(12)Indian Patent Application

(21) Application Number: 202241067668

(22) Filing Date: 24/11/2022 (43) Publication Date: 31/05/2024

(71) Applicant(s): L&T TECHNOLOGY SERVICES LIMITED

(72) Inventor(s): Kotichukkala, Praneeth Sai Kumar

(51) International Classifications: H03F 3/24 H04L 9/30 G11B 20/00 H04L 9/06 H04B 7/26

(54) Title: METHOD AND SYSTEM FOR GENERATING CARRIER SIGNALS AND ENCRYPTION KEYS

(57) Abstract: A method and system of generating carrier signals and encryption keys is disclosed that includes determining, by a processor, a frequency of occurrence of prime numbers in 9 consecutive natural numbers preceding each multiple of 10 for up to a pre-configured upper limit of natural numbers. A set of frequency sets are created for the multiples of 10, wherein each frequency set comprises a same frequency of occurrence of prime numbers. A pattern set is determined comprising a repetition of a sequence pattern, wherein the sequence pattern comprises multiples of 10 from each of the set of frequency sets in a pre-defined order. A harmonic signal is generated by applying an Inverse Fast Fourier Transform on the pattern set. The harmonic signal generated is decomposed into a plurality of decomposition signals. Carrier signal and an encryption key are generated based on at least one of the plurality of decomposition signals.

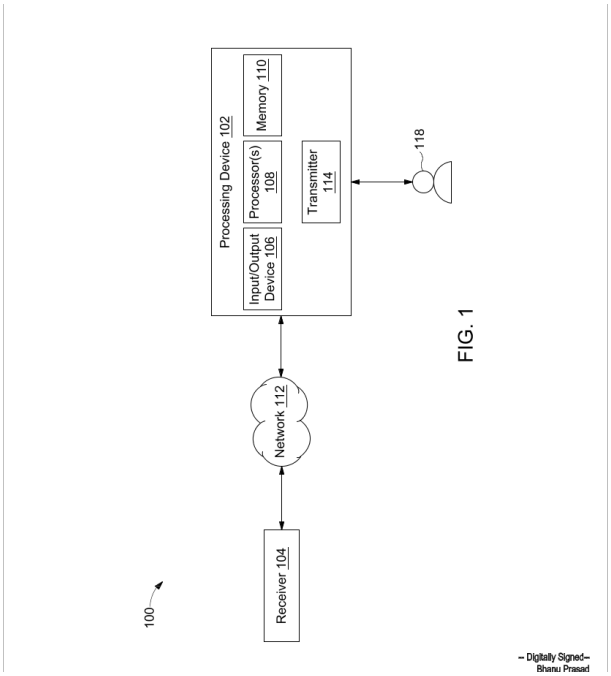


FIG. 1

FORM 2

THE PATENTS ACT 1970
(39 OF 1970)
&
The Patent Rules, 2003

Complete Specification
(See Section 10 and Rule 13)

1. TITLE OF THE INVENTION

METHOD AND SYSTEM FOR GENERATING CARRIER SIGNALS AND ENCRYPTION KEYS

2. APPLICANT(S)

(a) NAME : **L&T TECHNOLOGY SERVICES LIMITED**
(b) NATIONALITY : **INDIAN**
(c) ADDRESS : DLF IT SEZ Park, 2nd Floor – Block 3
1/124, Mount Poonamallee Road,
Ramapuram, Chennai – 600 089,
INDIA.

3. PREAMBLE TO THE DESCRIPTION

COMPLETE

The following specification describes the invention and the manner in which it is to be performed

DESCRIPTION

Technical Field

[001] This disclosure relates generally to data processing, and more particularly to a system and a method for generating carrier signals and encryption keys.

BACKGROUND

[002] Secure communication is essential to prevent leakage and misuse of digital information in current scenario. A third party may eavesdrop on a communication channel and can easily extract sensitive information from the data being shared over the communication channel and misuse the information in various ways. Various method of encryption are utilized to encrypt the digital data being transmitted in order to secure communication. Encryption requires data to be codified using a key in a particular manner such that the information is decipherable only by the intended receiver. Various methodologies are available to generating encryption keys, each having some pros and cons. Thus, an effective methodology is required for secured digital communication.

SUMMARY OF THE INVENTION

[003] In an embodiment, a method of generating carrier signals is provided. The method may include determining, by a modulator, a frequency of occurrence of prime numbers in 9 consecutive natural numbers preceding each multiple of 10 for up to a pre-configured upper limit of natural numbers. A set of frequency sets may be created for the multiples of 10, wherein each of the frequency set may comprise a same frequency of occurrence of prime numbers. A pattern set may be determined comprising a repetition of a sequence pattern, wherein the sequence pattern may comprise of multiples of 10 from each of the set of frequency sets in a pre-defined order. A harmonic signal may be generated by applying an Inverse Fast Fourier Transform (IFT) on the pattern set. The harmonic signal generated may be decomposed into a plurality of decomposition signals. A carrier signal may be generated based on at least one of the plurality of decomposition signals.

[004] In another embodiment, a system for creating carrier signals comprising one or more processors and a memory in a modulator is provided. The memory may store a plurality of processor-executable instructions which upon execution cause the one or more processors to determining a frequency of occurrence of prime numbers in 9 consecutive natural numbers

preceding each multiple of 10 for up to a pre-configured upper limit of natural numbers. A set of frequency sets may be created for the multiples of 10, wherein each of the frequency set may comprise a same frequency of occurrence of prime numbers. A pattern set may be determined comprising a repetition of a sequence pattern, wherein the sequence pattern may comprise of multiples of 10 from each of the set of frequency sets in a pre-defined order. A harmonic signal may be generated by applying an Inverse Fast Fourier Transform (IFT) on the pattern set. The harmonic signal generated may be decomposed into a plurality of decomposition signals. A carrier signal may be generated based on at least one of the plurality of decomposition signals.

[005] In yet another embodiment, a method of generating encryption keys is provided. The method may include determining a frequency of occurrence of prime numbers in 9 consecutive natural numbers preceding each multiple of 10 for up to a pre-configured upper limit of natural numbers. A set of frequency sets may be created for the multiples of 10, wherein each of the frequency set may comprise a same frequency of occurrence of prime numbers. A pattern set may be determined comprising a repetition of a sequence pattern, wherein the sequence pattern may comprise of multiples of 10 from each of the set of frequency sets in a pre-defined order. A harmonic signal may be generated by applying an Inverse Fast Fourier Transform (IFT) on the pattern set. The harmonic signal generated may be decomposed into a plurality of decomposition signals. An encryption key may be generated based on at least one of the plurality of decomposition signals.

[006] In yet another embodiment, a system of generating encryption keys comprising one or more processors and a memory in an encrypting device is provided. The memory may store a plurality of processor-executable instructions which upon execution cause the one or more processors to determining a frequency of occurrence of prime numbers in 9 consecutive natural numbers preceding each multiple of 10 for up to a pre-configured upper limit of natural numbers. A set of frequency sets may be created for the multiples of 10, wherein each of the frequency set may comprise a same frequency of occurrence of prime numbers. A pattern set may be determined comprising a repetition of a sequence pattern, wherein the sequence pattern may comprise of multiples of 10 from each of the set of frequency sets in a pre-defined order. A harmonic signal may be generated by applying an Inverse Fast Fourier Transform (IFT) on the pattern set. The harmonic signal generated may be decomposed into a plurality of decomposition signals. An encryption key may be generated based on at least one of the plurality of decomposition signals.

[007] Various objects, features, aspects and advantages of the inventive subject matter will become more apparent from the following detailed description of preferred embodiments, along with the accompanying drawing figures in which like numerals represent like components.

BRIEF DESCRIPTION OF THE DRAWINGS

[008] The accompanying drawings, which are incorporated in and constitute a part of this disclosure, illustrate exemplary embodiments and, together with the description, serve to explain the disclosed principles.

[009] **FIG. 1** is a block diagram of a processing system 100 for generating carrier signals and encryption keys, in accordance with an embodiment of the present disclosure.

[010] **FIG. 2** illustrates a functional block diagram of the processing device, in accordance with an embodiment of the present disclosure.

[011] **FIG. 3** is a flowchart 200 depicting a methodology of generating a carrier signal for modulating voice signals, in accordance with an embodiment of the present disclosure.

[012] **FIG. 4A** is an exemplary embodiment depicting configuration for the methodology of generating carrier signal as described in **FIG. 2**, in accordance with an embodiment of the present disclosure.

[013] **FIG. 4B** shown an exemplary embodiment depicting set of frequency sets of zero, one, two, three and four prime numbers as described in **FIG. 2**, in accordance with an embodiment of the present disclosure.

[014] **FIG. 5** is an exemplary embodiment depicting a sequence pattern and a pattern set, in accordance with an embodiment of the present disclosure.

[015] **FIG. 6A** discloses a harmonic signal generated by performing IFT on the pattern set of **FIG. 5**, in accordance with an embodiment of the present disclosure.

[016] **FIG. 6B** illustrates decomposition signals of the harmonic signal as shown in **FIG. 6A**, in accordance with an embodiment of the current disclosure.

