(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
2017 年 8 月 17 日(17.08.2017)

WIPO | PCT

(10) 国際公開番号
WO 2017/138616 A1

(51) 国際特許分類:
H04L 9/14 (2006.01)

(21) 国際出願番号: PCT/JP2017/004766

(22) 国際出願日: 2017 年 2 月 9 日(09.02.2017)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願 2016-023909 2016 年 2 月 10 日(10.02.2016) JP

(71) 出願人: 株式会社デンソー(DENSO CORPORATION) [JP/JP]; 〒4488661 愛知県刈谷市昭和町１丁目１番地 Aichi (JP).

(72) 発明者: 藤村 基(FUJIMURA, Motoi); 〒4488661 愛知県刈谷市昭和町１丁目１番地 株式会社デンソー内 Aichi (JP).

(74) 代理人: 名古屋国際特許業務法人(NAGOYA INTERNATIONAL PATENT FIRM); 〒4600003 愛知県名古屋市中区錦一丁目２０番１９号 名神ビル Aichi (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, 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, 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, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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),

[続葉有]

(54) **Title**: DATA STRUCTURE AND DATA PROCESSING DEVICE

(54) 発明の名称 : データ構造、及びデータ処理装置

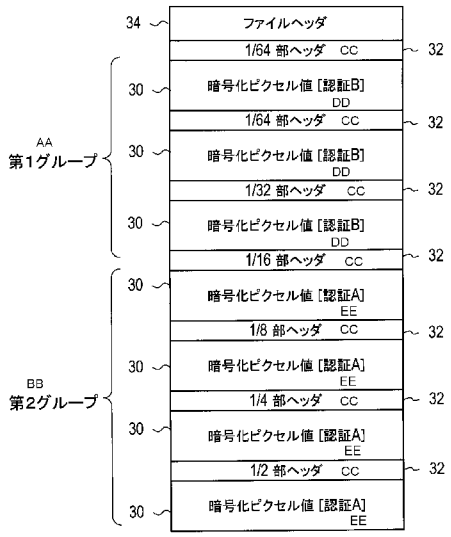

FIG. 3

34 File header
AA First group
BB Second group
CC Partial header
DD Encrypted pixel value [authentication B]
EE Encrypted pixel value [authentication A]

(57) **Abstract**: This data processing device is provided with an acquiring unit, a sorting unit, an adding unit, an encryption processing unit, and a generating unit. The sorting unit generates a plurality of field portions obtained by dividing data, which includes data values arrayed in accordance with an array, in accordance with a defined rule which is defined on the basis of the arrangement order of the data values in the array. The adding unit adds, to each of the plurality of field portions, a header portion indicating the content of the field portion. The encryption processing unit encrypts the data value included in at least one of the plurality of field portions. The data generated in this way has a data structure including the plurality of field portions (30) and a plurality of field header portions (32), and the data value included in at least one of the plurality of field portions is encrypted.

(57) 要約: データ処理装置は、取得部と、分類部と、付加部と、暗号処理部と、生成部とを備える。分類部は、配列に従ってデータ値が並べられたデータを、配列におけるデータ値の配置の順序に基づいて規定された規定ルールに従って区分けした複数のフィールド部を生成する。付加部は、複数のフィールド部の各々に、当該フィールド部の内容を表すヘッダ部を付加する。暗号処理部は、複数のフィールド部のうちの少なくとも１つのフィールド部に含まれるデータ値を暗号化する。これによって生成されるデータのデータ構造は、複数のフィールド部（３０）と、複数のフィールドヘッダ部（３２）とを備え、複数のフィールド部のうちの少なくとも１つのフィールド部に含まれるデータ値が暗号化されたものである。

WO 2017/138616 A1

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)）

明　細　書

発明の名称 ： データ構造、及びデータ処理装置

関連出願の相互参照

[0001] 本国際出願は、２０１６年２月１０日に日本国特許庁に出願された日本国特許出願第２０１６－２３９０９号に基づく優先権を主張するものであり、日本国特許出願第２０１６－２３９０９号の全内容を本国際出願に参照により援用する。

技術分野

[0002] 本開示は、配列構造を有したデータ構造、及びデータ処理装置に関する。

背景技術

[0003] 医療の用途に用いられる画像を撮像して管理するシステムや、バイタルサインを計測して管理するシステムである情報管理システムが知られている。情報管理システムでは、管理する情報、即ち、画像やバイタルサインなどの情報の機密性を担保することが求められている。

[0004] 情報の機密性を担保することを目的とした技術として、特許文献１に記載されているように、文書データにおいて選択されたページの一部分を被覆し、その被覆された部分を暗号化する技術が提案されている。

先行技術文献

特許文献

[0005] 特許文献1：特表２００９－５０８２４０号公報

発明の概要

[0006] 一方、情報管理システムは、医療の用途に用いられるものであるため、撮像される画像や計測されたバイタルサインの正確性を保つ必要があり、メンテナンスが重要となる。メンテナンスにおいては、情報管理システムにて管理する情報がどのような情報であるのかを、メンテナンスの担当者が確認しながら実施することが効率的である。

[0007] 情報管理システムにて管理する情報の機密性を担保するために、情報管理

システムに対して特許文献１に記載された技術を適用することを想定する。この場合、メンテナンスの担当者が情報管理システムにて管理する情報がどのような情報であるのかを確認するためには、データにおいて被覆されている部分を復号する必要がある。

[0008] しかしながら、メンテナンスの担当者は、復号のコードを知らないことが多く、情報管理システムにて管理している情報がどのような情報であるのかを認識できず、メンテナンスを効率よく実施できない。

[0009] また、メンテナンスの担当者が復号のコードを知得した場合には、被覆された全ての領域を閲覧可能となるため、情報の機密性を担保することが困難となる。

つまり、発明者の詳細な検討の結果、従来の技術では、最低限必要な情報を認識可能としつつ、情報の機密性を確保することが困難であるという課題が見出された。

[0010] 本開示の一局面は、最低限必要な情報を認識可能としつつ、情報の機密性を確保する技術を提供することにある。

本開示の一態様は、配列に従ってデータ値が並べられたデータのデータ構造に関する。

[0011] このデータ構造は、複数のフィールド部と、複数のフィールドヘッダ部とを備えている。

複数のフィールド部は、配列におけるデータ値の配置の順序に基づいて規定された規定ルールに従って、データを区分けしたものである。複数のフィールドヘッダ部は、複数のフィールド部の各々の内容を表すものである。

[0012] さらに、データ構造においては、複数のフィールド部のうちの少なくとも１つのフィールド部に含まれるデータ値が暗号化されている。

このようなデータ構造において、暗号化されていないフィールド部のデータ値については復号することなく閲覧できる。このため、利用者は、暗号化されていないフィールド部のデータ値から、データの全体像の一部分を把握できる。

[0013] しかも、フィールドヘッダ部は、フィールド部の各々の内容を表すものである。そのため、このようなデータ構造であれば、暗号化されたフィールド部を復号しなくとも、利用者は、そのフィールド部にどのような情報が含まれているのか、ひいては、データがどのような情報であるのかを認識できる。

[0014] これらのことから、このようなデータ構造によれば、最低限必要なデータの内容を利用者に認識させることができる。

一方、このようなデータ構造によれば、暗号化されたフィールド部に含まれるデータ値については、復号のコードの知らない限り復号することができないため、データの全体像に対する機密性を担保できる。

