(12) STANDARD PATENT (11) Application No. **AU 2021436355 B2**
(19) AUSTRALIAN PATENT OFFICE

(54) Title
Secure search method, system thereof, apparatus thereof, encryption apparatus, searcher terminal, and program

(51) International Patent Classification(s)
G09C 1/00 (2006.01)

(21) Application No: **2021436355** (22) Date of Filing: **2021.03.22**

(87) WIPO No: **WO22/201234**

(43) Publication Date: **2022.09.29**
(44) Accepted Journal Date: **2024.11.14**

(71) Applicant(s)
NIPPON TELEGRAPH AND TELEPHONE CORPORATION

(72) Inventor(s)
TAKAHASHI, Satoshi;CHIDA, Koji;HAMADA, Koki;ICHIKAWA, Atsunori

(74) Agent / Attorney
Griffith Hack, Level 15, 376-390 Collins Street, Melbourne, VIC, 3000, AU

(56) Related Art
WO 2016/203555 A1
JP 2017175244 A
JP 2016012111 A
JP 2017111793 A
CN 107220343 B

(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2022年9月29日(29.09.2022)

WIPO | PCT

(10) 国際公開番号
WO 2022/201234 A1

(51) 国際特許分類:
G09C 1/00 (2006.01)

(21) 国際出願番号： PCT/JP2021/011663

(22) 国際出願日： 2021年3月22日(22.03.2021)

(25) 国際出願の言語： 日本語

(26) 国際公開の言語： 日本語

(71) 出願人: 日本電信電話株式会社 (**NIPPON TELEGRAPH AND TELEPHONE CORPORATION**) [JP/JP]; 〒1008116 東京都千代田区大手町一丁目５番１号 Tokyo (JP).

(72) 発明者: 高橋 慧 (**TAKAHASHI, Satoshi**); 〒1808585 東京都武蔵野市緑町三丁目９番１１号 ＮＴＴ 知的財産センタ内 Tokyo (JP). 千田 浩司(**CHIDA, Koji**); 〒1808585 東京都武蔵野市緑町三丁目９番１１号 ＮＴＴ 知的財産センタ内 Tokyo (JP). 濱田 浩気(**HAMADA, Koki**); 〒1808585 東京都武蔵野市緑町三丁目９番１１号 ＮＴＴ 知的財産センタ内 Tokyo (JP). 市川 敦謙(**ICHIKAWA, Atsunori**); 〒1808585 東京都武蔵野市緑町三丁目９番１１号 ＮＴＴ 知的財産センタ内 Tokyo (JP).

(74) 代理人: 中尾 直樹, 外 (**NAKAO, Naoki** et al.); 〒1600022 東京都新宿区新宿三丁目１番２２号 新宿ＮＳＯビル６階 Tokyo (JP).

(81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ,

(54) **Title:** SECURE SEARCH METHOD, SECURE SEARCH SYSTEM, SECURE SEARCH DEVICE, ENCRYPTION DEVICE, SEARCHER TERMINAL, AND PROGRAM

(54) 発明の名称： 秘密検索方法、秘密検索システム、秘密検索装置、暗号化装置、検索者端末、およびプログラム

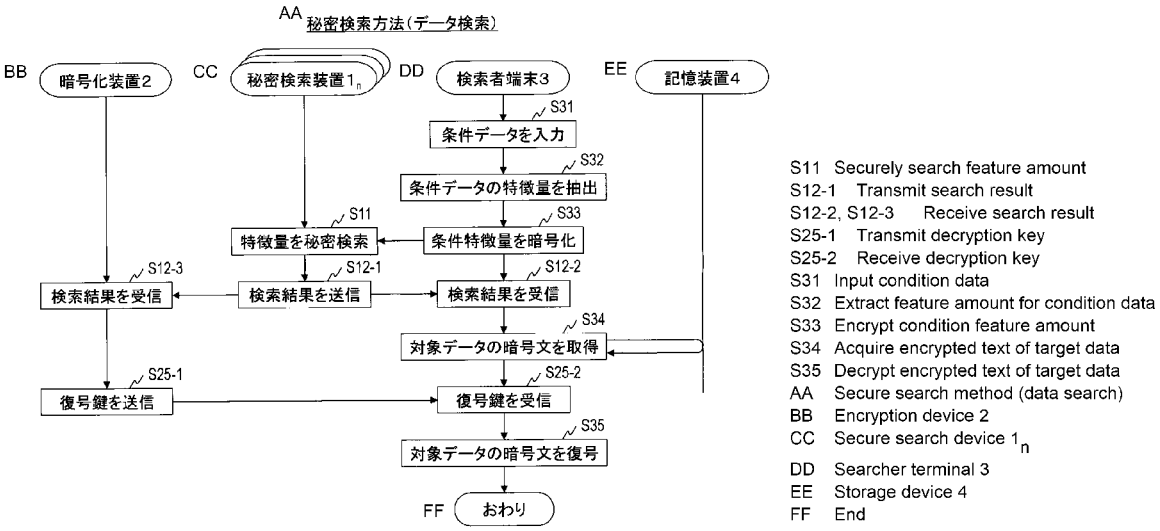

図6

(57) **Abstract:** The present invention efficiently performs a data search using secure computation, and safely provides the searched data. A searcher terminal (3) acquires condition data (S31). The searcher terminal (3) extracts a feature amount from the condition data (S32). The searcher terminal (3) encrypts the feature amount of the condition data (S33). A secure search device (1_n) acquires a search result indicating encrypted text of target data corresponding to the feature amount of target data similar to the feature amount of the condition data, while keeping the feature amount of the target data and the feature amount of the condition data secret (S11). The secure search device (1_n) transmits the search result to the encryption device (2) and the searcher terminal (3)

WO 2022/201234 A1

[続葉有]

BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類：

— 国際調査報告（条約第21条(3)）

(S13-1). The searcher terminal (3) acquires the encrypted text of the target data indicated by the search result (S34). The encryption device (2) transmits a decryption key to the searcher terminal (3) (S25-1). The searcher terminal (3) decrypts the encrypted text of the target data using the decryption key (S35).

(57) 要約：秘密計算によるデータ検索を効率的に行い、かつ、検索されたデータを安全に提供する。検索者端末（３）は、条件データを取得する（Ｓ３１）。検索者端末（３）は、条件データから特徴量を抽出する（Ｓ３２）。検索者端末（３）は、条件データの特徴量を暗号化する（Ｓ３３）。秘密検索装置（1_n）は、対象データの特徴量と条件データの特徴量を秘匿したまま、条件データの特徴量に類似する対象データの特徴量に対応する対象データの暗号文を示す検索結果を取得する（Ｓ１１）。秘密検索装置（1_n）は、検索結果を暗号化装置（２）と検索者端末（３）へ送信する（Ｓ１３－１）。検索者端末（３）は、検索結果が示す対象データの暗号文を取得する（Ｓ３４）。暗号化装置（２）は、復号鍵を検索者端末（３）へ送信する（Ｓ２５－１）。検索者端末（３）は、復号鍵を用いて対象データの暗号文を復号する（Ｓ３５）。

SECURE SEARCH METHOD, SYSTEM THEREOF, APPARATUS THEREOF, ENCRYPTION APPARATUS, SEARCHER TERMINAL, AND PROGRAM

TECHNICAL FIELD

[0001]

The present invention relates to a secure computation technology, and more particularly, to a technology for searching data similar to search condition data while keeping search target data secret.

BACKGROUND ART

[0002]

In recent years, surveillance cameras and Internet of Things (IoT) technologies have become widespread, and a large amount of private data such as surveillance camera videos are accumulated. By applying an image search technology, it is possible to extract image data similar to image data input as a search condition from the accumulated surveillance camera videos. Such a technology is expected to be utilized in various fields such as access and exit management to and from facilities and information provision to an investigative agency when an incident or an accident occurs. However, the image data to be searched is the record of personal life, and needs to be appropriately managed so that leakage of private data does not occur.

[0003]

Assuming the usage as described above, it is natural to apply a secure computation technology as a search technology while securing confidentiality of data. Patent Literature 1 discloses a technology in which features of a visitor extracted from a surveillance camera video or the like is kept secret by secret sharing or the like, and the secrecy information is searched to verify a visitor.

PATENT LITERATURE

[0004]

Patent Literature 1: JP 2016-71639 A

[0004a]

It is to be understood that if any prior art publication is referred to herein, such reference does not constitute an admission that the publication forms a part of the common general knowledge in the art, in Australia or any other country.