[017] **FIG. 6C** depicts the ‘d9’ 602 signal selected as the carrier signal as described in **FIG. 2**, in accordance with an embodiment of the present disclosure.

[018] **FIG. 7** is a flowchart depicting a methodology of generating encryption keys for encrypting in continuation to the methodology described in **FIG. 2**, in accordance with an embodiment of the present disclosure.

[019] **FIG. 8A** shows binary data generated for the discrete decimal data of the decomposition signal selected in accordance with an embodiment of the present disclosure.

[020] **FIG. 8B** shows an exemplary encryption key generated using the binary data, in accordance with an embodiment of the present disclosure.

[021] **FIG. 9** is a flowchart of a method of creating a carrier signal and an encryption key, in accordance with an embodiment of the present disclosure.

DETAILED DESCRIPTION OF THE DRAWINGS

[022] Exemplary embodiments are described with reference to the accompanying drawings. Wherever convenient, the same reference numbers are used throughout the drawings to refer to the same or like parts. While examples and features of disclosed principles are described herein, modifications, adaptations, and other implementations are possible without departing from the scope of the disclosed embodiments. It is intended that the following detailed description be considered as exemplary only, with the true scope being indicated by the following claims. Additional illustrative embodiments are listed.

[023] Data security is a critical matter when it comes to transfer of data through digital communication channels. Security of such communication can be ensured by using encryption techniques or modulating the signals in a manner so that the demodulation or decryption can only be performed by the intended person.

[024] The present disclosure provides methods and systems for generating carrier signal and encryption key. **FIG. 1** is a block diagram of a processing system 100 for generating carrier signals and encryption keys, in accordance with an embodiment of the present disclosure. The processing system 100 may include one or more processors 108, a memory 110 and a transmitter 114. The processing device 102 may be communicably connected to a receiver 104 through a network 112. The transmitter 114 may transmit data which may be modulated using a carrier signal or data which may be encrypted using an encryption key generated by the processing system 100 of the current disclosure. In an embodiment, the data may be stored in a

database enabled in cloud or a physical database or may be real time data such as an audio, image or video data.

[025] In an embodiment, the processing device 102 may be communicatively coupled to a data source through a wireless or wired communication network 112. In an embodiment, the processing device 102 may receive a real time voice or multimedia data from a user 118 to be transmitted to the receiver 104 through the network 112 in a secured manner. The data security may be ensured based on a security technique selected by the user 118 or an administrator using a user device (not shown). In an embodiment, user devices (not shown) can include a variety of computing systems, including but not limited to, a smart phone, a laptop computer, a desktop computer, a notebook, a workstation, a portable computer, a personal digital assistant, a handheld or a mobile device. In an embodiment, the processing device 102 may be in-built into the user device.

[026] In an embodiment, the user 118 may be authenticated by the data processing device 102 based on input of one or more authentication information including user-name and password. In an embodiment, the user 118 may be provided access to the processing device 102 based on authorization of the inputted authentication information.

[027] The processing device 102 may include one or more processor(s) 108 and a memory 110. In an embodiment, examples of processor(s) 108 may include, but are not limited to, an Intel® Itanium® or Itanium 2 processor(s), or AMD® Opteron® or Athlon MP® processor(s), Motorola® lines of processors, FortiSOC™ system on a chip processors or other future processors. The memory 110 may store instructions that, when executed by the processor 108, cause the processor 108 to enable data security, as discussed in greater detail below. The memory 110 may be a non-volatile memory or a volatile memory. Examples of non-volatile memory may include, but are not limited to a flash memory, a Read Only Memory (ROM), a Programmable ROM (PROM), Erasable PROM (EPROM), and Electrically EPROM (EEPROM) memory. Examples of volatile memory may include but are not limited to Dynamic Random Access Memory (DRAM), and Static Random-Access memory (SRAM).

[028] In an embodiment, the communication network 112 may be a wired or a wireless network or a combination thereof. The network 112 can be implemented as one of the different types of networks, such as but not limited to, ethernetIP network, intranet, local area network (LAN), wide area network (WAN), the internet, Wi-Fi, LTE network, CDMA network, and the

like. Further, the network 112 can either be a dedicated network or a shared network. The shared network represents an association of the different types of networks that use a variety of protocols, for example, Hypertext Transfer Protocol (HTTP), Transmission Control Protocol/Internet Protocol (TCP/IP), Wireless Application Protocol (WAP), and the like, to communicate with one another. Further the network 112 can include a variety of network devices, including routers, bridges, servers, computing devices, storage devices, and the like. In an embodiment, the network 112 may support the data security using methodology of the current disclosure.

[029] In an embodiment, the data received from a data source such as a user device in form of voice signals may be received by an input/output device 106 of the processing device 102. In an embodiment, the processor 108 may modulate the received voice signals using a carrier signal.

[030] **FIG. 2** illustrates a functional block diagram of the processing device, in accordance with an embodiment of the present disclosure. Referring now to FIG. 2, a functional block diagram 200 of the processing device 102 comprises a Prime Number Frequency Generator module 202, a Frequency Set Generator module 204, a Pattern Set Generator Module 206, a Harmonic Signal Generator Module 208, a Decomposing Module 210, a Carrier Signal Module 212, a Binary Converting Module 214, a Matching Module 216 and an Encryption Key Generator Module 218.

[031] The Prime Number Frequency Generator module 202 may determine all the prime numbers in a range of natural numbers up to a pre-defined upper limit of natural number. The upper limit of natural number may be selected such that a harmonic signal (defined later) of a pre-defined harmonic ratio may be generated. The Frequency Set Generator module 204 may generate frequency sets comprising multiples of ten each comprising same number of prime numbers occurring in the preceding 9 natural numbers. In an embodiment, 5 frequency sets may be generated comprising multiples of ten, whose 9 preceding numbers comprises zero, one, two, three and four prime numbers. The Pattern Set Generator Module 206 is configured to generate a plurality of sequence of the frequency sets to generate a pattern set. The pattern set may comprise the values of the frequency set in the sequence selected. The Harmonic Signal Generator Module 208 may generate a harmonic signal for each pattern set of each sequence from the plurality of sequences. In an embodiment, a final sequence may be selected based on a noise level of the harmonic signals generated of each of the pattern sets for the plurality of

sequences. In an embodiment, a harmonic signal having a minimum noise level and its corresponding sequence pattern may be selected. The Decomposing Module 210 may produce decomposition signals of the harmonic signal using a decomposition techniques such as, but not limited to Hilbert technique. The Carrier Signal Module 212 may select a decomposition signal as the carrier signal based on a harmonic ratio of the decomposition signals. The decomposition having a harmonic ratio below a pre-defined threshold may be selected as the carrier signal. The Binary Converting Module 214 may convert the discrete values of the carrier signal to 8-bit binary data. The Matching Module 216 may determine instances of binary data in sequence of its occurrence which correspond to a Unicode for a character of a natural language such as mandarin, Sanskrit, hindi, etc. A combination of the characters may be used as an encryption key. The encryption key may comprise of 8 characters, 16 characters, 32 characters, 64 characters, 128 characters, or 256 characters. In an embodiment, an encryption key of 8 characters may correspond to 64 bit encryption. In an embodiment, the encryption key may be generated based on various patterns of the characters of the natural language based on a permutation and combination technique.

[032] **FIG. 3** is a flowchart 300 depicting a methodology of generating a carrier signal for modulating voice signals, in accordance with an embodiment of the present disclosure.

[033] **FIG. 4A** is an exemplary embodiment depicting configuration for the methodology of generating carrier signal as described in **FIG. 3**, in accordance with an embodiment of the present disclosure.

[034] At step 302, an upper limit of natural numbers is selected. In an embodiment, the upper limit may be pre-defined by the user 118. At step 304, a frequency of occurrence of prime numbers may be determined in nine consecutive natural numbers preceding each multiple of ten.

[035] In an exemplary embodiment, table 400 of **FIG. 4A** depicts prime numbers up to an upper limit of hundred natural numbers. Further, first column 302 depicts the multiple of ten in first hundred natural numbers and the rows 304 depicts the prime numbers occurring in 9 consecutive natural numbers preceding each multiple of 10 in the first hundred natural numbers. In an embodiment, the upper limit may be selected as any natural number for which a harmonic signal with a pre-defined harmonic ratio may be determined.

[036] At step 306, a set of frequency set may be created for each multiple of 10s in the selected upper limit. The frequency set may comprise a same frequency of occurrence of prime numbers. For example, a frequency set for ‘4’ prime numbers may include ‘10’ and ‘20’ since, since they comprise of ‘4’ prime numbers in the preceding nine consecutive natural numbers. Similarly, frequency sets 410 for 0, 1, 2 and 3 prime numbers may be determined as shown in **FIG**. **4B**.

[037] **FIG. 4B** shown an exemplary embodiment depicting frequency sets 410 of zero, one, two, three and four prime numbers for an upper limit of 1000 natural numbers as described in **FIG. 3**, in accordance with an embodiment of the present disclosure.