[0015] つまり、このようなデータ構造を用いることで、最低限必要な情報を認識可能としつつ、情報の機密性を確保できる。

なお、本開示の別の態様は、取得部と、分類部と、付加部と、暗号処理部と、生成部とを備えるデータ処理装置であってもよい。

[0016] 取得部は、配列に従ってデータ値が並べられたデータを取得する。分類部は、取得部で取得したデータにおけるデータ値の各々を、配列におけるデータ値の配置の順序に基づいて規定された規定ルールに従って分類した複数のフィールド部を生成する。

[0017] 付加部は、分類部で生成された複数のフィールド部の各々の内容を表すフィールドヘッダ部を付加する。暗号処理部は、分類部で生成された複数のフィールド部のうちの少なくとも１つのフィールド部に含まれるデータ値を暗号化する。

[0018] 生成部は、複数のフィールド部、フィールドヘッダ部、及び暗号化されたフィールド部に基づいて、複数のフィールド部と、複数のフィールドヘッダ部とを有する。生成部は、複数のフィールド部のうちの少なくとも１つのフィールド部に含まれるデータ値が暗号化されているデータを生成する。

[0019] このようなデータ処理装置によれば、取得したデータを、上述したデータ構造のデータへと変換できる。このため、データ処理装置によれば、上述し

たデータ構造と同様の効果を得ることができる。

図面の簡単な説明

[0020] [図1]データ処理装置の概略構成を示すブロック図である。

[図2]データ生成処理の処理手順を示すフローチャートである。

[図3]第１実施形態における特定データのデータ構造を示す説明図である。

[図4]表示処理の処理手順を示すフローチャートである。

[図5A]第１実施形態の特定データにおける認証情報Ｂで復号されるピクセルを説明する図である。

[図5B]第１実施形態の特定データにおける認証情報Ａで復号されるピクセルを説明する図である。

[図6]第１実施形態において復号されたデータ値に基づく画像を説明する図である。

[図7]第２実施形態における特定データのデータ構造を示す説明図である。

[図8A]第２実施形態の特定データにおける暗号化されていないピクセルを説明する図である。

[図8B]第２実施形態の特定データにおける認証情報Ｂで復号されるピクセルを説明する図である。

[図9A]第２実施形態の特定データにおける認証情報Ａで復号されるピクセルを説明する図である。

[図9B]第２実施形態の特定データにおける復号されたデータ値に基づく画像を説明する図である。

[図10]第３実施形態における特定データのデータ構造を示す説明図である。

[図11A]第３実施形態の特定データにおける認証情報Ｂで復号されるピクセルを説明する図である。

[図11B]第３実施形態の特定データにおける認証情報Ａで復号されるピクセルを説明する図である。

[図12]変形例の特定データを復号した状態を示す説明図である。

[図13]変形例の特定データにおけるデータ構造を説明する説明図である。

[図14A]インタレース形式におけるデータ構造を示す図である。

[図14B]インタレース形式における復号したピクセルを説明する図である。

[図15A]インタレース形式におけるデータ構造を示す図である。

[図15B]インタレース形式における復号したピクセルを説明する図である。

[図16A]インタレース形式におけるデータ構造を示す図である。

[図16B]インタレース形式における復号したピクセルを説明する図である。

[図17]波形データを特定データとして例示する図である。

発明を実施するための形態

[0021] 以下に本開示の実施形態を図面と共に説明する。

［第１実施形態］

＜１．１　データ処理装置＞

図１に示すデータ処理装置１は、データの１つである原データを取得して特定データを生成する装置である。さらに、データ処理装置１は、特定データに基づく表示を実行する装置である。

[0022] 特定データとは、原データの少なくとも一部のデータ値を暗号化したデータであり、詳しくは後述するデータ構造のデータである。

データ処理装置１は、データ取得部１２と、表示部１４と、情報受付部１６と、出力部１８と、記憶部２０と、制御部２２とを備えている。

[0023] このうち、データ取得部１２は、原データを取得する。原データは、定められた配列に従ってデータ値が並べられたデータである。データ値とは、離散化された値である。配列とは、順序を決めて並べることの意味である。

[0024] 本実施形態における原データは、撮像装置で撮像した画像データである。画像データとは、データ値として画素値を並べたデータである。画素値とは、各ピクセルにおける輝度の強さを表す値である。

[0025] 本実施形態における画像データは、例えば、医用画像であってもよい。医用画像とは、人体を撮影または計測結果を画像化したものである。医用画像には、例えば、カメラで撮影した画像、Ｘ線撮影された画像、コンピュータ断層撮影された画像、核磁気共鳴画像、内視鏡にて撮影された画像、などを

含む。

[0026] 表示部１４は、制御部２２からの信号に基づいて情報を表示する。この表示部１４として、例えば、液晶ディスプレイなどを含む。

情報受付部１６は、外部からの情報の入力を受け付ける周知の機構である。この情報受付部１６として、例えば、キーボードやマウス、タッチパネルなどの周知の入力機構を含む。なお、情報受付部１６がタッチパネルによって構成されている場合には、情報受付部１６は、表示部１４と一体に構成されていてもよい。

[0027] 出力部１８は、制御部２２からの信号に従って情報を出力する。この出力部１８が情報を出力する出力先として、ネットワーク通信網や、プリンタ、外部記憶装置などが考えられる。

[0028] 記憶部２０は、記憶内容を読み書き可能に構成された不揮発性の記憶装置である。この記憶部２０には、各種処理プログラムや各種データが記憶される。

また、制御部２２は、ＲＯＭ２４、ＲＡＭ２６、ＣＰＵ２８を少なくとも有した周知のコンピュータ備えている。

[0029] このうち、制御部２２のＲＯＭ２４には、特定データを生成するデータ生成処理を制御部２２が実行するためのプログラムが格納されている。また、制御部２２のＲＯＭ２４には、特定データに基づく表示を実行する表示処理を制御部２２が実行するためのプログラムが格納されている。

＜１．２　データ生成処理＞

図２に示すデータ生成処理が起動されると、制御部２２は、まず、データ取得部１２を介して原データを取得する（Ｓ１１０）。

[0030] 続いて、制御部２２は、Ｓ１１０で取得した原データを、規定ルールに従って区分けした複数のフィールド部３０（図３参照）を生成する（Ｓ１２０）。規定ルールとは、原データの配列におけるデータ値の配置の順序に基づいて予め規定された規則である。実施形態における規定ルールは、インタレース形式におけるフィールドの各々へと区分けすることである。インタレー

ス形式とは、画像の走査に関する形式であり、規定された画素ごとに画像の走査を飛び飛びに実施する形式である。本実施形態においては、インタレース形式の実現手法として、規定されたピクセルの順序で走査する周知のアルゴリズムであるＡｄａｍ７を用いればよい。

[0031] また、フィールド部とは、原データを規定ルールに従って区分けしたものである。本実施形態におけるフィールド部３０の各々は、インタレース形式におけるフィールドである。

[0032] さらに、制御部２２は、Ｓ１２０で生成した複数のフィールド部３０の各々にフィールドヘッダ部３２（図３参照）を付加する（Ｓ１３０）。フィールドヘッダ部３２とは、フィールド部３０の内容を表す情報であり、フィールド部３０ごとに設けられる。フィールド部の内容とは、各フィールドに含まれるデータサイズや、各フィールドの転送情報などである。

[0033] 続いて、制御部２２は、情報受付部１６を介して認証情報を取得する（Ｓ１４０）。認証情報とは、利用者を識別する情報であり、例えば、ＩＤとパスワードである。本実施形態においては、認証情報を、暗号化されるフィールド部３０のグループごとに取得する。