SUMMARY OF THE INVENTION

[0005]

However, in case a secure computation technology is applied, it takes enormous computation cost to directly input image data and perform search by secure computation, which is not realistic. In addition, the conventional technology disclosed in Patent Literature 1 only outputs a

2021436355 17 Oct 2024

collation result, and cannot safely provide original image data to a user.

[0006]

In view of the above technical problems, it would be desirable to efficiently perform data search by secure computation and to safely provide retrieved data.

[0007]

A secure search method according to an aspect of the present invention is a secure search method performed by a secure search system including at least one secure search apparatus, an encryption apparatus, and a searcher terminal, the secure search method including: encrypting target features extracted by converting target data that is a search target by a target feature encryption unit of the encryption apparatus; encrypting the target data by a target data encryption unit of the encryption apparatus; encrypting a condition feature extracted by converting condition data that is a search condition, by a condition feature encryption unit of the searcher terminal; acquiring a search result indicating a ciphertext of target data corresponding to a target feature having a close Euclidean distance to the condition feature while keeping the target features and the condition feature secret using ciphertexts of the target features and a ciphertext of the condition

feature, by a feature search unit of a secure search apparatus; and decrypting the ciphertext of the target data indicated by a search result to acquire original target data by an encrypted data decryption unit of the searcher terminal, wherein the target data is image data, acoustic data or text data, and the target feature is image feature, acoustic feature or word embedding vector.

[0007a]

A secure search system according to an aspect of the present invention comprises at least one secure search apparatus, an encryption apparatus, and a searcher terminal, the encryption apparatus including: a target feature encryption unit that encrypts target features extracted by converting target data that is a search target, and a target data encryption unit that encrypts the target data, the searcher terminal including: a condition feature encryption unit that encrypts a condition feature extracted by converting condition data that is a search condition, and an encrypted data decryption unit that decrypts a ciphertext of the target data indicated by a search result to acquire original target data, the secure search apparatus including: a feature search unit that acquires a search result indicating the ciphertext of the target data corresponding to the target feature having a close Euclidean distance to the condition feature while

keeping the target features and the condition feature secret using ciphertexts of the target features and a ciphertext of the condition feature, wherein the target data is image data, acoustic data or text data, and the target feature is image feature, acoustic feature or word embedding vector.

[0007b]

A secure search apparatus according to an aspect of the present invention receives a request from a searcher terminal and performs a search for target data held in a storage, the searcher terminal encrypting a condition feature extracted by converting condition data that is a search condition, the secure search apparatus comprising: an encrypted feature storage that stores encrypted target features extracted by converting the target data by an encryption apparatus; a feature search unit that obtains a search result of searching for the target feature having a close Euclidean distance to the condition feature while keeping the target features and the condition feature secret using the ciphertexts of the target features and the condition feature; and a transmission unit that transmits the search result to the searcher terminal and the encryption apparatus, wherein the target data is image data, acoustic data or text data, and the target feature is image feature, acoustic feature or word embedding vector.

[0007c]

An encryption apparatus according to an aspect of the present invention provides encrypted data to a secure search apparatus and a storage, the encryption apparatus comprising: a target feature encryption unit that encrypts target features extracted by converting the target data and stores them in the secure search apparatus; a target data encryption unit that encrypts the target data and stores them in the storage; and a decryption key transmission unit, wherein, a searcher terminal encrypts a condition feature extracted by converting condition data that is a search condition, the encryption apparatus obtains a result (a search result) of searching for the target feature having a close Euclidean distance to the condition feature while keeping the target features and the condition feature secret using the ciphertexts of the target features and the condition feature from the secure search apparatus, the decryption key transmitting unit transmits a key for decrypting the ciphertext of the target data corresponding to the search result to the searcher terminal, and the target data is image data, acoustic data or text data, and the target feature is image feature, acoustic feature or word embedding vector.

[0007d]

A searcher terminal according to an aspect of the

present invention requests a search for target data held in a storage to a secure search apparatus that retains target features extracted by converting the target data, the searcher terminal comprises: a condition feature encryption unit that encrypts condition feature extracted by converting the condition data; an encrypted data acquisition unit; and an encrypted data decryption unit, wherein the target data and the target features are encrypted by an encryption apparatus, the searcher terminal acquires a search result of searching for the target feature having a close Euclidean distance to the condition feature while keeping the target features and the condition feature secret using the ciphertexts of the target features and the condition feature from the secure search apparatus, the encrypted data acquisition unit acquires a ciphertext of the target data corresponding to the search result from the storage, the encrypted data decryption unit acquires a key to decrypt the ciphertext of the target data corresponding to the search result from the encryption apparatus, and the target data is image data, acoustic data or text data, and the target feature is image feature, acoustic feature or word embedding vector.

[0007e]

In the claims which follow and in the preceding description of the invention, except where the context

requires otherwise due to express language or necessary implication, the word "comprise" or variations such as "comprises" or "comprising" is used in an inclusive sense, i.e. to specify the presence of the stated features but not to preclude the presence or addition of further features in various embodiments of the invention.

EFFECTS OF THE INVENTION

[0008]

According to preferred embodiments of the present invention, it is possible to efficiently perform data search by secure computation and to safely provide retrieved data.

BRIEF DESCRIPTION OF THE DRAWINGS

[0009]

Fig. 1 is a diagram illustrating a functional configuration of a secure search system.

Fig. 2 is a diagram illustrating a functional configuration of a secure search apparatus.

Fig. 3 is a diagram illustrating a functional configuration of an encryption apparatus.

Fig. 4 is a diagram illustrating a functional configuration of a searcher terminal.

Fig. 5 is a diagram illustrating a processing

procedure of a secure search method (data registration).

Fig. 6 is a diagram illustrating a processing procedure of a secure search method (data search).

Fig. 7 is a diagram illustrating a functional configuration of a computer.

DETAILED DESCRIPTION OF THE EMBODIMENTS

[0010]

The present invention applies a secure computation technology to implement a secure search system for sensitive data. In order to efficiently perform search even when secure computation of a large computation cost is used, a feature is extracted from original data in advance outside of the search system (for example, when the original data as the search target is the surveillance camera video, at the surveillance camera itself or at an intermediate server installed between the surveillance camera and the search system), and the feature and the original data are encrypted and registered in the search system. The search system performs data search by secure computation using only ciphertext(s) of the feature. Based on the result of the data search, the search system provides search result(s) indicating the ciphertext of the original data separately stored to a searcher who has performed the search. The searcher decrypts the ciphertext

of the original data obtained as the search result to obtain the original data.

[0011]

Hereinafter, an embodiment of the present invention will be described in detail. In the drawings, constituents having the same functions are denoted by the same reference numerals, and redundant description will be omitted.

[0012]

[Embodiment]

An embodiment of the present invention is secure search system and method for searching, from the stored search target data, the data similar to data input as a search condition by secure computation keeping each data secret. In the present embodiment, such a usage is assumed as image data included in surveillance camera videos captured by a surveillance camera is a search target, image data in which a specific person appears is a search condition, and, from the stored search target image data, image data in which a person appearing in the image data of the search condition is included is output as a search result. However, the data to be searched in the present invention is not limited to image data. Any type of data can be a search target as long as it is data from which certain feature can be extracted, such as voice data and text data for example.

[0013]

As illustrated in Fig. 1, a secure search system 100 of the embodiment includes N (≥ 1) secure search apparatuses 1_1,..., 1_N, an encryption apparatus 2, a searcher terminal 3, and a storage 4. A plurality of encryption apparatuses 2 and a plurality of searcher terminals 3 may be included. To the encryption apparatus 2, C (≥ 1) surveillance cameras 5_1,..., 5_C are connected by a wired or wireless interface. When a plurality of encryption apparatuses 2 are included, the number C of surveillance cameras 5_c (c ∈ = 1,..., C) connected to each encryption apparatus 2 may be different from each other. The storage 4 can be omitted by implementing its function in any one of the secure search apparatuses 1_1,..., 1_N.

[0014]

Each of the secure search apparatuses 1_1,..., 1_N, the encryption apparatus 2, the searcher terminal 3, and the storage 4 is connected to a communication network 9. The communication network 9 is a circuit-switching or packet-switching communication network configured such that the connected apparatuses can communicate each other, and for example, the Internet, a local area network (LAN), a wide area network (WAN), or the like can be used.