[038] At step 308, a pattern set may be generated comprising a repetition of a sequence pattern comprising multiples of ten from each of the set of frequency sets 410. The sequence pattern may comprise of a pre-defined order of the set of frequency sets as shown in **FIG. 5**.

[039] As shown in **FIG. 5**, an exemplary embodiment depicting a sequence pattern and a pattern set is provided, in accordance with an embodiment of the present disclosure. The sequence pattern 502 depicts an exemplary sequence pattern based on the set of frequency sets of prime numbers. In an embodiment, the sequence pattern may be created based on any one of the various permutation and combination of the set of frequency sets for frequency of 0 to 4 prime numbers other than as shown in 502.

[040] In an embodiment, a pattern set 504 may be generated based on the values of the set of frequency sets in accordance with the selected sequence pattern.

[041] At step 310, a harmonic signal of the pattern set 504 may be generated by performing an Inverse Fast Fourier Transform (IFT) of the pattern set 504. In an embodiment, the harmonic signal may be generated by using digital signal processing software such as, but not limited to, MATLAB, etc.

[042] **FIG. 6A** discloses a harmonic signal 600 generated by performing IFT on the pattern set 504 of **FIG. 5**, in accordance with an embodiment of the present disclosure. In an embodiment, the harmonic signal 600 may have a frequency sample range of 1000 Hz and 24 bits.

[043] At step 312, the harmonic signal 600 may be decomposed into plurality of decomposition signals and a de-noise signal. The plurality of decomposition signals may be generated by using digital signal processing software such as, but not limited to, MATLAB, etc.

[044] **FIG. 6B** illustrates decomposition signals 602 of the harmonic signal 600 as shown in **FIG. 6A**, in accordance with an embodiment of the current disclosure. In an embodiment, the harmonic signal 600 may be decomposed by using digital signal processing software such as, but not limited to, MATLAB, etc. In an embodiment, the harmonic signal 600 may be decomposed using decomposition techniques, such as but not limited to, Hilbert technique. Further, the decomposition may be performed based on user defined parameters such as, but not limited to, a number of decomposition levels, a type of wavelet, level of decomposition, etc.

[045] At step 314, a decomposition signal from the plurality of decomposition signals 610 generated in step 312 may be selected as a carrier signal. The decomposition signal having a harmonic ratio less than a pre-defined threshold level may be selected as a carrier signal. The selected carrier signal may be used for the modulation of the voice signals from the user 118 for transmission by the transmitter 114 by using a modulator device (not shown). In an embodiment, frequency modulation may be performed to modulate the carrier signal in accordance with the voice signals for transmission. In an exemplary embodiment, the decomposition signal ‘d9’ 602 may be selected as the carrier signal as it may be determined to have a harmonic ratio less than the pre-defined threshold level. **FIG. 6C** depicts the ‘d9’ 602 signal selected as the carrier signal as described in **FIG. 3**, in accordance with an embodiment of the present disclosure. The carrier signal thus generated may be modulated in accordance with the voice signals received from the user 118 using a modulation technique such as frequency modulation by a modulator and transmitted by the transmitter 114 to the receiver 104. In an embodiment, the transmitter 114 and the receiver 104 used may be configured to transmit the modulated voice signals.

[046] **FIG. 7** is a flowchart 700 depicting a methodology of generating encryption keys for encryption in continuation to the methodology described in **FIG. 3**, in accordance with an embodiment of the present disclosure.

[047] In continuation with the steps 302 to 312 as shown in **FIG. 3**, at step 702, discrete decimal data of at least one of the decomposition signals may be determined.

[048] At step 704, the discrete decimal data may be converted into binary data of pre-defined bit number. In an embodiment, the size of the binary data may be, but not limited to, 8 bit, 16 bit, 32 bit, 64 bit, 128 bit or 256 bits. In an embodiment, the discrete decimal data may be converted to binary using a known in the art techniques.

[049] At step 706, the binary data may be compared with a Unicode for a pre-defined natural language in precedence of their occurrence. **FIG. 8A** shows a table 800 of binary data generated for the discrete decimal data of the decomposition signal selected in accordance with an embodiment of the present disclosure.

[050] At step 708, characters of the natural language which correspond to the Unicode based on the match with the binary data may be determined. An encryption key may be generated based on the characters selected based on the match. In an embodiment, a random combination of the characters may be created in order to generate the encryption key. In an embodiment, an encryption key may be generated comprising of 8 characters, 16 characters, 32 characters, 64 characters, 128 characters, or 256 characters.

[051] **FIG. 8B** shows an exemplary encryption key generated using the binary data, in accordance with an embodiment of the present disclosure. In an embodiment, 802 depicts an encryption key from the binary data 800 that corresponds to Unicode of a natural language. In an example, row 3 and row 4 corresponds to a mandarin language character. In an embodiment, the encryption key 802 may be used to encrypt any data such as voice data of the user 118 using an encryptor to transmit the encrypted data from the transmitter 114 to the receiver 104 through the network 112.

[052] **FIG. 9** is a flowchart of a method of creating a carrier signal and an encryption key, in accordance with an embodiment of the present disclosure.

[053] At step 902, a frequency of occurrence of prime numbers in 9 consecutive natural numbers preceding each multiple of 10 for up to a pre-configured upper limit of natural numbers may be determined. At step 904, a set of frequency sets may be created for the multiples of 10, wherein each of the frequency set may comprise a same frequency of occurrence of prime numbers. A pattern set may be determined comprising a repetition of a sequence pattern, wherein the sequence pattern may comprise of multiples of 10 from each of the set of frequency sets in a pre-defined order. At step 906, a harmonic signal may be generated by applying an Inverse Fast Fourier Transform (IFT) on the pattern set generated at step 904. At step 908, the harmonic signal

generated may be decomposed into a plurality of decomposition signals. At step 910, a carrier signal may be generated based on at least one of the plurality of decomposition signals generated at step 908. At step 912, an encryption key may be generated based on at least one of the plurality of decomposition signals generated at step 908.

[054] It is intended that the disclosure and examples be considered as exemplary only, with a true scope of disclosed embodiments being indicated by the following claims.

WE CLAIM:

1. A method of generating carrier signals, the method comprising:

determining, by a modulator, a frequency of occurrence of prime numbers in 9 consecutive natural numbers preceding each multiple of 10 for up to a pre-configured upper limit of natural numbers;

generating, by the modulator, a pattern set comprising a repetition of a sequence pattern, wherein the sequence pattern comprises multiples of 10 from each of the set of frequency sets in a pre-defined order;

generating, by the modulator, a harmonic signal by applying an Inverse Fast Fourier Transform (IFT) on the pattern set;

decomposing, by the modulator, the harmonic signal into a plurality of decomposition signals; and

generating, by the modulator device, a carrier signal based on at least one of the plurality of decomposition signals.

2. The method as claimed in claim 1, wherein the pre-configured upper limit of natural number is a multiple of 10 and is selected to include prime numbers in order of at least 1,000.

3. The method as claimed in claim 1, wherein the set of frequency sets comprises 5 frequency sets, and wherein each of the frequency set comprises a frequency of occurrence of prime numbers in a range of 0 to 4.

4. The method as claimed in claim 1, further comprising modulating, by the modulator, the carrier signal to carry an information.

5. The method as claimed in claim 1, wherein generating the carrier signal further comprises selecting one of the plurality of the decomposition signal based on its harmonic ratio.

6. A method of generating encryption keys, the method comprising:

determining, by an encrypting device, a frequency of occurrence of prime numbers in 9 consecutive natural numbers preceding each multiple of 10 for up to a pre-configured upper limit of natural number;

creating, by the encrypting device, a set of frequency sets for the multiples of 10, wherein each of the frequency set comprises a same frequency of occurrence of prime numbers;

generating, by the encrypting device, a pattern set comprising a repetition of a sequence pattern, wherein the sequence pattern comprises multiples of 10 from each of the set of frequency sets in a pre-defined order;

generating, by the encrypting device, a harmonic signal by applying an Inverse Fast Fourier Transform (IFT) on the pattern set;

decomposing, by the encrypting device, the harmonic signal into a plurality of decomposition signals; and

generating, by the encrypting device, an encryption key based on based on at least one of the plurality of decomposition signals.

7. The method as claimed in claim 6, wherein generating the encryption key further comprises selecting one of the plurality of the decomposition signal based on its harmonic ratio.

8. The method as claimed in claim 6, wherein generating the encryption key further comprises:

determining, by the encrypting device, discrete decimal data based on the at least one of the plurality of decomposition signals;

converting, by the encrypting device, the discrete decimal data into a pre-defined binary data;

generating, by the encrypting device, the encryption key based on the pre-define binary data.

9. The method as claimed in claim 8, wherein the pre-define binary data comprises one of 8-bit binary data, 16-bit-binary data, 32-bit binary data, 64-bit binary data, 128-bit binary data, or 256-bit binary data.

10. The method as claimed in claim 8, wherein generating the encryption key further comprises:

matching each value in the pre-define binary data, in a sequence of occurrence, against a Unicode for each of a plurality of characters of a pre-defined natural language;

selecting a set of characters of the plurality of characters based on the match;

generating the encryption key based on the set of characters.