[0034] そして、制御部２２は、Ｓ１４０で取得した認証情報に基づいて、Ｓ１２０で生成した複数のフィールド部３０のうち少なくとも１つのフィールド部３０に含まれるデータ値の暗号化を実行する（Ｓ１５０）。Ｓ１５０における暗号化は、複数のフィールド部３０のうち規定された数のフィールド部３０に含まれるデータ値に対して実行する。本実施形態における規定された数とは、フィールド部３０の個数である。Ｓ１５０では、全てのフィールド部３０に含まれるデータ値が暗号化される。

[0035] また、暗号化とは、認証情報を知らない第三者がデータを閲覧不可能とする処理である。本実施形態においては、図３に示すように、複数のフィールド部３０のうち、２つの１／６４部フィールド、及び１／３２部フィールドの３つのフィールド部３０（即ち、第１グループ）については、Ｓ１４０で取得した認証情報のうちの認証情報Ｂを用いて暗号化する。複数のフィール

ド部３０のうち、残りの４つのフィールド部３０（即ち、第２グループ）については、Ｓ１４０で取得した認証情報のうちの認証情報Ａを用いて暗号化する。これらの認証情報は、フィールド部３０に付加される。

[0036] 続いて、制御部２２は、Ｓ１２０からＳ１５０までのステップが実行された原データを特定データとして再構成して記憶する（Ｓ１６０）。

特定データとは、配列に従ってデータ値が並べられたデータであり、少なくとも一部のフィールド部３０が暗号化されたデータである。本実施形態における特定データは、図３に示すように、複数のフィールド部３０と、各フィールド部３０に対するフィールドヘッダ部３２と、データ全体の内容を表すファイルヘッダ部３４とを備えている。

[0037] 本実施形態においては、複数のフィールド部３０のうちの第１グループのフィールド部３０については、認証情報Ｂを用いて暗号化されている。また、第２グループのフィールド部３０については、認証情報Ｂとは異なる情報である認証情報Ａを用いて暗号化されている。

[0038] また、再構成とは、複数のフィールド部３０と、複数のフィールドヘッダ部３２とを備えたデータを生成することである。本実施形態においては、原データを特定データへと変換するという意味である。

[0039] なお、Ｓ１６０において、特定データを記憶する記憶先は、記憶部２０であってもよいし、外部記憶装置であってもよい。外部記憶装置には、データ処理装置１に接続されたサーバを含む。

[0040] 制御部２２は、その後、本データ生成処理を終了する。

つまり、本データ生成処理では、原データをインタレース形式のデータへと変換し、そのインタレース形式のデータにおけるフィールド部３０の一部を、認証情報Ａを用いて暗号化する。また、残りのフィールド部３０を、認証情報Ｂを用いて暗号化する。そして、これらの暗号化されたフィールド部３０を備えた特定データを生成する。

[0041] このため、特定データは、図３に示すように、複数のフィールド部３０と、フィールドヘッダ部３２と、ファイルヘッダ部３４とを備え、フィールド

部３０に含まれるデータ値が暗号化されたデータ構造となる。

＜１．３　表示処理＞

次に、図４に示す表示処理が起動されると、制御部２２は、まず、情報受付部１６を介して指定された特定データを取得する（Ｓ２１０）。

[0042] 続いて、制御部２２は、情報受付部１６を介して認証情報を取得する（Ｓ２２０）。以下、Ｓ２２０で取得した認証情報を入力情報と称す。

そして、制御部２２は、Ｓ２２０で取得した入力情報を、Ｓ２１０で取得した特定データに含まれる認証情報に照合し、認証に成功したか否かを判定する（Ｓ２３０）。本実施形態では、特定データに含まれる認証情報と入力情報が一致していれば、認証に成功したものと判定し、不一致であれば、認証に成功していないものとすればよい。

[0043] このＳ２３０での判定の結果、認証に成功していなければ（Ｓ２３０：ＮＯ）、制御部２２は、特定データに基づいて暗号化された画像を表示部１４に表示する（Ｓ２４０）。

制御部２２は、その後、本表示処理を終了する。

[0044] 一方、Ｓ２３０での判定の結果、認証に成功していれば（Ｓ２３０：ＹＥＳ）、制御部２２は、認証に成功したフィールド部３０に含まれるデータ値を復号する（Ｓ２５０）。続いて、制御部２２は、復号したデータ値に基づく画像を表示部１４に表示する（Ｓ２６０）。

[0045] すなわち、複数の認証情報のうち、認証情報Ｂに対する認証に成功した場合、Ｓ２６０では、制御部２２は、図５Ａに示すように、認証情報Ｂで暗号化されたフィールド部３０に含まれ、Ｓ２５０で復号されたデータ値に基づく画像を表示部１４に表示する。また、複数の認証情報のうち、認証情報Ａに対する認証に成功した場合、Ｓ２６０では、制御部２２は、図５Ｂに示すように、認証情報Ａで暗号化されたフィールド部３０に含まれ、Ｓ２５０で復号されたデータ値に基づく画像を表示部１４に表示する。

[0046] このように、一部のデータ値に基づく画像を表示する場合、復号されていないデータ値に対応するピクセルは、復号されたデータ値に基づいて補完さ

れていてもよい。

一方、複数の認証情報のうち、認証情報Ａ、及び認証情報Ｂの双方での認証に成功した場合、Ｓ２６０では、制御部２２は、図６に示すように、全てのフィールド部３０に含まれるデータ値（即ち、全画素値）に基づく画像を表示部１４に表示する。

[0047] なお、図５Ａ，図５Ｂ，図６におけるハッチングの相違は、フィールド部３０の相違を意味する。

制御部２２は、その後、本表示処理を終了する。

[0048] つまり、表示処理では、認証に成功したフィールド部３０に含まれるデータ値を復号し、その復号されたデータ値に基づく画像を表示する。

［１．４　第１実施形態の効果］

（１Ａ）　したがって、メンテナンスの担当者などの利用者の一部に、複数の認証情報のうちの一部だけを教示すれば、その利用者は、特定データの一部だけを復号でき、特定データの全ては復号できない。

[0049] したがって、認証情報のうちの一部の認証情報を知る利用者は、特定データがどのような情報であるのかの大枠、即ち、必要最低限の情報を認識できる。

この結果、医療の用途に用いられる画像を撮像して管理するシステムのメンテナンスの効率化を図ることができる。

[0050] （１Ｂ）　一方、認証情報のうちの一部の認証情報を知る利用者は、特定データの全容を把握することはできない。

よって、上述したデータ構造を有した特定データによれば、データの機密性を担保できる。

[0051] （１Ｃ）　つまり、上述したデータ構造を有した特定データによれば、複数の認証情報を使い分けて復号可能な範囲を変更することで、医療の用途に用いられる画像を撮像して管理するシステムの利用者が最低限必要な情報を認識可能としつつ、情報の機密性を確保できる。

[0052] （１Ｄ）　さらに、表示処理において、認証に成功したフィールド部３０

だけに含まれ、復号されたデータ値に基づく画像を表示部１４に表示する場合に、復号されていないデータ値に対応するピクセルを、復号されたデータ値に基づいて補完してもよい。このようにすれば、情報の機密性を確保しつつも、その画像の視認性を向上させることができる。