[0015]

In case there are a plurality of secure search

apparatuses 1_n ($n \in \{1,..., N\}$) (that is, when $N \geq 2$,), the secure search apparatus 1_n performs a search in cooperation with another secure search apparatus $1_{n'}$ ($n' \in \{1,..., N\}$ and $n \neq n'$) using a secure computation method based on secret sharing such as Shamir's Secret Sharing or replicated secret sharing. In case there is one secure search apparatus 1_n (that is, when $N = 1$), the secure search apparatus 1_n performs a search using a secure computation method based on encryption such as homomorphic encryption.

[0016]

For example, as illustrated in Fig. 2, the secure search apparatus 1_n ($n = 1,..., N$) includes an encrypted feature storage 10, a feature search unit 11, and a search result transmission unit 12. For example, as illustrated in Fig. 3, the encryption apparatus 2 includes a decryption key storage 20, a target data acquisition unit 21, a target feature extraction unit 22, a target feature encryption unit 23, a target data encryption unit 24, and a decryption key transmission unit 25. For example, as illustrated in Fig. 4, the searcher terminal 3 includes a condition data input unit 31, a condition feature extraction unit 32, a condition feature encryption unit 33, an encrypted data acquisition unit 34, and an encrypted data decryption unit 35.

[0017]

The secure search apparatuses $1_1, \ldots, 1_N$, the encryption apparatus 2, the searcher terminal 3, and the storage 4 included in the secure search system 100 perform the processing of each step illustrated in Figs. 5 and 6 in cooperation with each other, thereby implementing the secure search method of the embodiment. The secure search method of the embodiment includes two stages, data registration processing where search target data is registered in the secure search system 100, and data search processing where a data similar to the search condition data is searched from search target data by secure computation. Fig. 5 is a flowchart illustrating a procedure of data registration processing, and Fig. 6 is a flowchart illustrating a procedure of data search processing.

[0018]

Each apparatus or terminal included in the secure search system 100 is a special apparatus configured such that a special program is read by a known or dedicated computer including, for example, a central processing unit (CPU), a main storage (random access memory (RAM)), and the like. For example, each apparatus or terminal executes each processing under a control of the central processing unit. The data which is input to each apparatus or

terminal or the data obtained by each processing is stored in, for example, the main storage. The data stored in the main storage is read to the central processing unit, and is used for another processing as necessary. At least some of processing units of each apparatus or terminal may be configured by hardware such as an integrated circuit. Each storage included in each apparatus or terminal may include, for example, a main storage such as a random access memory (RAM), an auxiliary storage including a hard disk, an optical disc, or a semiconductor memory element such as a flash memory, or middleware such as a relational database or a key value store.

[0019]

The secure search apparatus 1_n and the encryption apparatus 2 are, to be specific, information processing devices having a data communication function such as a tower type or rack mount type server computer. The searcher terminal 3 is, to be specific, an information processing apparatus having a data communication function such as a desktop or laptop personal computer, or a mobile terminal such as a smartphone or a tablet. The storage 4 is, to be specific, an information processing apparatus having a data communication function and a data storage function such as a tower type or rack mount type server computer to which a mass storage is connected or a network

connected storage incorporating a mass storage.

[0020]

The surveillance camera 5_C is, for example, an imaging apparatus including a video camera that captures a moving image of a person or an object as a subject. There are no limitations on functions that the surveillance camera 5_C should have, such as available resolutions, a recording medium for a video, with or without a microphone, and digital recording or analog recording. In general, any imaging apparatus can be used as long as the imaging apparatus can capture a moving image.

[0021]

A processing procedure at the time of data registration in the secure search method performed by the secure search system 100 according to the embodiment will be described with reference to Fig. 5.

[0022]

In step S21, the target data acquisition unit 21 of the encryption apparatus 2 acquires data to be searched (hereinafter, referred to as "target data"). The target data is, for example, image data included in the surveillance camera video captured by the surveillance camera 5_C. At this time, information such as a capturing place and a capturing date and time may be tagged to the target data. The target data acquisition unit 21 outputs

the acquired target data to the target feature extraction unit 22 and the target data encryption unit 24.

[0023]

In step S22, the target feature extraction unit 22 of the encryption apparatus 2 receives the target data from the target data acquisition unit 21 and extracts a feature (hereinafter, referred to as "target feature") from the target data. The target feature extraction unit 22 outputs the extracted target feature to the target feature encryption unit 23.

[0024]

The method of extracting the feature can be arbitrarily determined according to the type of the target data. For example, in case such a use scene is assumed as the target data is image data included in a video in which an unspecified number of people are captured, and a face of a specific person is searched for from the target data, the feature may be extracted in the following two steps. First, regions to be searched (for example, the faces of humans) are extracted from image data captured by the surveillance camera 5_C (step 1). For the region extraction, for example, a general method such as principal component analysis may be used (see Reference Document 1). Next, the extracted face image data are converted into features (step 2). In the feature conversion of the face

image data, for example, the pixel value of each pixel of the image may be adopted as it is as the feature, or the change of each pixel may be adopted as the feature using a general edge extraction method (see Reference Document 2).

[0025]

[Reference Document 1] Mante Opel, "Facial recognition using principal component analysis", [online], [retrieved on March 9, 2020], Internet <URL: https://qiita.com/manteopel/items/703e9946e1903c6e2aa3>

[Reference Document 2] SUNSHINE, "Feature" of "image recognition" (2): Summarized are What is "edge detection"? What kind of mechanism? What is a "spatial filter"? How is it used?", [online], [retrieved on March 9, 2020], Internet <URL: https://it-mint.com/2018/11/05/feature-value-in-image-recognition-whats-edge-detection-and-spatial-filter-1839.html>

[0026]

In case the target data is voice data, a known acoustic feature may be extracted. In case the target data is text data, a feature such as a known word embedding vector may be extracted.

[0027]

In step S23-1, the target feature encryption unit 23 of the encryption apparatus 2 receives the target feature from the target feature extraction unit 22 and encrypts the

target feature. The target feature encryption unit 23 encrypts the target feature using any encryption method or secret sharing method capable of secure computation. Specifically, examples of the encryption method capable of secure computation include homomorphic encryption, and examples of the secret sharing method capable of secure computation include Shamir's Secret Sharing and replicated secret sharing. The generated ciphertext is one ciphertext in the case of the encryption method, and are split values consisting of a plurality of shares in the case of the secret sharing method. The target feature encryption unit 23 transmits the ciphertext of the target feature to each secure search apparatus 1_n. Here, "transmitting the ciphertext to each secure search apparatus 1_n" means transmitting one ciphertext to one secure search apparatus 1_1 if the ciphertext is in an encryption method, and distributing the split values so that each of the plurality of secure search apparatuses $1_1,\ldots, 1_N$ holds one share without overlapping if the ciphertext is in a secret sharing method. The same applies to the following description.

[0028]

In step S23-2, each secure search apparatus 1_n receives the ciphertext of the target feature from the encryption apparatus 2 and stores the ciphertext of the

target feature in the encrypted feature storage 10.

[0029]

In step S24-1, the target data encryption unit 24 of the encryption apparatus 2 receives the target data from the target data acquisition unit 21 and encrypts the target data. The encryption method used by the target data encryption unit 24 is an encryption method different from the encryption method used by the target feature encryption unit 23, and is an encryption method in which original data cannot be obtained unless a valid decryption key is used. Such an encryption method may be common key encryption or public key encryption. The target data encryption unit 24 associates information indicating the ciphertext of the target data with information indicating a decryption key necessary for decrypting the ciphertext of the target data, and stores the information in the decryption key storage 20. The information indicating the decryption key may be the decryption key itself or may be information that can identify the decryption key exchanged in advance between the encryption apparatus 2 and the searcher terminal 3 by a secure method. The target data encryption unit 24 transmits the ciphertext of the target data to the storage 4.

[0030]

In step S24-2, the storage 4 receives the ciphertext

of the target data from the encryption apparatus 2 and stores the ciphertext of the target data.

[0031]

A processing procedure at the time of data search in the secure search method performed by the secure search system 100 according to the embodiment will be described with reference to Fig. 6.