11. The method as claimed in claim 10, wherein the set of characters comprises one of 8 characters, 16 characters, 32 characters, 64 characters, 128 characters, or 256 characters.

12. The method as claimed in claim 6, further comprises encrypting, by the encrypting device, an information using the encryption key.

13. A system for creating carrier signals, comprising:

one or more processors;

a memory communicatively coupled to the processors, wherein the memory stores a plurality of processor-executable instructions, which, upon execution, cause the processors to:

determine a frequency of occurrence of prime numbers in 9 consecutive natural numbers preceding each multiple of 10 for up to a pre-configured upper limit of natural numbers;

create a set of frequency sets for the multiples of 10, wherein each of the frequency set comprises a same frequency of occurrence of prime numbers;

generate a pattern set comprising a repetition of a sequence pattern, wherein the sequence pattern comprises multiples of 10 from each of the set of frequency sets in a pre-defined order;

generate a harmonic signal by applying an Inverse Fast Fourier Transform (IFT) on the pattern set;

decompose the harmonic signal into a plurality of decomposition signals; and

generate a carrier signal based on at least one of the plurality of decomposition signals.

14. The system as claimed in claim 13, wherein the pre-configured upper limit of natural number is a multiple of 10 and is selected to include prime numbers in order of at least 1,000.

15. The system as claimed in claim 13, wherein the set of frequency sets comprises 5 frequency sets, and wherein each of the frequency set comprises a frequency of occurrence of prime numbers in a range of 0 to 4.

16. The system as claimed in claim 13, wherein the one or more processors are further configured to modulate the carrier signal to carry an information.

17. The system as claimed in claim 13, wherein the generation of the carrier signal is based on a selection of one of the plurality of the decomposition signal based on its harmonic ratio.

18. A system for generating encryption keys, comprising:

one or more processors;

a memory communicatively coupled to the processors, wherein the memory stores a plurality of processor-executable instructions, which, upon execution, cause the processors to:

determine a frequency of occurrence of prime numbers in 9 consecutive natural numbers preceding each multiple of 10 for up to a pre-configured upper limit of natural number;

create a set of frequency sets for the multiples of 10, wherein each of the frequency set comprises a same frequency of occurrence of prime numbers;

generate a pattern set comprising a repetition of a sequence pattern, wherein the sequence pattern comprises multiples of 10 from each of the set of frequency sets in a pre-defined order;

generate a harmonic signal by applying an Inverse Fast Fourier Transform (IFT) on the pattern set;

decompose the harmonic signal into a plurality of decomposition signals; and

generate, an encryption key based on based on at least one of the plurality of decomposition signals.

19. The system as claimed in claim 18, wherein generation the encryption key is based on selection of one of the plurality of the decomposition signal based on its harmonic ratio.

20. The system as claimed in claim 18, wherein generation of the encryption key further comprises:

determining a discrete decimal data based on the at least one of the plurality of decomposition signals;

converting the discrete decimal data into a pre-defined binary data; and

generating the encryption key based on the pre-define binary data.

Dated this 24th day of November 2022

-- Digitally Signed--
Bhanu Prasad
(INPA No: **3253**)
Manager, IPR Dept.,
L&T Technology Services Limited,
DLF 3rd Block, 2nd Floor,
Manapakkam, Chennai - 600089.

ABSTRACT

METHOD AND SYSTEM FOR GENERATING CARRIER SIGNALS AND ENCRYPTION KEYS

A method and system of generating carrier signals and encryption keys is disclosed that includes determining, by a processor, a frequency of occurrence of prime numbers in 9 consecutive natural numbers preceding each multiple of 10 for up to a pre-configured upper limit of natural numbers. A set of frequency sets are created for the multiples of 10, wherein each frequency set comprises a same frequency of occurrence of prime numbers. A pattern set is determined comprising a repetition of a sequence pattern, wherein the sequence pattern comprises multiples of 10 from each of the set of frequency sets in a pre-defined order. A harmonic signal is generated by applying an Inverse Fast Fourier Transform on the pattern set. The harmonic signal generated is decomposed into a plurality of decomposition signals. Carrier signal and an encryption key are generated based on at least one of the plurality of decomposition signals.

[To be published with FIG. 1]

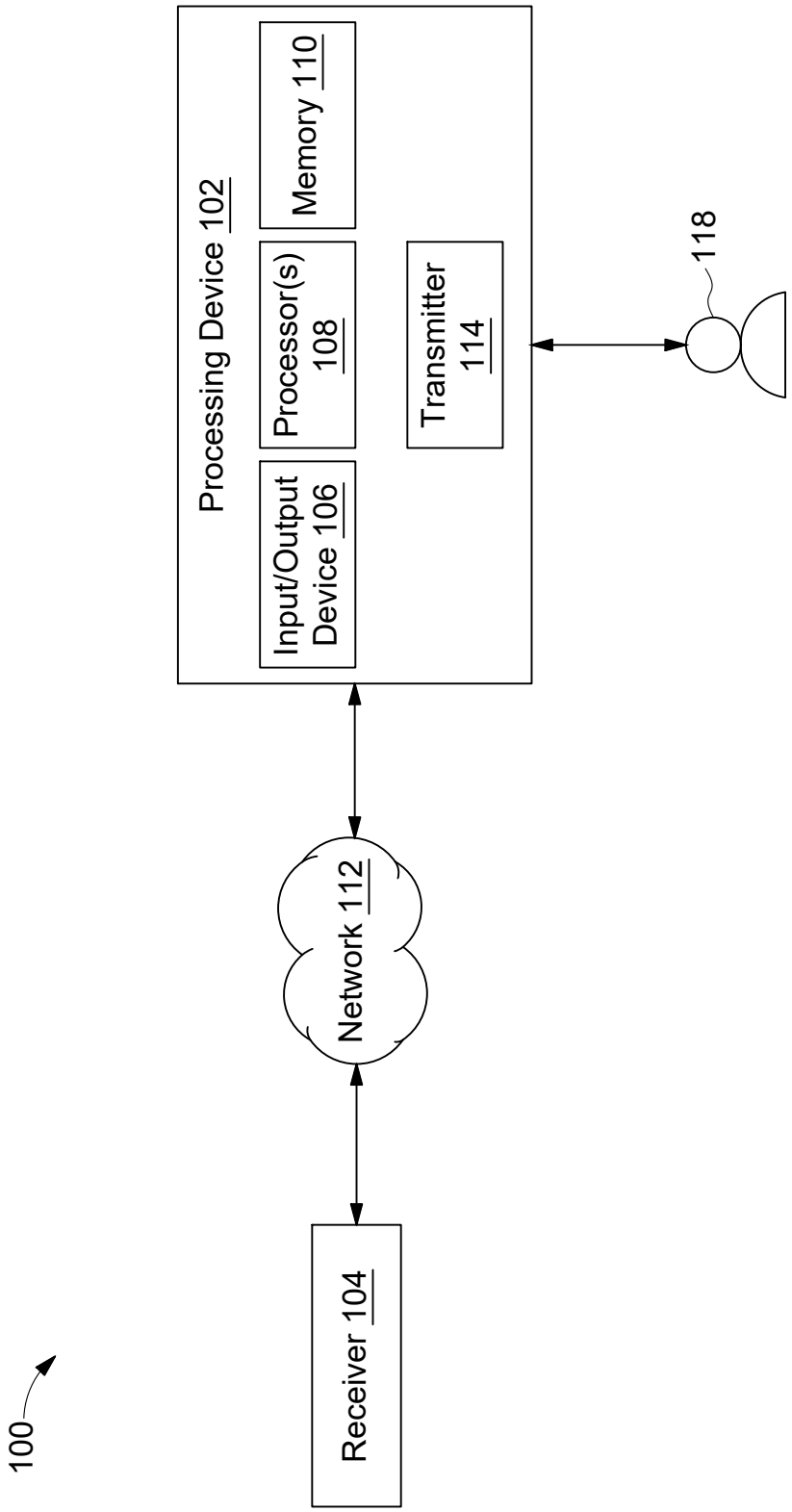


FIG. 1

-- Digitally Signed--
Bhanu Prasad
(INPA No: 3253)
Manager, IPR Dept.,
L&T Technology Services Limited,
DLF 3rd Block, 2nd Floor,
Manapakkam, Chennai - 600089.