[0053] （１Ｅ） なお、全ての認証情報を知っている利用者であれば、特定データの全容を認識できる。

［第２実施形態］

第２実施形態は、第１実施形態とは、主として、特定データのデータ構造が異なる。このため、本実施形態においては、第１実施形態と相違する特定データのデータ構造について説明する。

[0054] ＜２．１ 特定データ＞

本実施形態の特定データは、図７に示すように、複数のフィールド部３０と、フィールドヘッダ部３２と、ファイルヘッダ部３４とを備える。

[0055] 本実施形態においては、複数のフィールド部３０のうちの少なくとも１つのフィールド部３０に含まれるデータ値は暗号化しない。

すなわち、データ生成処理のＳ１５０では、複数のフィールド部３０のうち、２つのフィールド部３０を第１グループとして、認証情報Ｂを用いて暗号化する。そして、複数のフィールド部３０のうち、４つのフィールド部３０を第２グループとして、認証情報Ａを用いて暗号化する。残りの１つのフィールド部３０については、暗号化することなく、Ｓ１６０にて、特定データを生成する。

[0056] さらに、表示処理のＳ２４０では、制御部２２は、図８Ａに示すように暗号化されていないフィールド部３０のデータ値に基づく画像を表示部１４に表示する。

一方、複数の認証情報のうち認証情報Ｂに対する認証に成功した場合、表示処理のＳ２６０では、制御部２２は、図８Ｂに示すように、暗号化されていないフィールド部３０のデータ値、及び、認証情報Ｂで暗号化されたフィールド部３０に含まれ、Ｓ２５０で復号されたデータ値に基づく画像を表示

部１４に表示する。また、複数の認証情報のうち認証情報Ａに対する認証に成功した場合、表示部のＳ２６０では、制御部２２は、図９Ａに示すように、暗号化されていないフィールド部３０のデータ値、及び、認証情報Ａで暗号化されたフィールド部３０に含まれ、Ｓ２５０で復号されたデータ値に基づく画像を表示部１４に表示する。

[0057] 認証情報Ａ，認証情報Ｂの双方の認証に成功した場合には、制御部２２は、図９Ｂに示すように、全てのフィールド部３０に含まれるデータ値に基づく画像を表示部１４に表示する。

[0058] なお、図８Ａ，図８Ｂ，図９Ａ，図９Ｂにおけるハッチングの相違は、フィールド部３０の相違を意味する。

［２．２　第２実施形態の効果］

このようなデータ構造を有した特定データによれば、利用者は、暗号化されていないフィールド部３０については、復号することなくデータ値を把握できる。このため、利用者は、暗号化していないフィールド部３０のデータ値から、特定データの全容の一部を把握できる。

[0059] 一方、利用者は、全ての認証情報を知っていれば、特定データの全容を認識できる。

［第３実施形態］

第３実施形態は、第１実施形態とは、主として、特定データのデータ構造が異なる。このため、本実施形態においては、第３実施形態と相違する特定データのデータ構造について説明する。

[0060] ＜３．１　特定データ＞

本実施形態の特定データは、図１０に示すように、ファイルヘッダ部３４と、本体フィールド部４０と、重複フィールド部４２とを備える。

[0061] 本体フィールド部４０は、全てのフィールド部３０を有している。すなわち、本体フィールド部４０は、原データに含まれるデータ値を、規定ルールに従って分類した全てのフィールド部３０である。

[0062] 重複フィールド部４２は、本体フィールド部４０に含まれるフィールド部

３０の一部と同じ内容のフィールド部３０である。この同じ内容のフィールド部３０とは、配列における位置及びデータ値が重複する少なくとも１つのフィールド部３０である。すなわち、重複フィールド部４２におけるフィールド部３０の各々は、本体フィールド部４０に含まれるフィールド部３０と、同じデータ値を有している。本実施形態における重複フィールド部４２のフィールド部３０の個数は、３つである。

[0063] なお、本実施形態において、本体フィールド部４０におけるフィールド部３０の各々は、認証情報Ｂを用いて暗号化される。また、重複フィールド部４２におけるフィールド部３０の各々は、認証情報Ｂとは異なる認証情報Ａを用いて暗号化される。

[0064] すなわち、データ生成処理のＳ１５０では、本体フィールド部４０におけるフィールド部３０の各々を第２グループとして、認証情報Ａを用いて暗号化する。重複フィールド部４２におけるフィールド部３０の各々を第１グループとして、認証情報Ｂを用いて暗号化する。

[0065] さらに、表示処理のＳ２４０では、制御部２２は、特定データに基づいて暗号化された画像を表示部１４に表示する。

一方、表示処理のＳ２６０では、制御部２２は、認証情報Ｂによる認証に成功していれば、図１１Ａに示すように、重複フィールド部４２におけるフィールド部３０のデータ値を復号し、その復号されたデータ値に基づく画像を表示部１４に表示する。また、認証情報Ａによる認証に成功した場合には、Ｓ２６０では、制御部２２は、図１１Ｂに示すように、本体フィールド部４０におけるフィールド部３０に含まれるデータ値を復号し、その復号されたデータ値に基づく画像を表示部１４に表示する。

[0066] なお、図１１Ａ，図１１Ｂにおけるハッチングの相違は、フィールド部３０の相違を意味する。

［３．２　第３実施形態の効果］

このようなデータ構造によれば、重複フィールド部４２を復号した場合には、データ値の一部が認識可能となり、本体フィールド部４０を復号した場

合には、全てのデータ値を認識可能となる。

[0067] よって、このようなデータ構造によれば、複数の認証情報を使い分けて復号可能な範囲を変更することで、データの機密性を担保しつつ、データの利用における利便性を高めることができる。

［４． その他の実施形態］

以上、本開示の実施形態について説明したが、本開示は上記実施形態に限定されるものではなく、本開示の要旨を逸脱しない範囲において、様々な態様にて実施することが可能である。

[0068] （４．１） 上記第１実施形態から第３実施形態では、特定データにおける配列を８行８列であるものとして説明したが、特定データにおける配列は、これに限るものではない。

[0069] 例えば、特定データにおける配列は、図１２に示すように、１６行１６列であってもよい。この場合、特定データのデータ構造では、図１３に示すように、フィールド部３０の個数を増加させることで、上述した効果が得られる。

[0070] なお、図１２におけるハッチングの相違は、フィールド部３０の相違を意味する。

また、特定データにおける配列は、これに限るものではなく、順序を決めて並べられたものであれば、１行Ｍ列であってもよいし、Ｍ行１列であってもよいし、Ｍ行Ｎ列であってもよい。ただし、Ｍ，Ｎは１以上の整数である。

[0071] （４．２） 上記実施形態においては、インタレース形式の走査方法として、周知のＡｄａｍ７を用いていたが、インタレース形式の走査方法は、これに限るものではない。

インタレース形式の走査方法は、例えば、図１４Ａ，図１４Ｂに示すように、特定の行と、その特定の行から規定数の行の後の行を第１のフィールドとし、残りの行を第２のフィールドとして、画像の走査を飛び飛びに実施する形式であってもよい。

[0072] また、インタレース形式の走査方法は、例えば、図１５Ａ，図１５Ｂに示すように、特定の列と、その特定の列から規定数の列の後の列を第１のフィールドとし、残りの列を第２のフィールドとして、画像の走査を飛び飛びに実施する形式であってもよい。

[0073] さらには、インタレース形式の走査方法は、例えば、図１６Ａ，図１６Ｂに示すように、特定の行における規定されたピクセルを第１のフィールドとし、残りの全てのピクセルを第２のフィールドとして、画像の走査を飛び飛びに実施する形式であってもよい。