[0032]

In step S31, the condition data input unit 31 of the searcher terminal 3 acquires data (hereinafter, referred to as "condition data") as a search condition input to the searcher terminal 3 by the searcher using the searcher terminal 3. The condition data is, for example, image data in which a face of a person to be searched is captured. The condition data input unit 31 outputs the acquired condition data to the condition feature extraction unit 32.

[0033]

In step S32, the condition feature extraction unit 32 of the searcher terminal 3 receives condition data from the condition data input unit 31 and extracts a feature (hereinafter, referred to as a "condition feature") from the condition data. The feature extracted by the condition feature extraction unit 32 is similar to the feature extracted by the target feature extraction unit 22 of the encryption apparatus 2. The condition feature extraction

unit 32 outputs the extracted condition feature to the condition feature encryption unit 33.

[0034]

In step S33, the condition feature encryption unit 33 of the searcher terminal 3 receives the condition feature from the condition feature extraction unit 32 and encrypts the condition feature. The encryption method used by the condition feature encryption unit 33 is similar to the encryption method used by the target feature encryption unit 23 of the encryption apparatus 2. The condition feature encryption unit 33 transmits the ciphertext of the condition feature to each secure search apparatus 1_n.

[0035]

In step S11, the feature search unit 11 of each secure search apparatus 1_n receives the ciphertext of the condition feature from the searcher terminal 3, and searches for the target feature similar to the condition feature by secure computation using the ciphertext of the target feature stored in the encrypted feature storage 10 and the ciphertext of the condition feature received from the searcher terminal 3. That is, the ciphertext of the target feature similar to the condition feature is extracted while keeping the target feature and the condition feature secret. The feature search unit 11 outputs information (hereinafter, referred to as a "search

result") indicating the ciphertext of the target data corresponding to the extracted ciphertext of the target feature to the search result transmission unit 12.

[0036]

The feature search by the secure computation can be performed by calculating Euclidean distances between the condition data and all the target data and comparing the calculation result with a predetermined threshold using secure computation. The Euclidean distance is calculated as follows. It is assumed that the data to be searched (target data) and the search data (condition data) are image data of n × m pixels. When the pixel values of the search data (feature) are $x = [x_{ij}]$ and the pixel values of the search data are $y = [y_{ij}]$ ($i = 1, \ldots, m$, $j = 1, \ldots, n$), the Euclidean distance D is expressed by the following formula (see Reference Document 3).

[0037]

[Math. 1]

$$D = \sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n}(x_{ij} - y_{ij})}$$

[0038]

[Reference Document 3] Kohei Inoue, Kiichi Urahama, "Filtering Method for Image Retrieval Based on Lower Bound of Euclidean Distance", Journal of The Institute of Image

Information and Television Engineers, Vol. 59, No. 11, pp. 1701-1704, 2005

[0039]

The secure computation of the Euclidean distance D can be easily achieved by utilizing secure computation having the additive homomorphism.

[0040]

A search result can be generated by calculating the Euclidean distance D for all target data and comparing the calculation result with a predetermined threshold. For example, target data whose Euclidean distance D are equal to or less than a predetermined threshold, or a predetermined number of pieces of target data from the head when the Euclidean distance D is sorted in ascending order may be output as the search result. For the sort computation on the secure computation, for example, the method described in Reference Document 4 can be used.

[0041]

[Reference Document 4] Dai Ikarashi, Koki Hamada, Ryo Kikuchi, Koji Chida, "A Design and an Implementation of Super-High-Speed Multi-Party Sorting: The Day When Multi-Party Computation Reaches Scripting Languages", Computer Security Symposium (CSS), 2017

[0042]

In step S12-1, the search result transmission unit

12 of each secure search apparatus 1_n receives the search result from the feature search unit 11 and transmits the search result to the searcher terminal 3. In addition, the search result transmission unit 12 transmits the search result and information indicating the searcher terminal 3 to the encryption apparatus 2.

[0043]

In step S12-2, the searcher terminal 3 receives the search result from each secure search apparatus 1_n and obtains information indicating the ciphertext of the target data from the search result. In case the feature search unit 11 performs a search by a secure computation method based on secret sharing, information indicating the ciphertext of the target data may be obtained by restoring the share of the search result received from each secure search apparatus 1_n. In case the feature search unit 11 performs a search by a secure computation method based on encryption, information indicating the ciphertext of the target data may be obtained by decrypting the search result received from the secure search apparatus 1_1 according to a predetermined decryption method. The searcher terminal 3 inputs obtained information indicating the ciphertext of the target data to the encrypted data acquisition unit 34.

[0044]

In step S12-3, the encryption apparatus 2 receives

the search result and the information indicating the searcher terminal 3 from each secure search apparatus 1_n, and obtains information indicating the ciphertext of the target data from the search result, similarly to the searcher terminal 3. The encryption apparatus 2 inputs obtained information indicating the ciphertext of the target data and information indicating the searcher terminal 3 to the decryption key transmission unit 25.

[0045]

In step S34, the encrypted data acquisition unit 34 of the searcher terminal 3 acquires the ciphertext of the target data indicated by the input information from the storage 4. The encrypted data acquisition unit 34 outputs the acquired ciphertext of the target data to the encrypted data decryption unit 35.

[0046]

In step S25-1, the decryption key transmission unit 25 of the encryption apparatus 2 acquires, from the decryption key storage 20, information indicating a decryption key for decrypting the ciphertext of the target data indicated by the input information. The decryption key transmission unit 25 transmits acquired information indicating the decryption key to the searcher terminal 3.

[0047]

In step S25-2, the searcher terminal 3 receives

information indicating a decryption key from the encryption apparatus 2 and acquires the decryption key. The searcher terminal 3 inputs the acquired decryption key to the encrypted data decryption unit 35.

[0048]

In step S35, the encrypted data decryption unit 35 of the searcher terminal 3 receives the ciphertext of the target data from the encrypted data acquisition unit 34, and decrypts the ciphertext of the target data using the input decryption key. The encrypted data decryption unit 35 outputs the original target data obtained by decryption. In case the target data acquisition unit 21 has tagged information such as a capturing place and a capturing date and time to the target data, such information may be added to the output target data.

[0049]

With the above configuration, the secure search apparatuses 1_1,..., and 1_N search the target data using only the feature, so that the computation cost of the data search by the secure computation can be reduced. In addition, the searcher terminal 3 can acquire, as the search result, original data itself that is similar to the search condition data among the pieces of target data. Here, since the original data is encrypted by an encryption method that cannot be decrypted without a decryption key,

information regarding the original data is not leaked to the secure search apparatuses 1_1,..., 1_N. Therefore, the original data can be safely provided to the searcher terminal as the search result.

[0050]

[Modification]

In the secure search system of the embodiment, the encryption apparatus 2 extracts a feature from each of image data captured by the plurality of surveillance cameras 5_1,..., 5_C, encrypts the feature and the original image data, and stores the encrypted feature and the original image data so as to be usable from the secure computation apparatuses 1_1,..., 1_N. However, the encryption apparatus 2 can be omitted by implementing the feature extraction and encryption functions in the surveillance cameras 5_1, ..., 5_C themselves. In this case, the surveillance cameras 5_1, ..., 5_C include the decryption key storage 20, the target feature extraction unit 22, the target feature encryption unit 23, the target data encryption unit 24, and the decryption key transmission unit 25 included in the encryption apparatus 2 of the embodiment. That is, in the secure search system of the modification, each of the surveillance cameras 5_1, ..., 5_C is configured to correspond to the encryption apparatus 2.

[0051]

While the embodiment of the present invention has been described above, a specific configuration is not limited to the embodiment, and it goes without saying that an appropriate design change or the like not departing from the gist of the present invention is included in the present invention. The various processes described in the embodiments may be executed not only in chronological order according to the described order, but also in parallel or individually according to the processing capability of an apparatus that executes the processes or as needed.

[0052]

[Program and Recording Medium]

In case various types of processing functions in each apparatus described in the embodiment are implemented by a computer, processing content of the functions of each apparatus is described by a program. By causing a memory 1020 of a computer illustrated in Fig. 7 to read this program and causing a calculation unit 1010, an input unit 1030, an output unit 1040, and the like to execute the program, various kinds of processing functions in each of the foregoing devices are implemented on the computer.

[0053]

The program describing the processing content may be recorded on a computer-readable recording medium. The computer-readable recording medium is, for example, a non-

transitory recording medium, and is a magnetic recording apparatus, an optical disc, or the like.