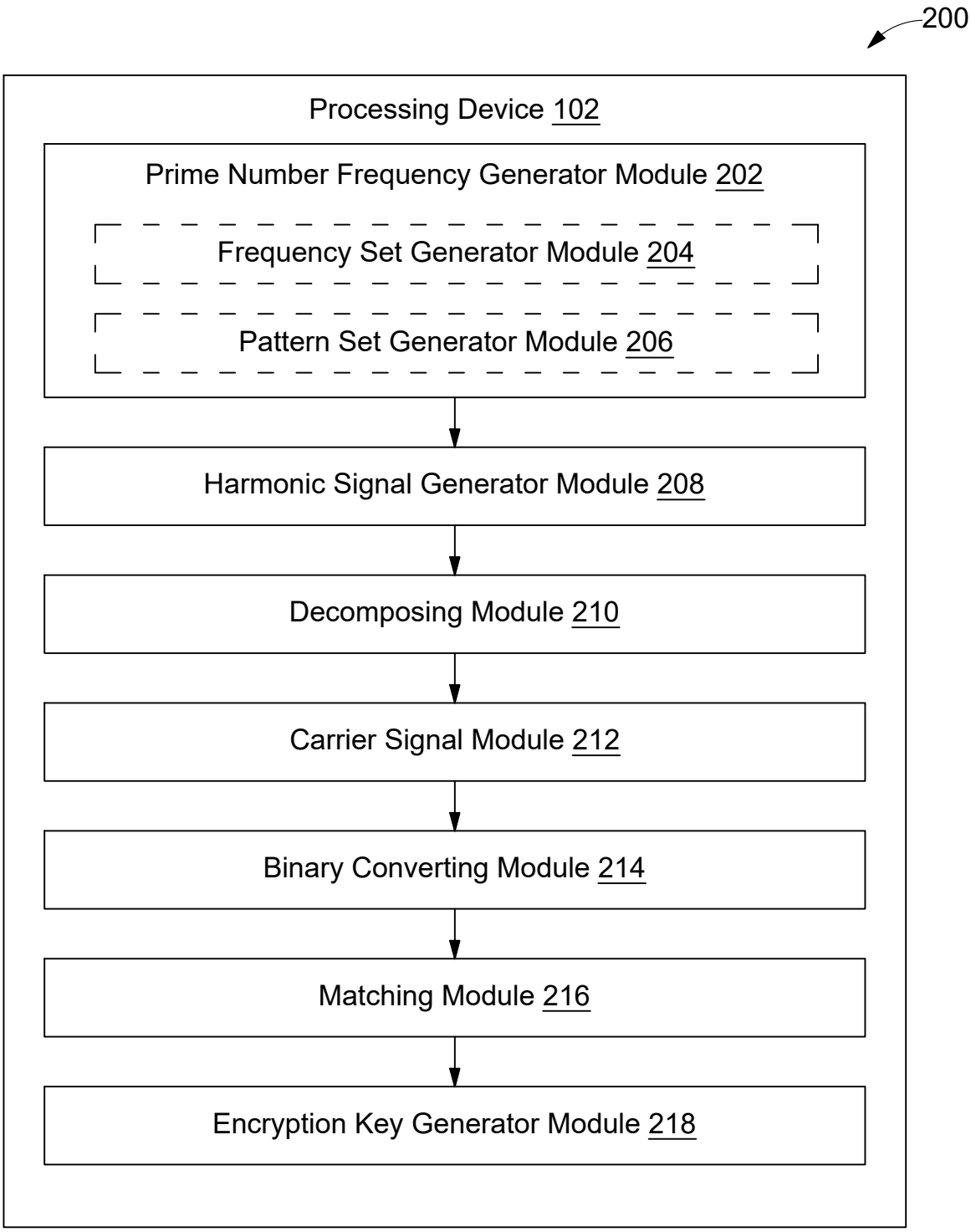


FIG. 2

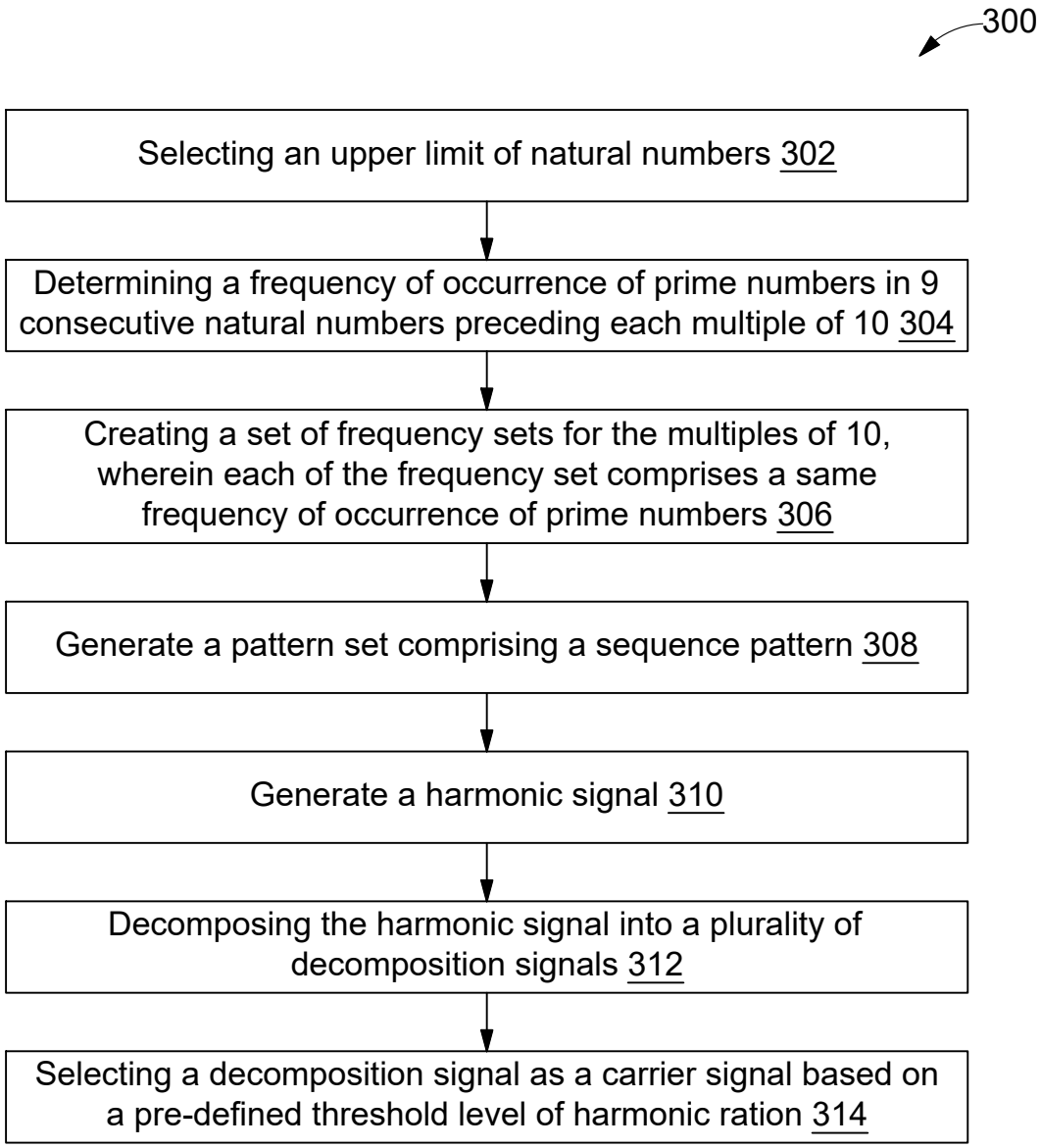


FIG. 3

-- Digitally Signed--
Bhanu Prasad
(INPA No: 3253)
Manager, IPR Dept.,
L&T Technology Services Limited,
DLF 3rd Block, 2nd Floor,
Manapakkam, Chennai - 600089.

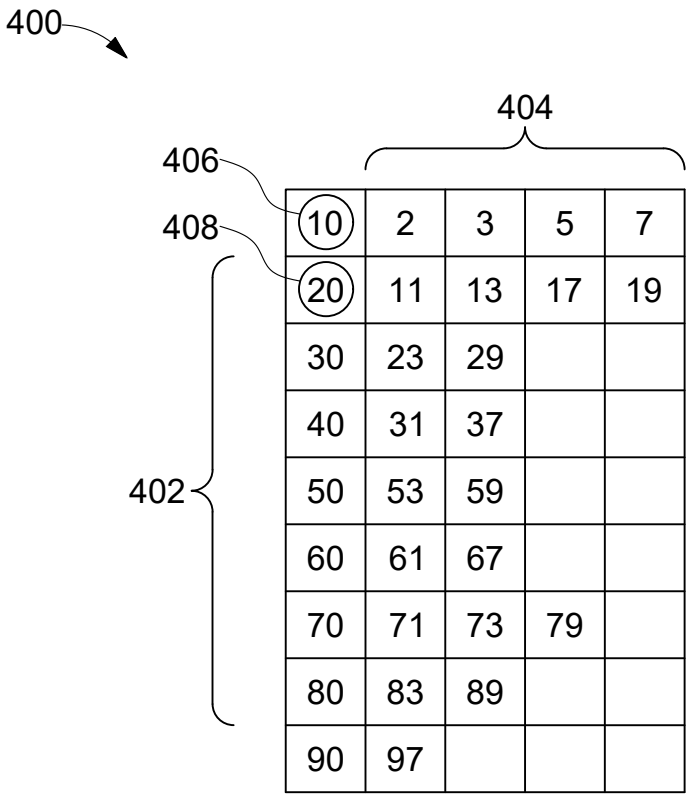


FIG. 4A

-- Digitally Signed--
Bhanu Prasad
(INPA No: 3253)
Manager, IPR Dept.,
L&T Technology Services Limited,
DLF 3rd Block, 2nd Floor,
Manapakkam, Chennai - 600089.