[0074] なお、図１４Ｂ，図１５Ｂ，図１６Ｂにおけるハッチングの相違は、第１のフィールドと第２のフィールドとの相違を意味する。

（４．３） 上記実施形態では、１つの認証情報で複数のフィールド部３０を暗号化していたが、１つの認証情報で暗号化する対象は、これに限るものではなく、例えば、１つの認証情報で１つのフィールド部３０を暗号化してもよい。すなわち、フィールド部３０ごとに異なる認証情報を用いて暗号化されていてもよい。

[0075] （４．４） 上記実施形態では、原データを画像データとして取得していたが、原データとして取得する対象は、これに限るものではない。原データとして取得する対象は、例えば、図１７に示すように、波形における振幅を標本化した値をデータ値とした波形データであってもよい。この波形データは、計測機器にて計測した計測結果を示すものであってもよい。

[0076] （４．５） 上記実施形態における制御部２２が実行する機能の一部または全部は、一つあるいは複数のＩＣ等によりハードウェア的に構成されていてもよい。

（４．６） 上記実施形態においては、ＲＯＭ２４にプログラムが格納されていたが、プログラムを格納する記憶媒体は、これに限るものではなく、半導体メモリなどの非遷移的実体的記憶媒体に格納されていてもよい。

[0077] （４．７） また、制御部２２は非遷移的実体的記録媒体に格納されたプログラムを実行してもよい。このプログラムが実行されることで、プログラ

ムに対応する方法が実現される。

[0078] （４．８） なお、上記実施形態の構成の一部を省略した態様も本開示の実施形態である。また、上記実施形態と変形例とを適宜組み合わせて構成される態様も本開示の実施形態である。また、特許請求の範囲に記載した文言によって特定される本開示の本質を逸脱しない限度において考え得るあらゆる態様も本開示の実施形態である。

[0079] （４．９）上記実施形態の説明で用いる符号を特許請求の範囲にも適宜使用しているが、各請求項に係る本開示の理解を容易にする目的で使用しており、各請求項に係る本開示の技術的範囲を限定する意図ではない。

［５． 対応関係］

データ生成処理のＳ１１０を実行することで得られる機能が、取得部に相当する。Ｓ１２０を実行することで得られる機能が、分類部に相当する。さらに、Ｓ１３０を実行することで得られる機能が、付加部に相当する。そして、Ｓ１４０～Ｓ１５０を実行することで得られる機能が、暗号処理部に相当する。Ｓ１６０を実行することで得られる機能が、生成部に相当する。

請求の範囲

[請求項1] データ処理装置（１）であって、

配列に従ってデータ値が並べられたデータを取得する取得部（２２，Ｓ１１０）と、

前記取得部で取得したデータを、前記配列におけるデータ値の配置の順序に基づいて規定された規定ルールに従って区分けした複数のフィールド部を生成する分類部（２２，Ｓ１２０）と、

前記分類部で生成された複数のフィールド部の各々の内容を表すフィールドヘッダ部を付加する付加部（２２，Ｓ１３０）と、

前記分類部で生成された複数のフィールド部のうちの少なくとも１つのフィールド部に含まれるデータ値を暗号化する暗号処理部（２２，Ｓ１４０，Ｓ１５０）と、

前記分類部で生成された複数のフィールド部、前記付加部で付加されたフィールドヘッダ部、及び前記暗号処理部で暗号化されたフィールド部に基づいて、複数のフィールド部（３０）と、前記複数のフィールドヘッダ部（３２）とを有し、前記複数のフィールド部のうちの少なくとも１つのフィールド部に含まれるデータ値が暗号化されているデータを生成する生成部（２２，Ｓ１６０）と

を備える、データ処理装置。

[請求項2] 配列に従ってデータ値が並べられたデータのデータ構造であって、

前記配列におけるデータ値の配置の順序に基づいて規定された規定ルールに従って、前記データを区分けした複数のフィールド部（３０）と、

前記複数のフィールド部の各々の内容を表す複数のフィールドヘッダ部（３２）と

を備え、

前記複数のフィールド部のうちの少なくとも１つのフィールド部に含まれるデータ値が暗号化されている、データ構造。

[請求項3] 前記複数のフィールド部のうちの１つのフィールド部は、暗号化されていない、請求項２に記載のデータ構造。

[請求項4] 前記複数のフィールド部のうち、前記データ値が暗号化されたフィールド部は、

認証に用いられる情報である認証情報を更に有する、請求項２または請求項３に記載のデータ構造。

[請求項5] 前記認証情報は、

前記フィールド部ごとに規定されている、請求項４に記載のデータ構造。

[請求項6] 前記配列における配置、及び前記データ値が重複する少なくとも１つのフィールド部である重複フィールド部（４２）を更に備え、

前記複数のフィールド部において、前記重複フィールド部以外の全てのフィールド部を本体フィールド部（４０）とし、

前記本体フィールド部に対する認証情報と、前記重複フィールド部に対する認証情報とが異なる、請求項４または請求項５に記載のデータ構造。

[請求項7] 前記データ値は、画素値であり、

前記フィールド部は、

インタレース形式におけるフィールドである、請求項２から請求項６までのいずれか一項に記載のデータ構造。

[請求項8] 前記データ値は、波形における振幅を標本化した値である、請求項２から請求項６までのいずれか一項に記載のデータ構造。

[図1]

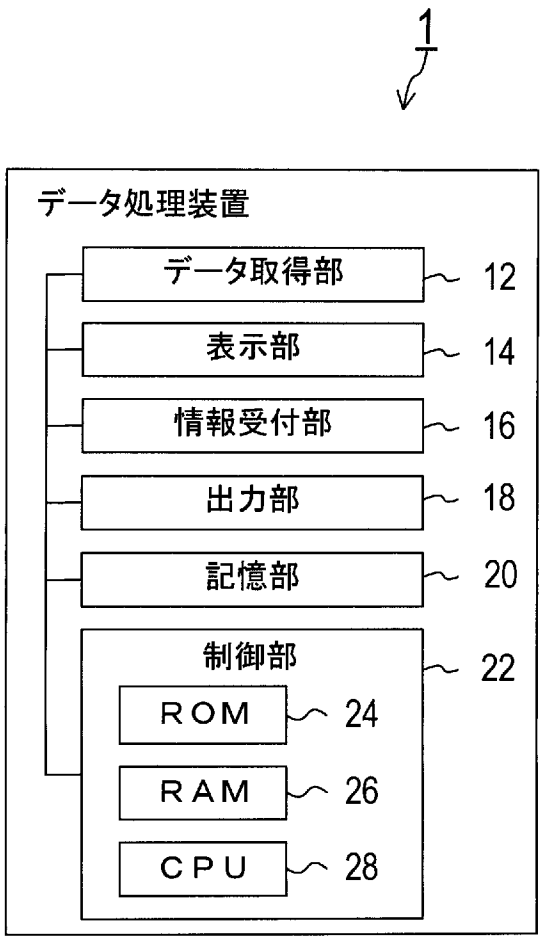
1
データ処理装置
データ取得部
12
表示部
14
情報受付部
16
出力部
18
記憶部
20
制御部
22
ROM
24
RAM
26
CPU
28

FIG. 1

[図2]