[0054]

Distribution of the program is performed by, for example, selling, transferring, or renting a portable recording medium such as a DVD or a CD-ROM on which the program is recorded. Further, a configuration in which the program is stored in a storage in a server computer and the program is distributed by transferring the program from the server computer to other computers via a network may also be employed.

[0055]

For example, the computer that executes such a program first temporarily stores the program recorded in a portable recording medium or the program transferred from the server computer in an auxiliary storage 1050 that is a non-transitory storage device of the computer. In addition, when executing processing, the computer reads the program stored in the auxiliary storage 1050 that is a non-transitory storage device of the computer, into the memory 1020 that is a temporary storage device, and executes processing according to the read program. Further, as another embodiment of the program, a computer may directly read the program from a portable recording medium and execute processing according to the program, and a computer

may sequentially execute processing according to the received program each time the program is transferred from a server computer to the computer. Further, the above-described processing may be executed by a so-called application service provider (ASP) type service that implements a processing function only by an execution instruction and result acquisition without transferring the program from the server computer to the computer. The program according to the present embodiment includes information used for a process by an electronic computer and equivalent to the program (data or the like that is not a direct command to the computer but has a property that defines a process of the computer).

[0056]

Although the various apparatuses described in the embodiment are configured by executing a predetermined program on a computer in the description above, at least part of the processing content may be implemented by hardware.

2021436355 17 Oct 2024

CLAIMS

[Claim 1]

A secure search method performed by a secure search system including at least one secure search apparatus, an encryption apparatus, and a searcher terminal, the secure search method comprising:

encrypting target features extracted by converting target data that is a search target, by a target feature encryption unit of the encryption apparatus;

encrypting the target data by a target data encryption unit of the encryption apparatus;

encrypting a condition feature extracted by converting condition data that is a search condition, by a condition feature encryption unit of the searcher terminal;

acquiring a search result indicating a ciphertext of the target data corresponding to the target feature having a close Euclidean distance to the condition feature while keeping the target features and the condition feature secret using ciphertexts of the target features and a ciphertext of the condition feature, by a feature search unit of the secure search apparatus; and

decrypting the ciphertext of the target data indicated by the search result to acquire original target data by an encrypted data decryption unit of the searcher terminal,

wherein the target data is image data, acoustic data or text data, and the target feature is image feature, acoustic feature or word embedding vector.

[Claim 2]

The secure search method according to claim 1,

wherein the ciphertext of the target feature and the ciphertext of the condition feature are encrypted by a first encryption method capable of secure computation,

the ciphertext of the target data is encrypted by a second encryption method that is different from the first encryption method and requires a decryption key for decryption,

a decryption key transmission unit of the encryption apparatus transmits information indicating the decryption key for decrypting the ciphertext of the target data indicated by the search result to the searcher terminal, and

the encrypted data decryption unit decrypts the ciphertext of the target data indicated by the search result using the decryption key.

[Claim 3]

The secure search method according to claim 1,

wherein the target data is image data included in a video captured by a surveillance camera, and

the condition data is image data in which a face of

a specific person is captured.

[Claim 4]

A secure search system comprising at least one secure search apparatus, an encryption apparatus, and a searcher terminal,

the encryption apparatus including:

a target feature encryption unit that encrypts target features extracted by converting target data that is a search target, and

a target data encryption unit that encrypts the target data,

the searcher terminal including:

a condition feature encryption unit that encrypts a condition feature extracted by converting condition data that is a search condition, and

an encrypted data decryption unit that decrypts a ciphertext of the target data indicated by a search result to acquire original target data,

the secure search apparatus including:

a feature search unit that acquires a search result indicating the ciphertext of the target data corresponding to the target feature having a close Euclidean distance to the condition feature while keeping the target features and the condition feature secret using ciphertexts of the target

features and a ciphertext of the condition feature,

wherein the target data is image data, acoustic data or text data, and the target feature is image feature, acoustic feature or word embedding vector.

[Claim 5]

A secure search apparatus that receives a request from a searcher terminal and performs a search for target data held in a storage,

the searcher terminal encrypting a condition feature extracted by converting condition data that is a search condition, the secure search apparatus comprising:

an encrypted feature storage that stores encrypted target features extracted by converting the target data by an encryption apparatus;

a feature search unit that obtains a search result of searching for the target feature having a close Euclidean distance to the condition feature while keeping the target features and the condition feature secret using the ciphertexts of the target features and the condition feature; and

a transmission unit that transmits the search result to the searcher terminal and the encryption apparatus,

wherein the target data is image data, acoustic data or text data, and the target feature

is image feature, acoustic feature or word embedding vector.

[Claim 6]

An encryption apparatus that provides encrypted data to a secure search apparatus and a storage, the encryption apparatus comprising:

a target feature encryption unit that encrypts target features extracted by converting the target data and stores them in the secure search apparatus;

a target data encryption unit that encrypts the target data and stores them in the storage; and

a decryption key transmission unit,

wherein, a searcher terminal encrypts a condition feature extracted by converting condition data that is a search condition,

the encryption apparatus obtains a result (a search result) of searching for the target feature having a close Euclidean distance to the condition feature while keeping the target features and the condition feature secret using the ciphertexts of the target features and the condition feature from the secure search apparatus,

the decryption key transmitting unit transmits a key for decrypting the ciphertext of the target data corresponding to the search result to the searcher terminal, and

the target data is image data, acoustic data or text data, and the target feature is image feature, acoustic feature or word embedding vector.

[Claim 7]

A searcher terminal that requests a search for target data held in a storage to a secure search apparatus that retains target features extracted by converting the target data, the searcher terminal comprises:

a condition feature encryption unit that encrypts condition feature extracted by converting the condition data;

an encrypted data acquisition unit; and

an encrypted data decryption unit,

wherein the target data and the target features are encrypted by an encryption apparatus,

the searcher terminal acquires a search result of searching for the target feature having a close Euclidean distance to the condition feature while keeping the target features and the condition feature secret using the ciphertexts of the target features and the condition feature from the secure search apparatus,

the encrypted data acquisition unit acquires a ciphertext of the target data corresponding to the search result from the storage,

the encrypted data decryption unit acquires a key to

decrypt the ciphertext of the target data corresponding to the search result from the encryption apparatus, and

the target data is image data, acoustic data or text data, and the target feature is image feature, acoustic feature or word embedding vector.

[Claim 8]

A program for causing a computer to execute each step of the secure search method according to any one of claims 1 to 3.