410

- frequency set of four prime numbers: [10, 20, 110, 200, 830]
- frequency set of three prime numbers: [50, 80, 140, 230, 320, 440, 470, 620, 650, 860, 890]
- frequency set of two prime numbers: [30, 40, 60, 70, 90, 160, 170, 180, 240, 260, 270, 280, 290, 340, 350, 360, 380, 390, 410, 450, 500, 510, 530, 550, 570, 580, 600, 610, 660, 680, 710, 740, 760, 770, 920, 950, 980, 1000]
- frequency set of one prime number: [100, 120, 130, 150, 190, 220, 250, 300, 310, 370, 400, 420, 430, 460, 480, 490, 560, 590, 640, 670, 690, 700, 720, 730, 750, 780, 790, 800, 810, 820, 840, 870, 880, 910, 930, 940, 960, 970, 990]
- frequency set of zero prime number: [210, 330, 520, 540, 630, 850, 900]

FIG. 4B

-- Digitally Signed--
Bhanu Prasad
(INPA No: 3253)
Manager, IPR Dept.,
L&T Technology Services Limited,
DLF 3rd Block, 2nd Floor,
Manapakkam, Chennai - 600089.

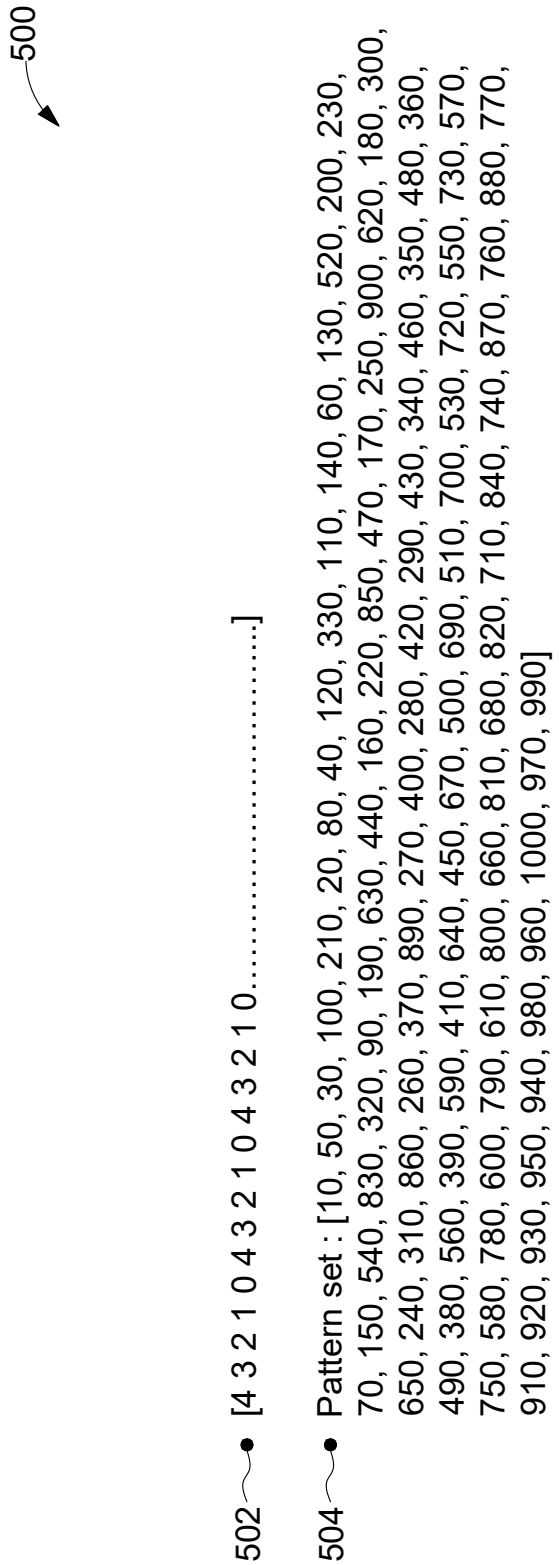


FIG. 5

-- Digitally Signed--
Bhanu Prasad
(INPA No: 3253)
Manager, IPR Dept.,
L&T Technology Services Limited,
DLF 3rd Block, 2nd Floor,
Manapakkam, Chennai - 600089.