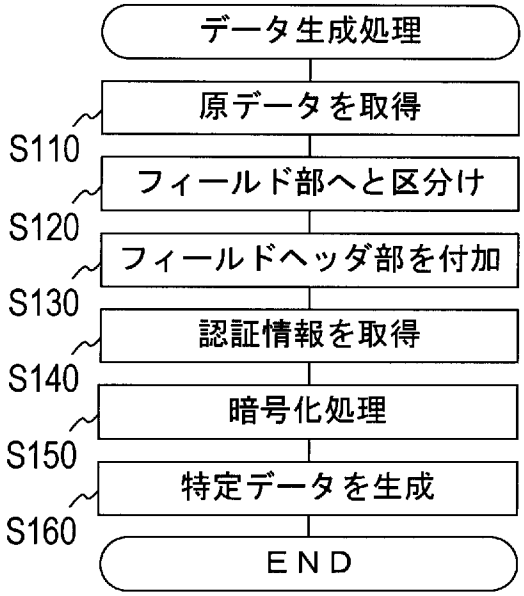
データ生成処理
原データを取得
S110
フィールド部へと区分け
S120
フィールドヘッダ部を付加
S130
認証情報を取得
S140
暗号化処理
S150
特定データを生成
S160
ＥＮＤ

FIG. 2

[図3]

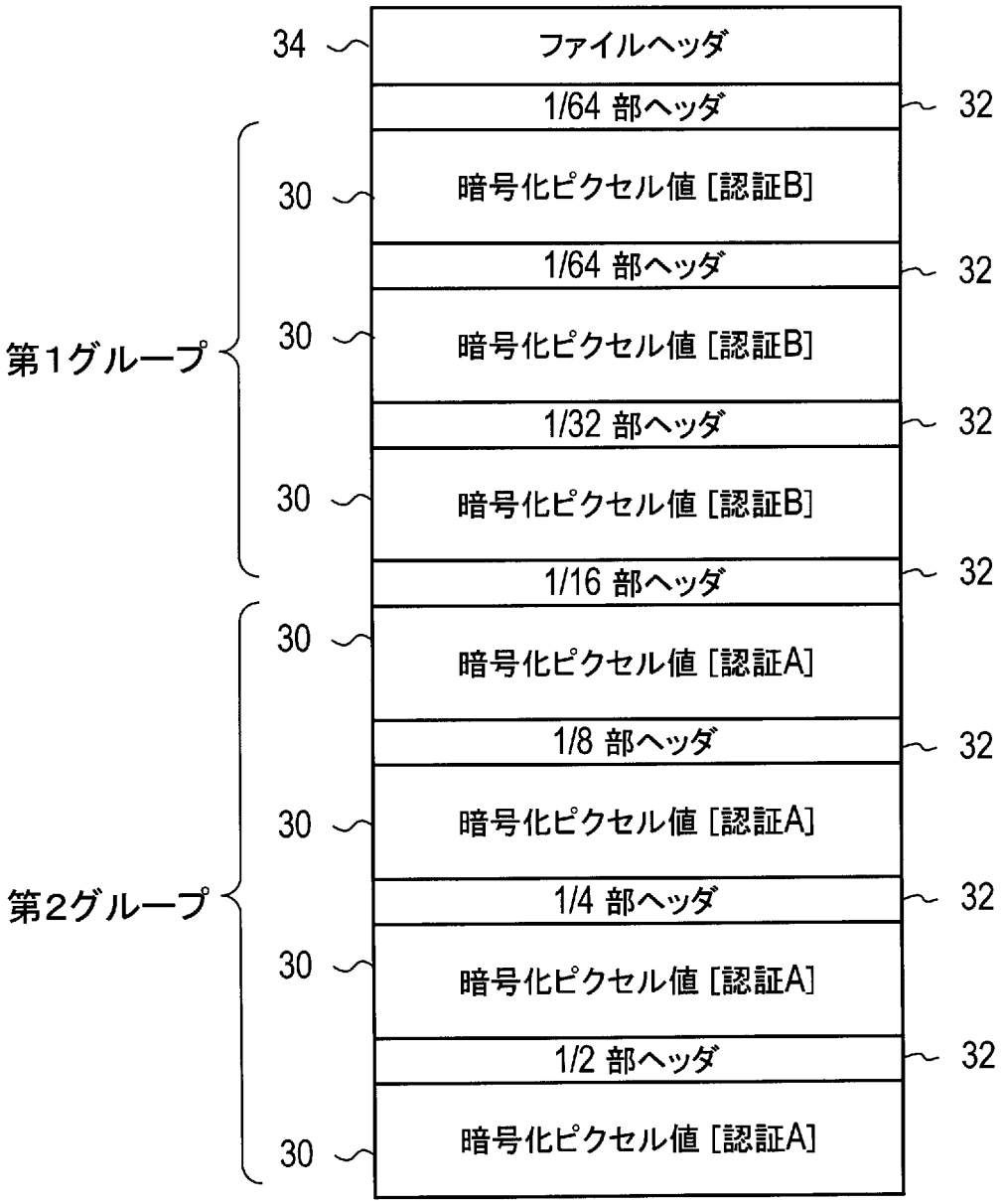
34
ファイルヘッダ
1/64 部ヘッダ
32
30
暗号化ピクセル値 [認証B]
1/64 部ヘッダ
32
30
暗号化ピクセル値 [認証B]
1/32 部ヘッダ
32
30
暗号化ピクセル値 [認証B]
1/16 部ヘッダ
32
第1グループ
30
暗号化ピクセル値 [認証A]
1/8 部ヘッダ
32
30
暗号化ピクセル値 [認証A]
1/4 部ヘッダ
32
第2グループ
30
暗号化ピクセル値 [認証A]
1/2 部ヘッダ
32
30
暗号化ピクセル値 [認証A]

FIG. 3

[図4]

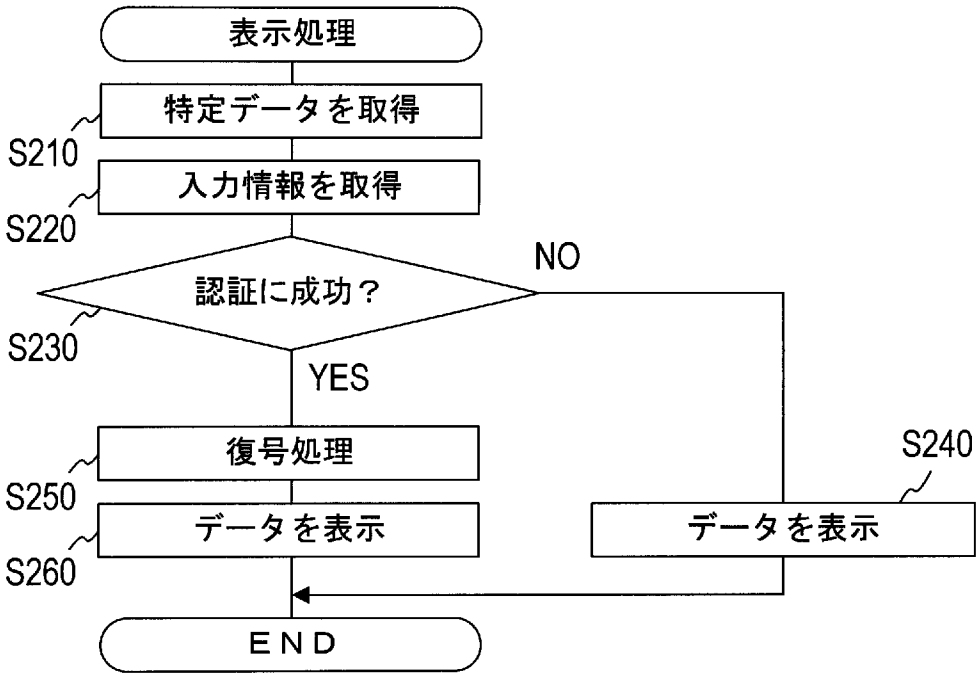
表示処理
特定データを取得
S210
入力情報を取得
S220
認証に成功？
S230
NO
YES
復号処理
S250
データを表示
S260
S240
データを表示
END