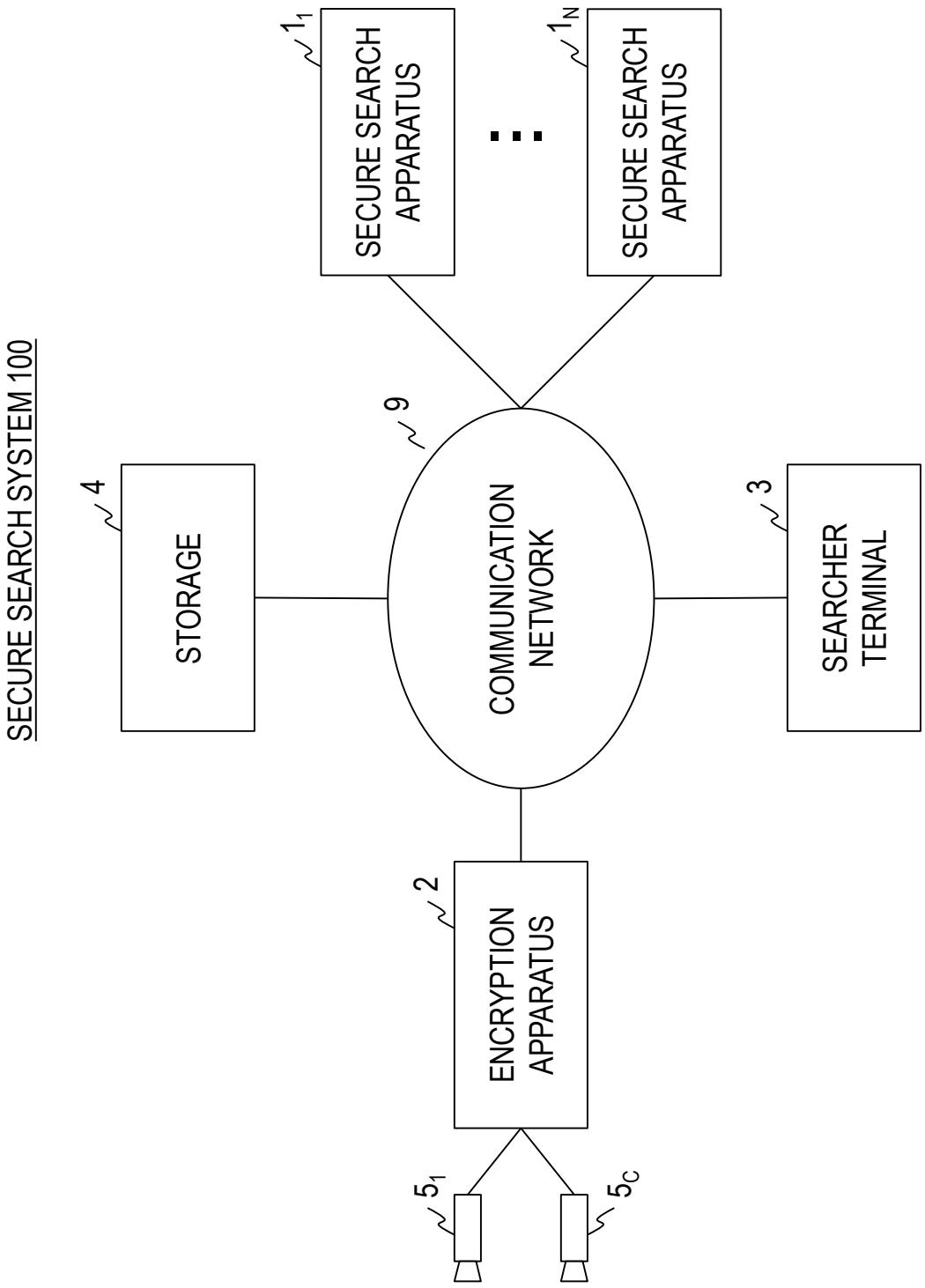
SECURE SEARCH SYSTEM 100
SECURE SEARCH APPARATUS
1₁
SECURE SEARCH APPARATUS
1N
9
COMMUNICATION NETWORK
STORAGE
4
SEARCHER TERMINAL
3
ENCRYPTION APPARATUS
2
5₁
5C

FIG. 1

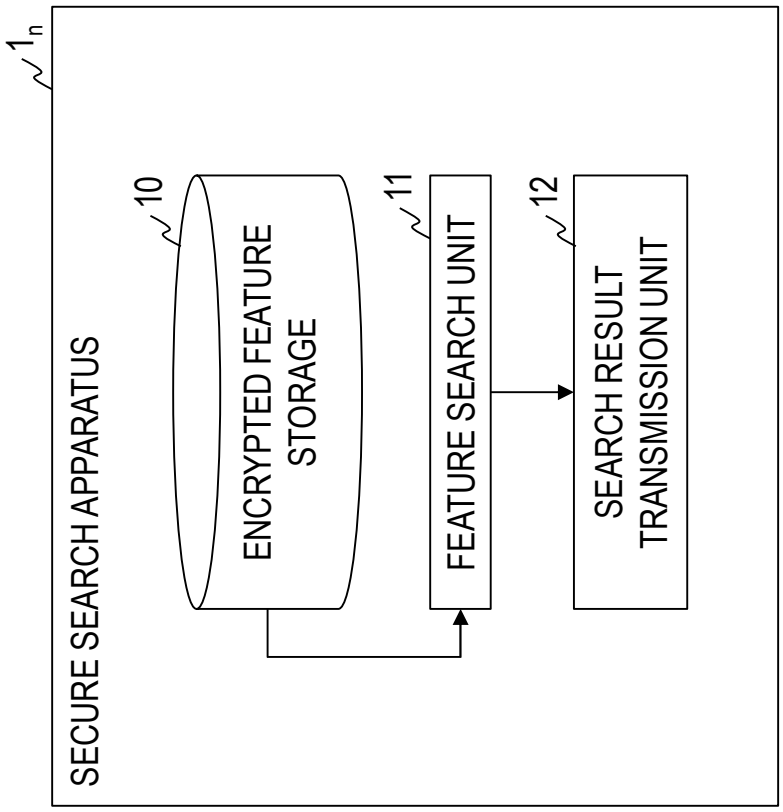
1n
SECURE SEARCH APPARATUS
10
ENCRYPTED FEATURE STORAGE
11
FEATURE SEARCH UNIT
12
SEARCH RESULT TRANSMISSION UNIT

FIG. 2

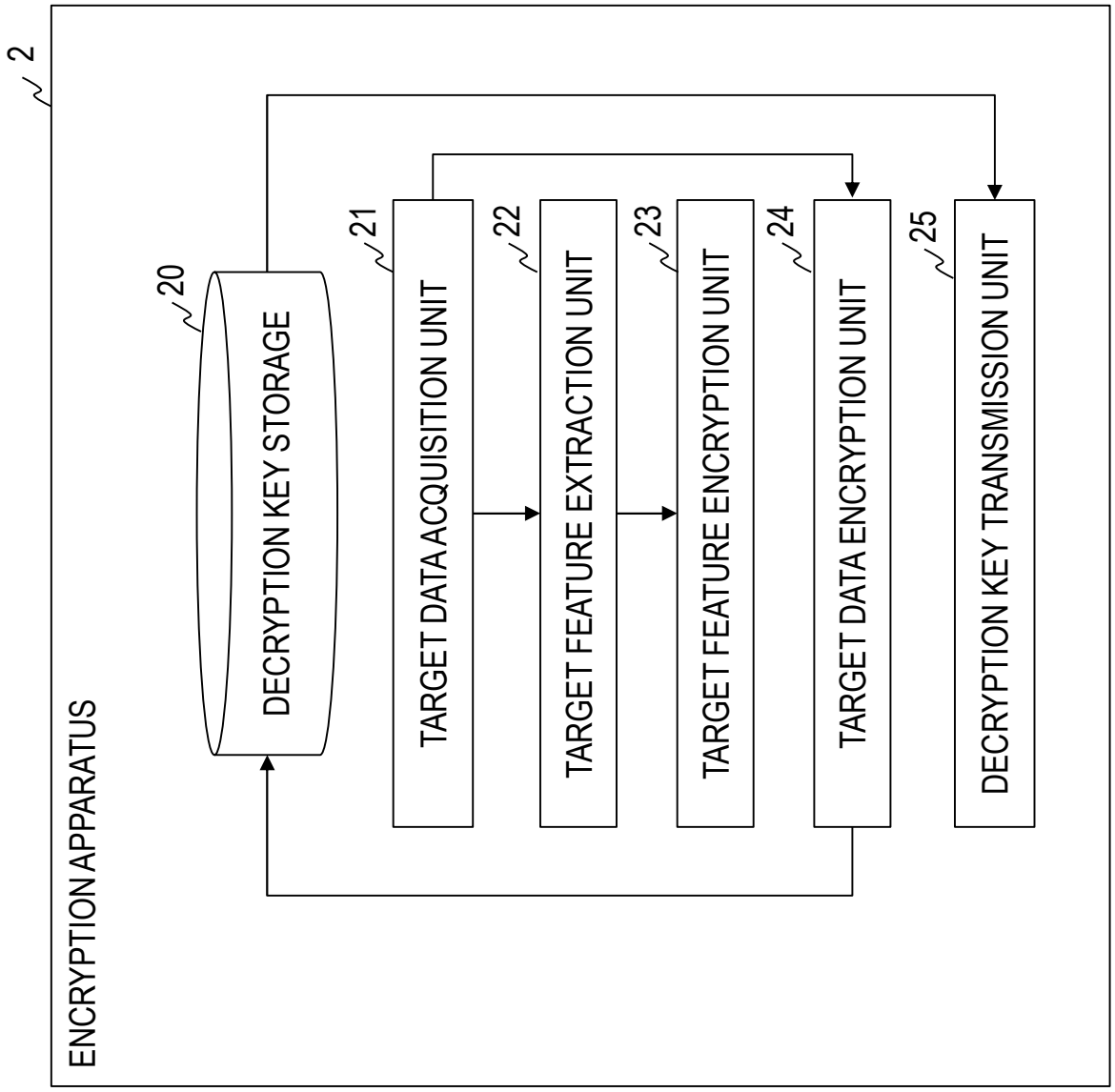
2
ENCRYPTION APPARATUS
20
DECRYPTION KEY STORAGE
21
TARGET DATA ACQUISITION UNIT
22
TARGET FEATURE EXTRACTION UNIT
23
TARGET FEATURE ENCRYPTION UNIT
24
TARGET DATA ENCRYPTION UNIT
25
DECRYPTION KEY TRANSMISSION UNIT