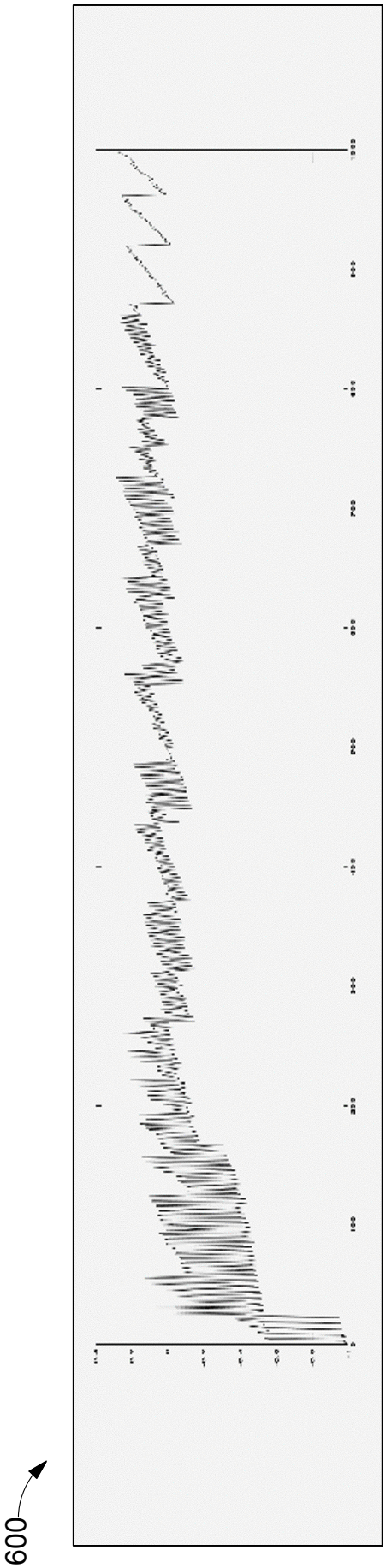


FIG. 6A

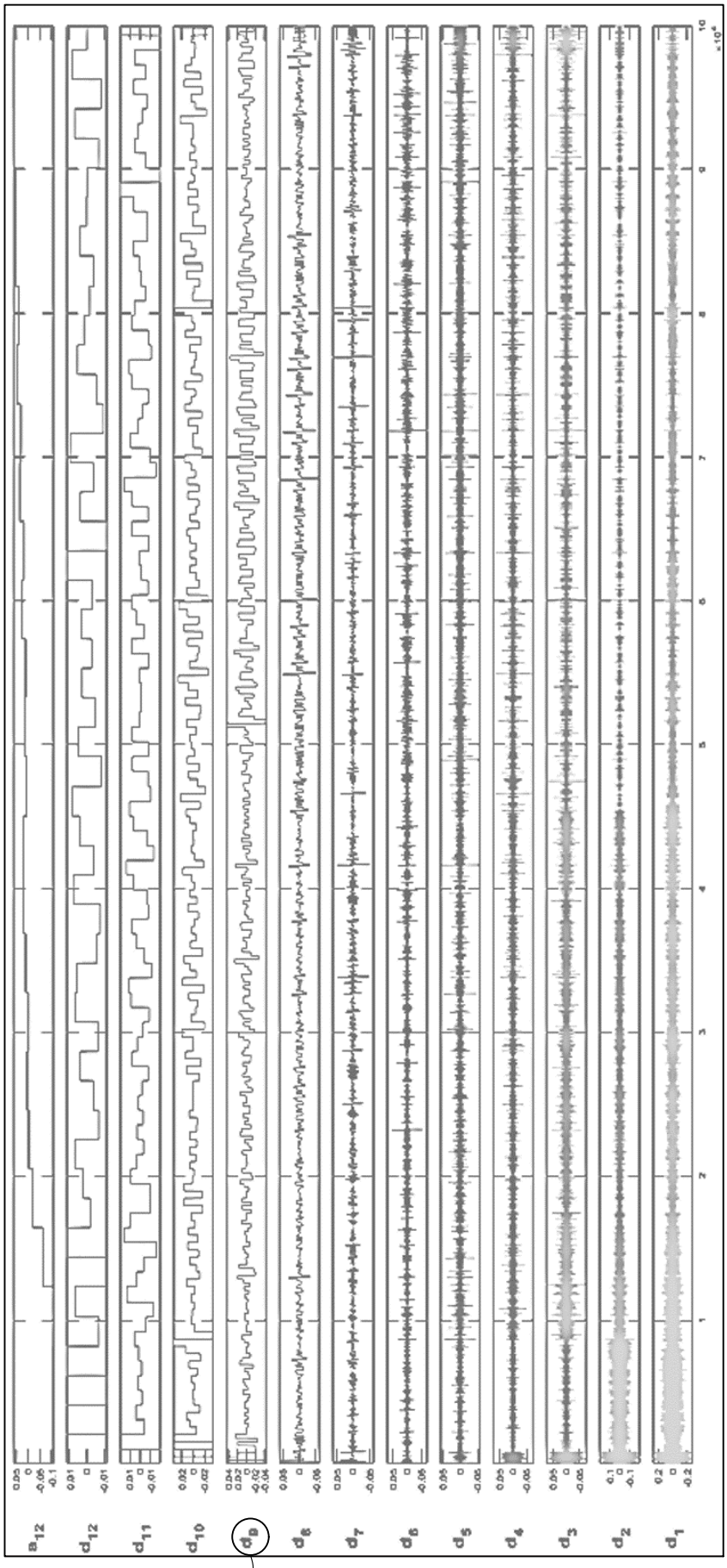


FIG. 6B

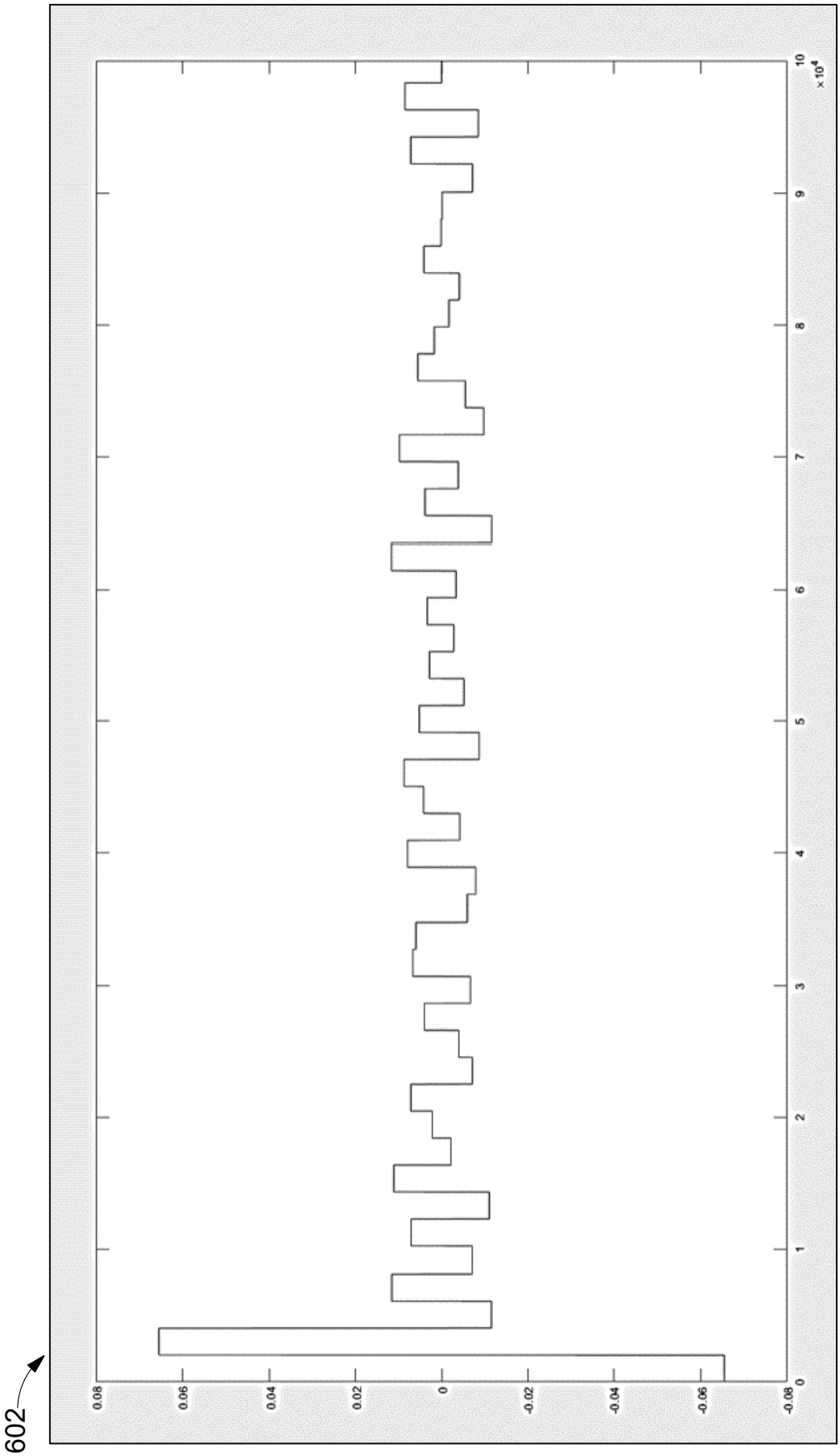


FIG. 6C

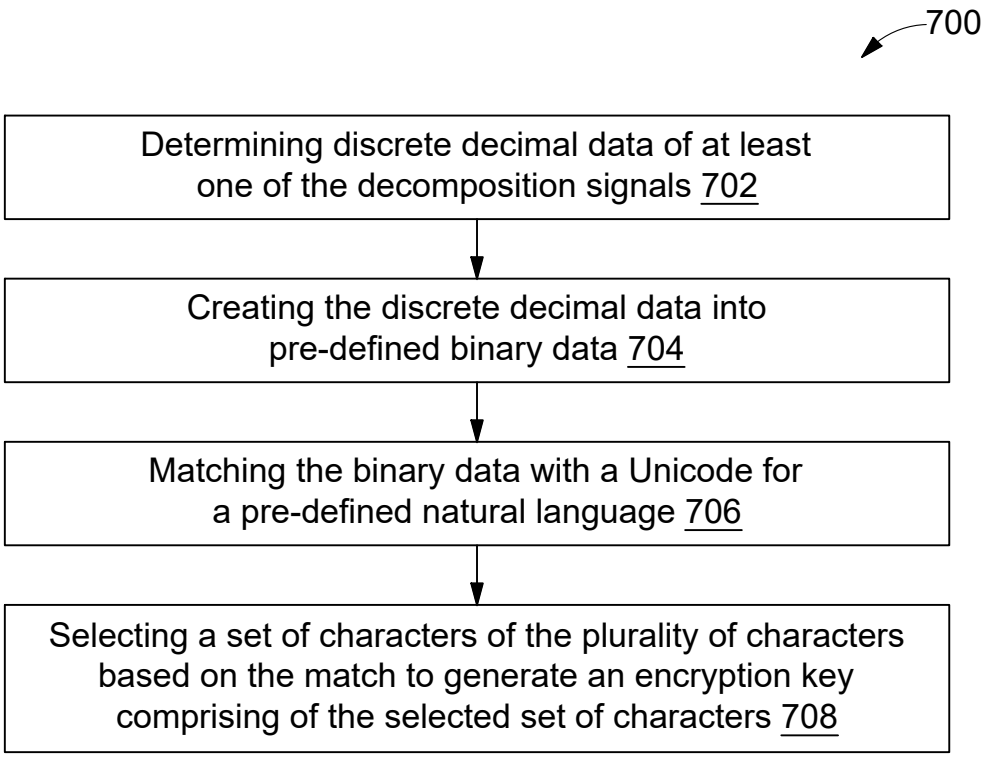
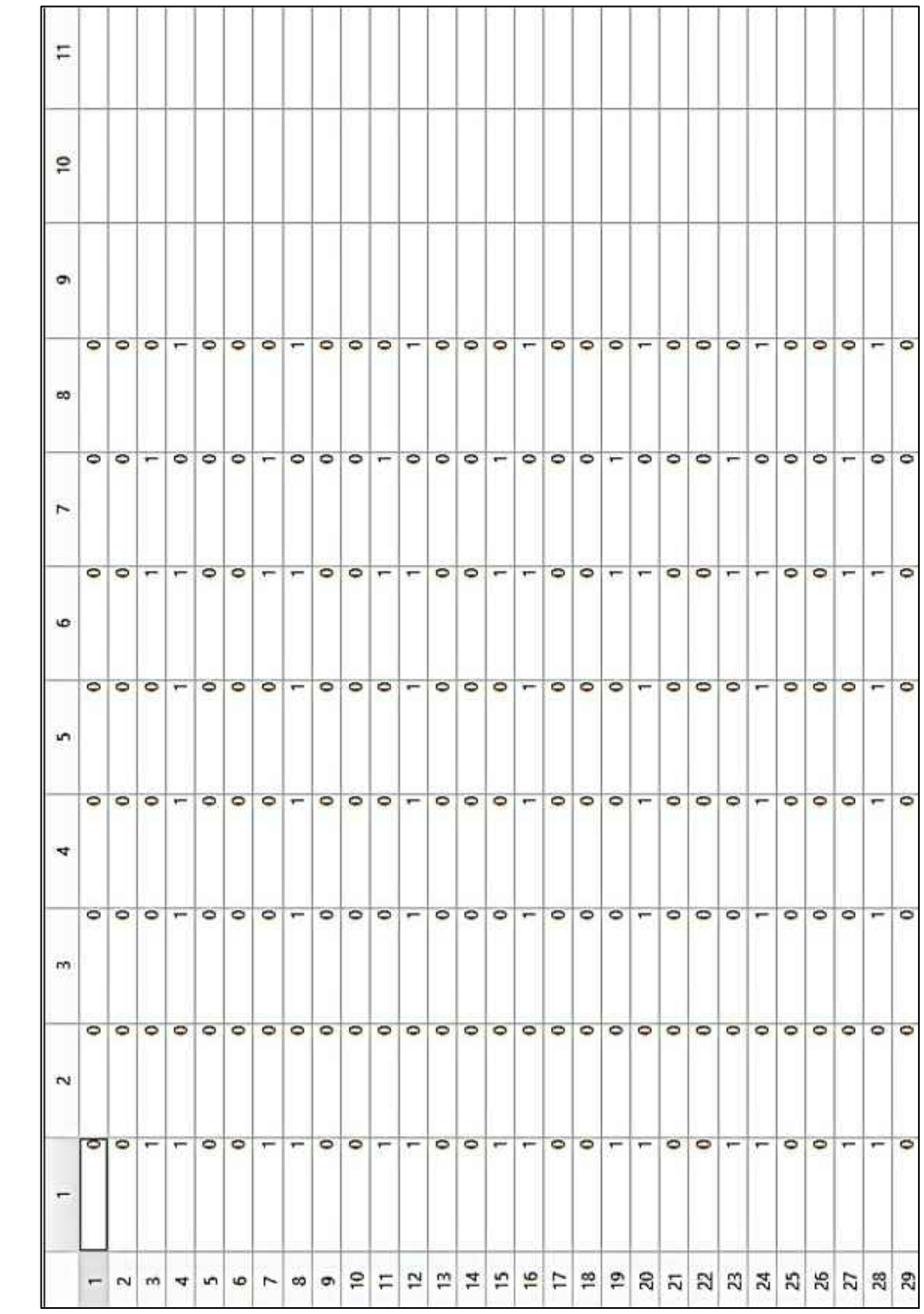