FIG. 4

[図5A]

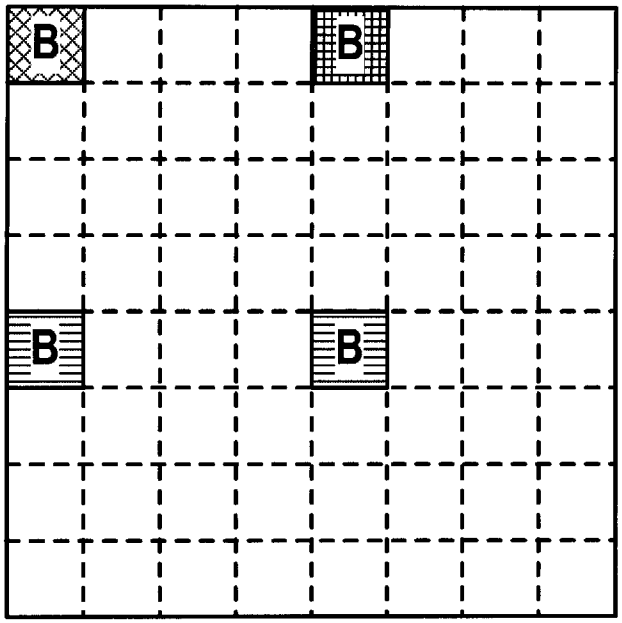

FIG. 5A

[図5B]

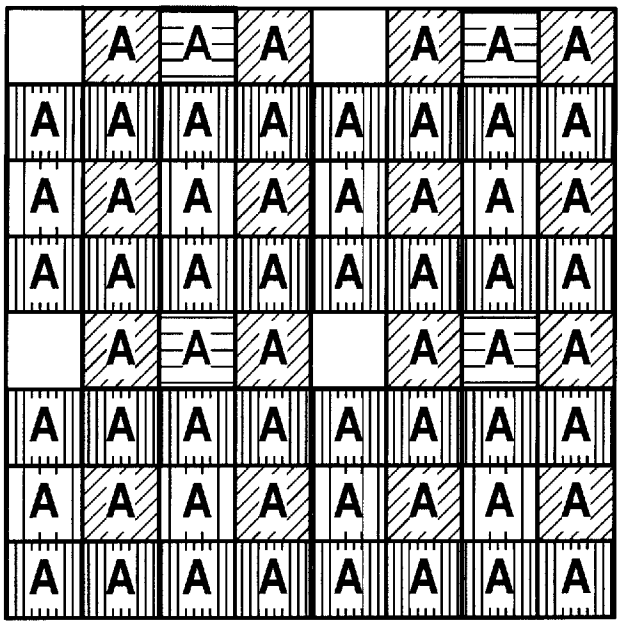

FIG. 5B

[図6]

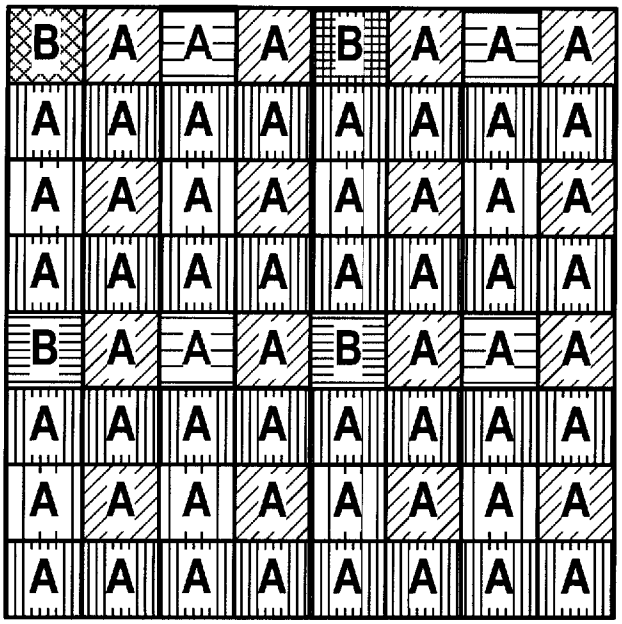
B A A A B A A A
A A A A A A A A
A A A A A A A A
A A A A A A A A
B A A A B A A A
A A A A A A A A
A A A A A A A A
A A A A A A A A

FIG. 6

[図7]

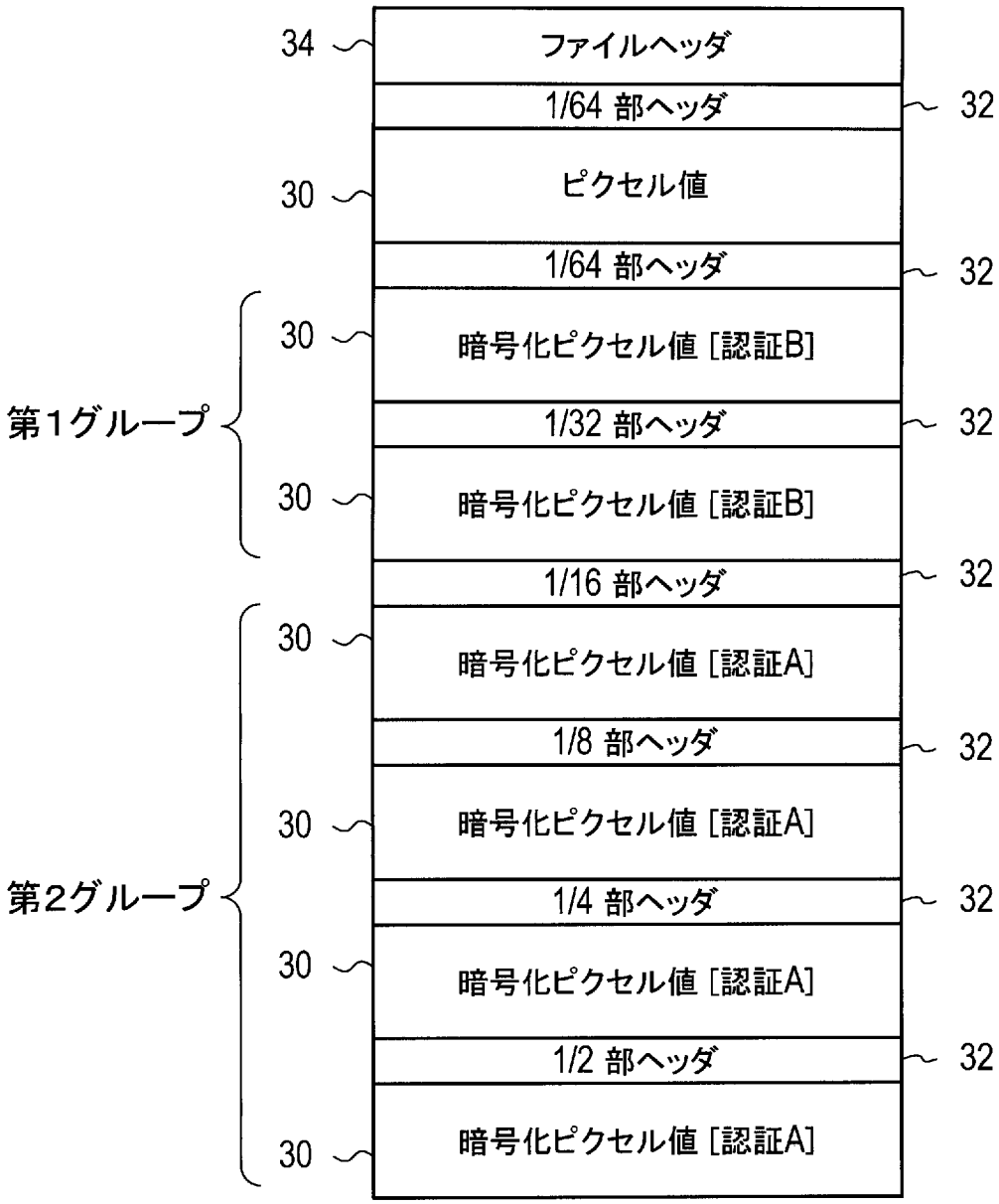
34
ファイルヘッダ
1/64 部ヘッダ
32
30
ピクセル値
1/64 部ヘッダ
32
30
暗号化ピクセル値 [認証B]
第1グループ
1/32 部ヘッダ
32
30
暗号化ピクセル値 [認証B]
1/16 部ヘッダ
32
30
暗号化ピクセル値 [認証A]
1/8 部ヘッダ
32
30
暗号化ピクセル値 [認証A]
第2グループ
1/4 部ヘッダ
32
30
暗号化ピクセル値 [認証A]
1/2 部ヘッダ
32
30
暗号化ピクセル値 [認証A]