FIG. 3

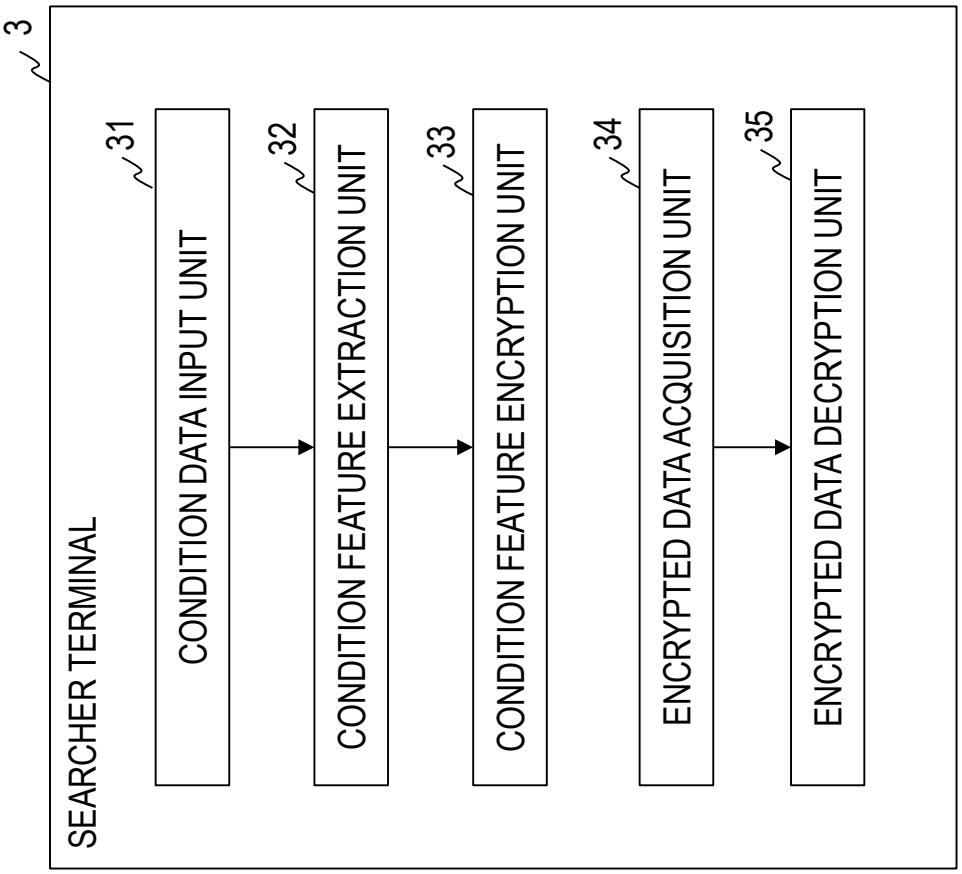
3
SEARCHER TERMINAL
31
CONDITION DATA INPUT UNIT
32
CONDITION FEATURE EXTRACTION UNIT
33
CONDITION FEATURE ENCRYPTION UNIT
34
ENCRYPTED DATA ACQUISITION UNIT
35
ENCRYPTED DATA DECRYPTION UNIT

FIG. 4

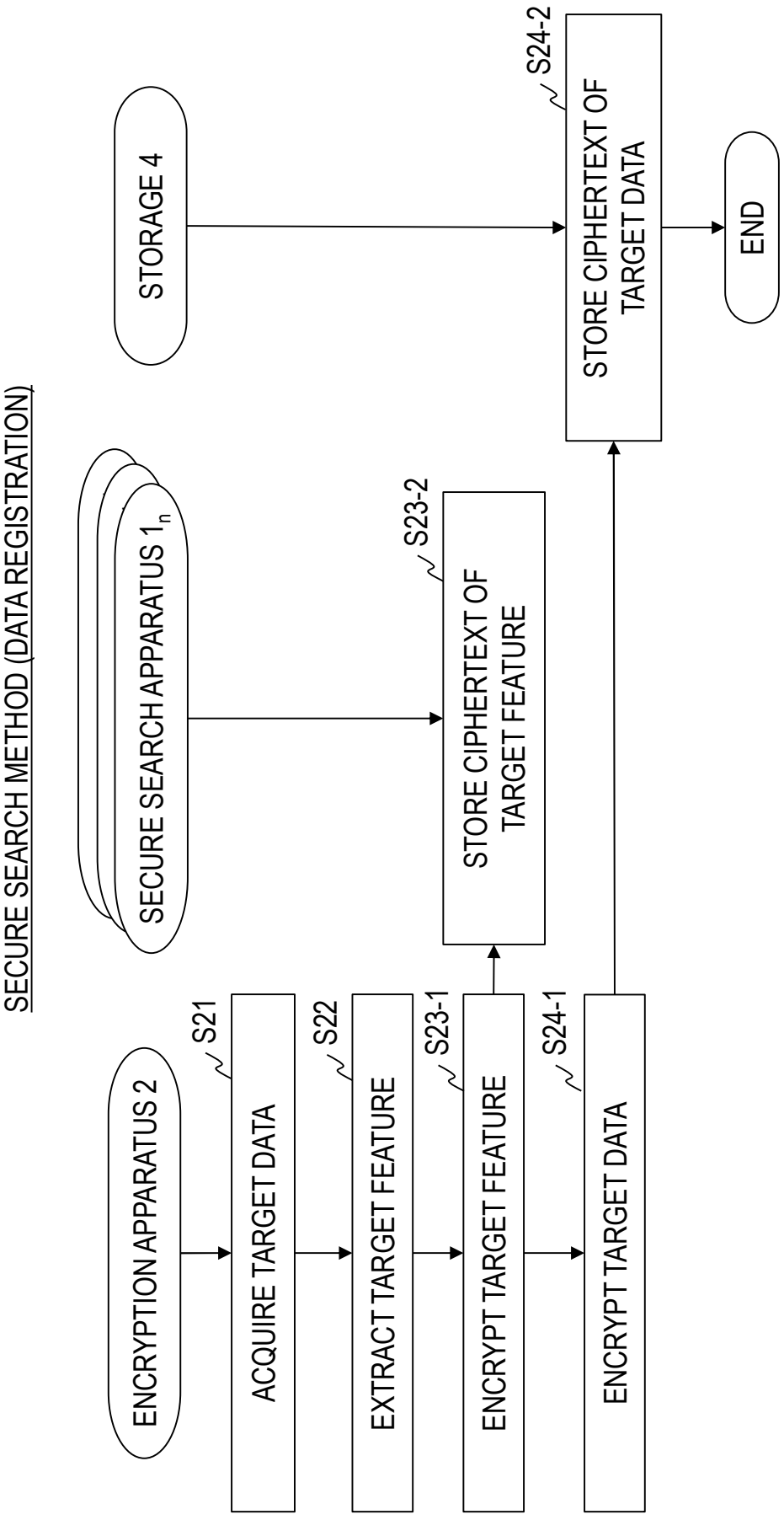
SECURE SEARCH METHOD (DATA REGISTRATION)
ENCRYPTION APPARATUS 2
S21
ACQUIRE TARGET DATA
S22
EXTRACT TARGET FEATURE
S23-1
ENCRYPT TARGET FEATURE
S24-1
ENCRYPT TARGET DATA
SECURE SEARCH APPARATUS 1n
S23-2
STORE CIPHERTEXT OF TARGET FEATURE
STORAGE 4
S24-2
STORE CIPHERTEXT OF TARGET DATA
END