FIG. 7



	1	2	3	4	5	6	7	8	9	10	11
1	0	0	0	0	0	0	0	0			
2	0	0	0	0	0	0	0	0			
3	1	0	0	0	0	1	1	0			
4	1	0	1	1	1	1	0	1			
5	0	0	0	0	0	0	0	0			
6	0	0	0	0	0	0	0	0			
7	1	0	0	0	0	1	1	0			
8	1	0	1	1	1	1	0	1			
9	0	0	0	0	0	0	0	0			
10	0	0	0	0	0	0	0	0			
11	1	0	0	0	0	1	1	0			
12	1	0	1	1	1	1	0	1			
13	0	0	0	0	0	0	0	0			
14	0	0	0	0	0	0	0	0			
15	1	0	0	0	0	1	1	0			
16	1	0	1	1	1	1	0	1			
17	0	0	0	0	0	0	0	0			
18	0	0	0	0	0	0	0	0			
19	1	0	0	0	0	1	1	0			
20	1	0	1	1	1	1	0	1			
21	0	0	0	0	0	0	0	0			
22	0	0	0	0	0	0	0	0			
23	1	0	0	0	0	1	1	0			
24	1	0	1	1	1	1	0	1			
25	0	0	0	0	0	0	0	0			
26	0	0	0	0	0	0	0	0			
27	1	0	0	0	0	1	1	0			
28	1	0	1	1	1	1	0	1			
29	0	0	0	0	0	0	0	0			

800

FIG. 8A

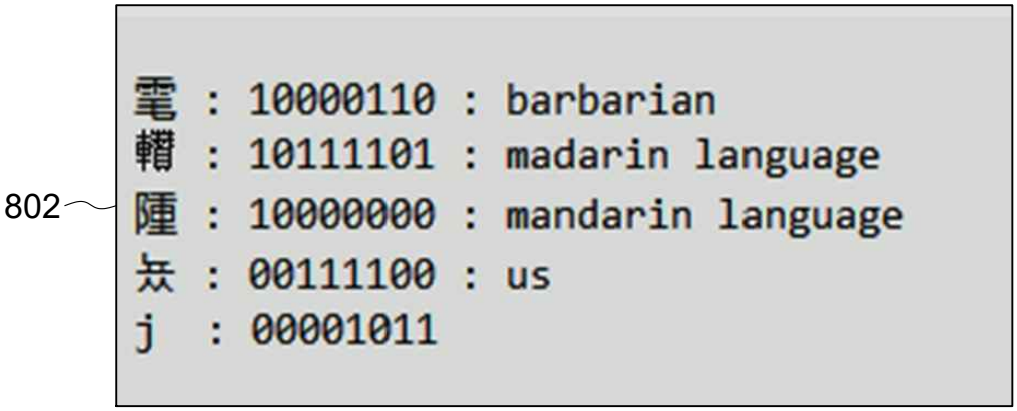


FIG. 8B

-- Digitally Signed--
Bhanu Prasad
(INPA No: 3253)
Manager, IPR Dept.,
L&T Technology Services Limited,
DLF 3rd Block, 2nd Floor,
Manapakkam, Chennai - 600089.

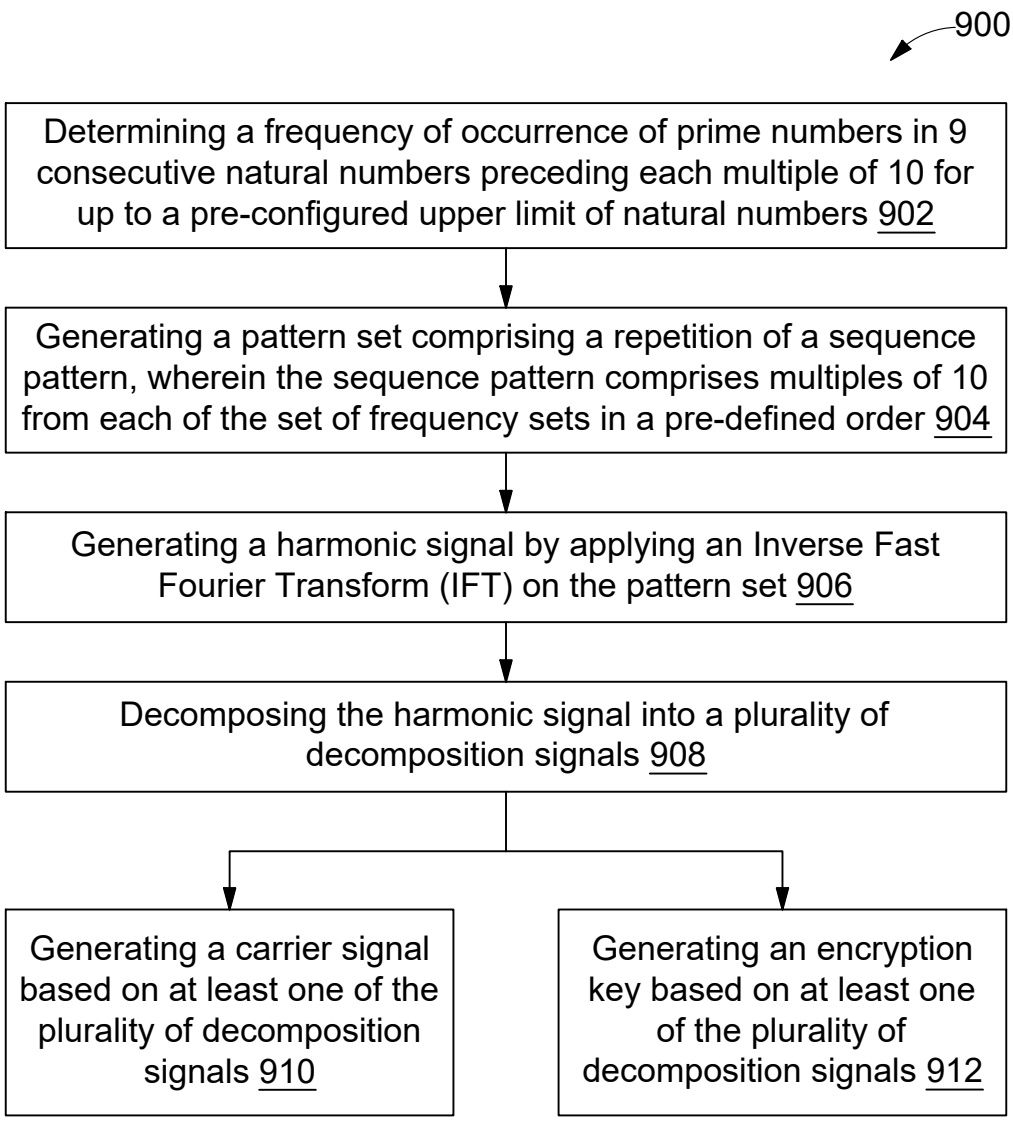


FIG. 9