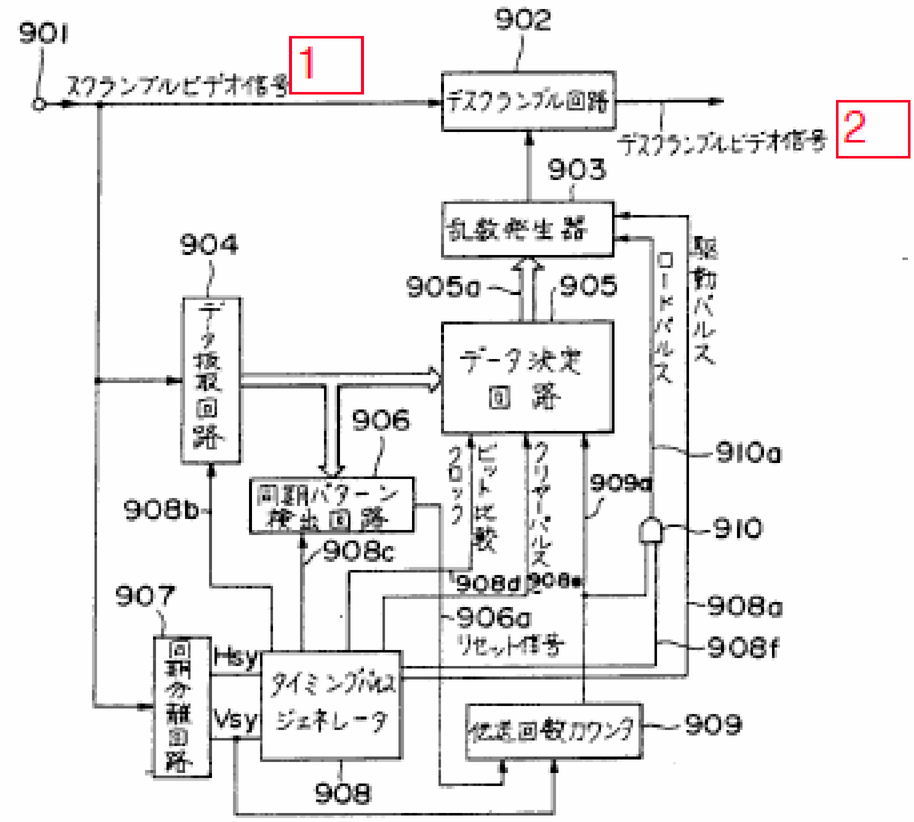

FIG. 9

1-scrambled video signal. 2-descrambled video signal, 902-descramble circuit, 903-random number generator, 904-data extraction circuit, 905-data decision circuit, 906-synchronous pattern detection circuit, 906a-reset signal, 907-synchronous separator circuit, 908-timing pulse generator, 908a-drive pulse, 908d-bit comparison clock, 908e-clear pulse, 909-transmission frequency counter

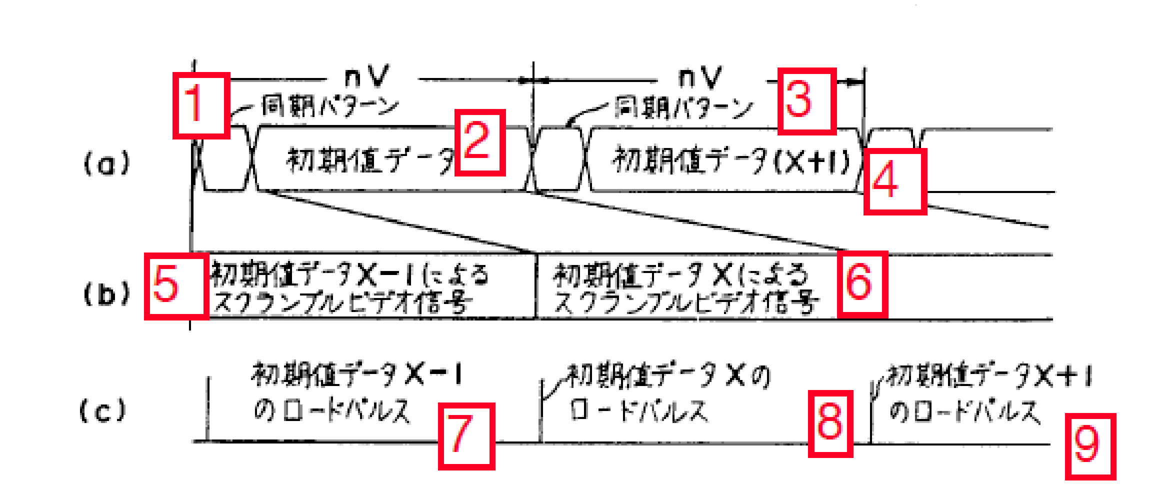

FIG. 10

1-synchronous pattern, 2-initial value data, 3-synchronous pattern, 4-initial value data (X +1), 5-scrambled video signal according to initial value data X-1, 6- scrambled video signal according to initial value data X, 7-load pulse for initial valeu data X-1, 8-load pulse for initial value data X, 9-load pulse for initial value data X + 1.