FIG. 5

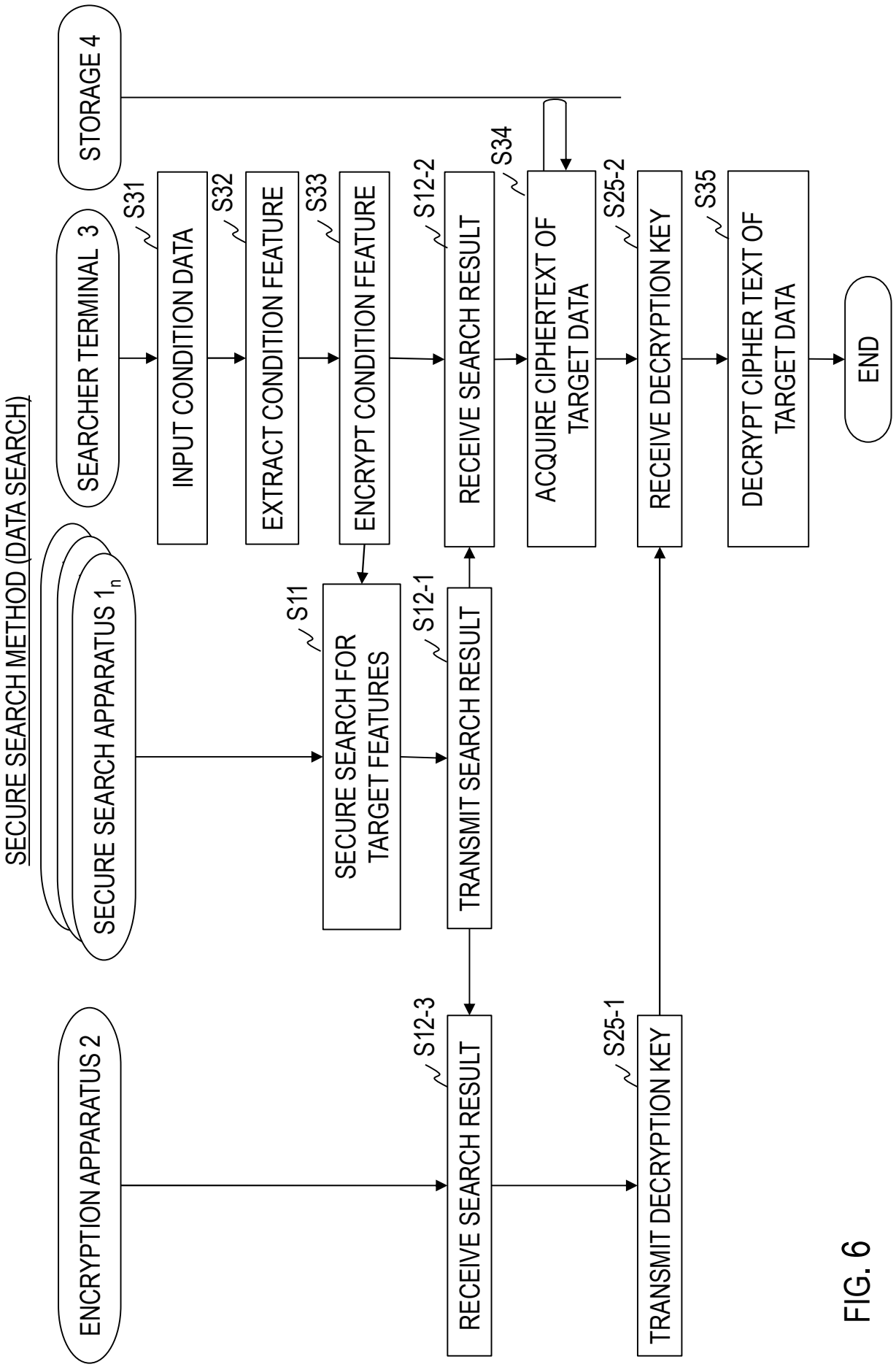
SECURE SEARCH METHOD (DATA SEARCH)
STORAGE 4
SEARCHER TERMINAL 3
SECURE SEARCH APPARATUS 1n
ENCRYPTION APPARATUS 2
S31
INPUT CONDITION DATA
S32
EXTRACT CONDITION FEATURE
S33
ENCRYPT CONDITION FEATURE
S11
SECURE SEARCH FOR TARGET FEATURES
S12-1
TRANSMIT SEARCH RESULT
S12-2
RECEIVE SEARCH RESULT
S34
ACQUIRE CIPHERTEXT OF TARGET DATA
S25-2
RECEIVE DECRYPTION KEY
S35
DECRYPT CIPHER TEXT OF TARGET DATA
END
S12-3
RECEIVE SEARCH RESULT
S25-1
TRANSMIT DECRYPTION KEY

FIG. 6

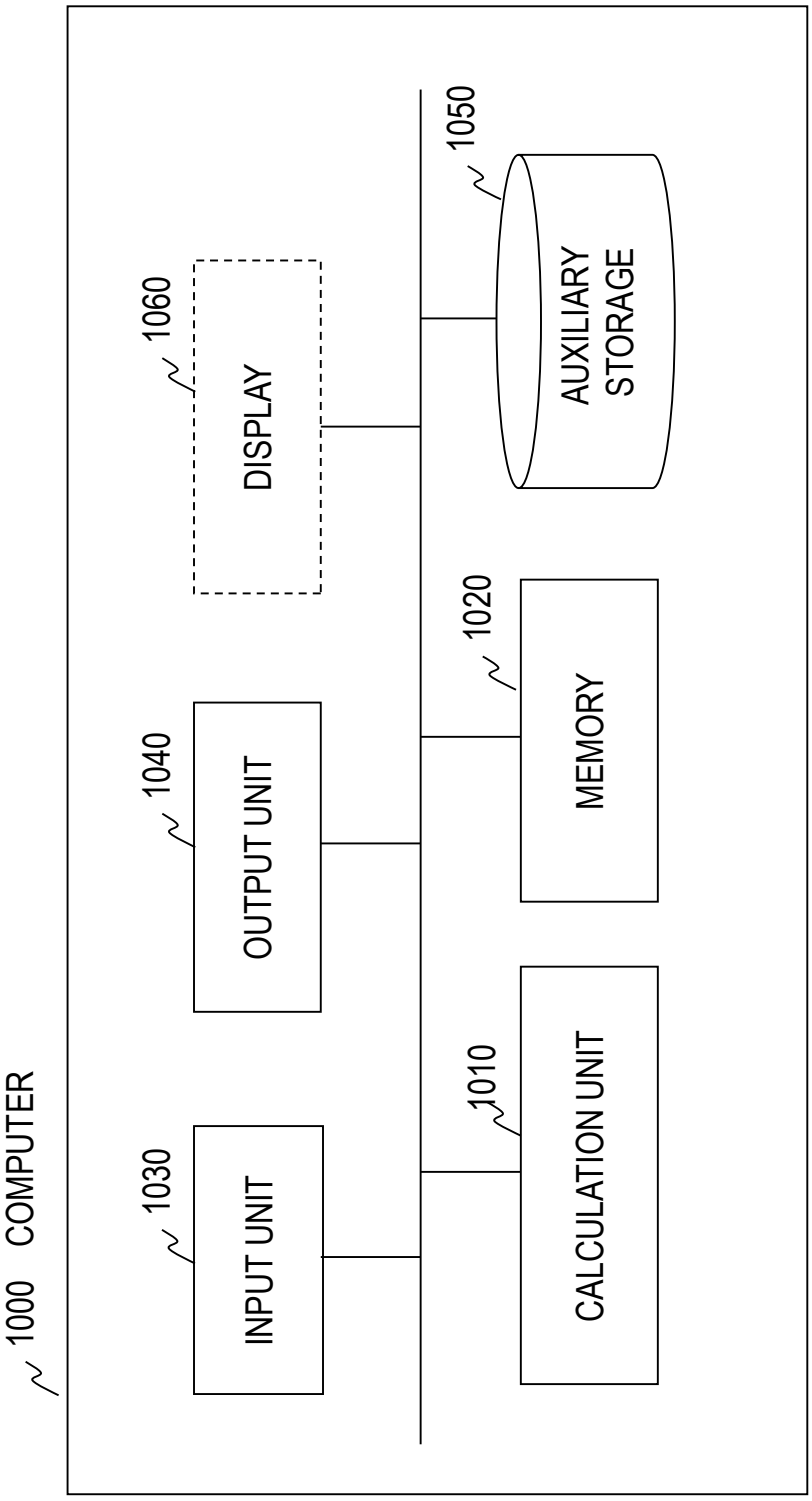
1000 COMPUTER
1030
INPUT UNIT
1040
OUTPUT UNIT
1060
DISPLAY
1010
CALCULATION UNIT
1020
MEMORY
1050
AUXILIARY STORAGE

FIG. 7