FIG. 7

[図8A]

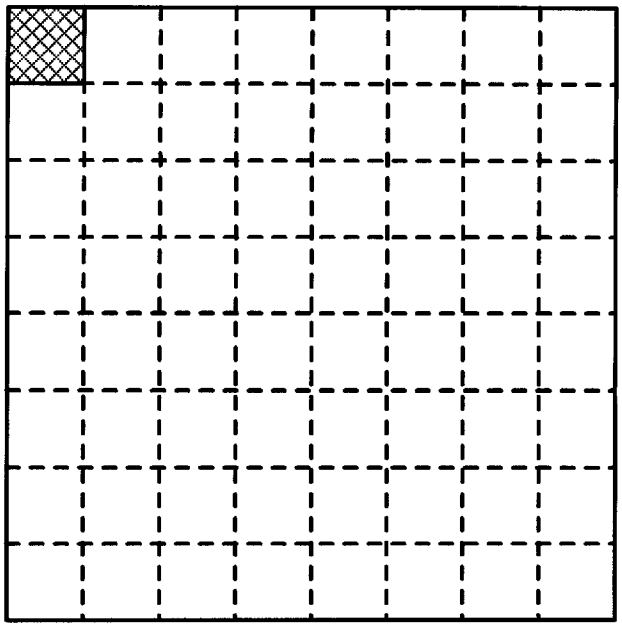

FIG. 8A

[図8B]

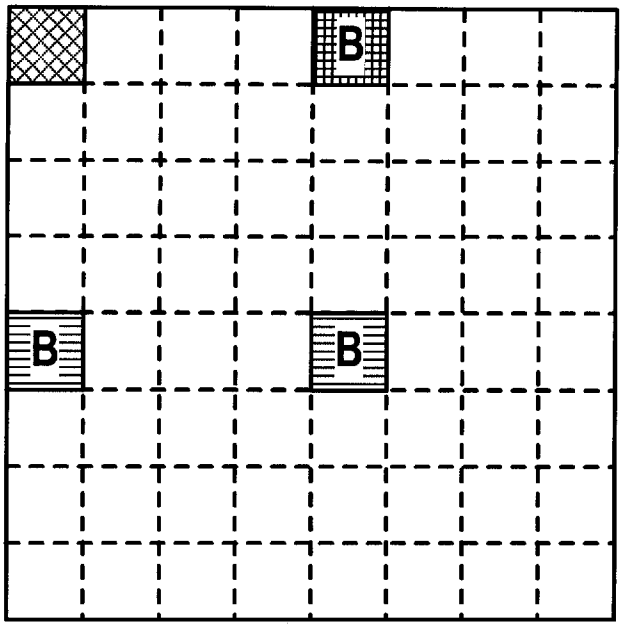

FIG. 8B

[図9A]

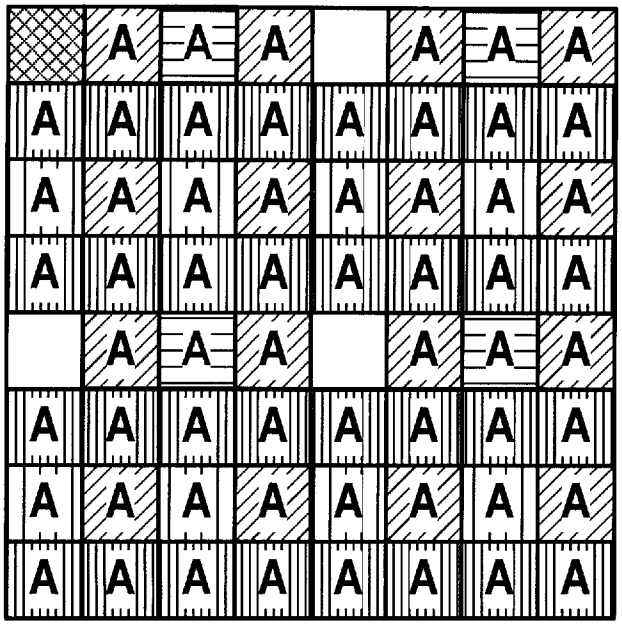

FIG. 9A

[図9B]

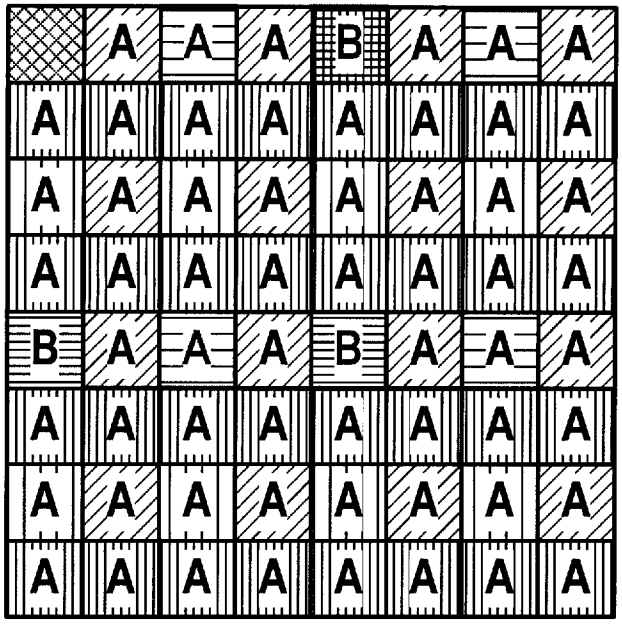
A A A B A A A
A A A A A A A A
A A A A A A A A
A A A A A A A A
B A A A B A A A
A A A A A A A A
A A A A A A A A
A A A A A A A A

FIG. 9B

[図10]

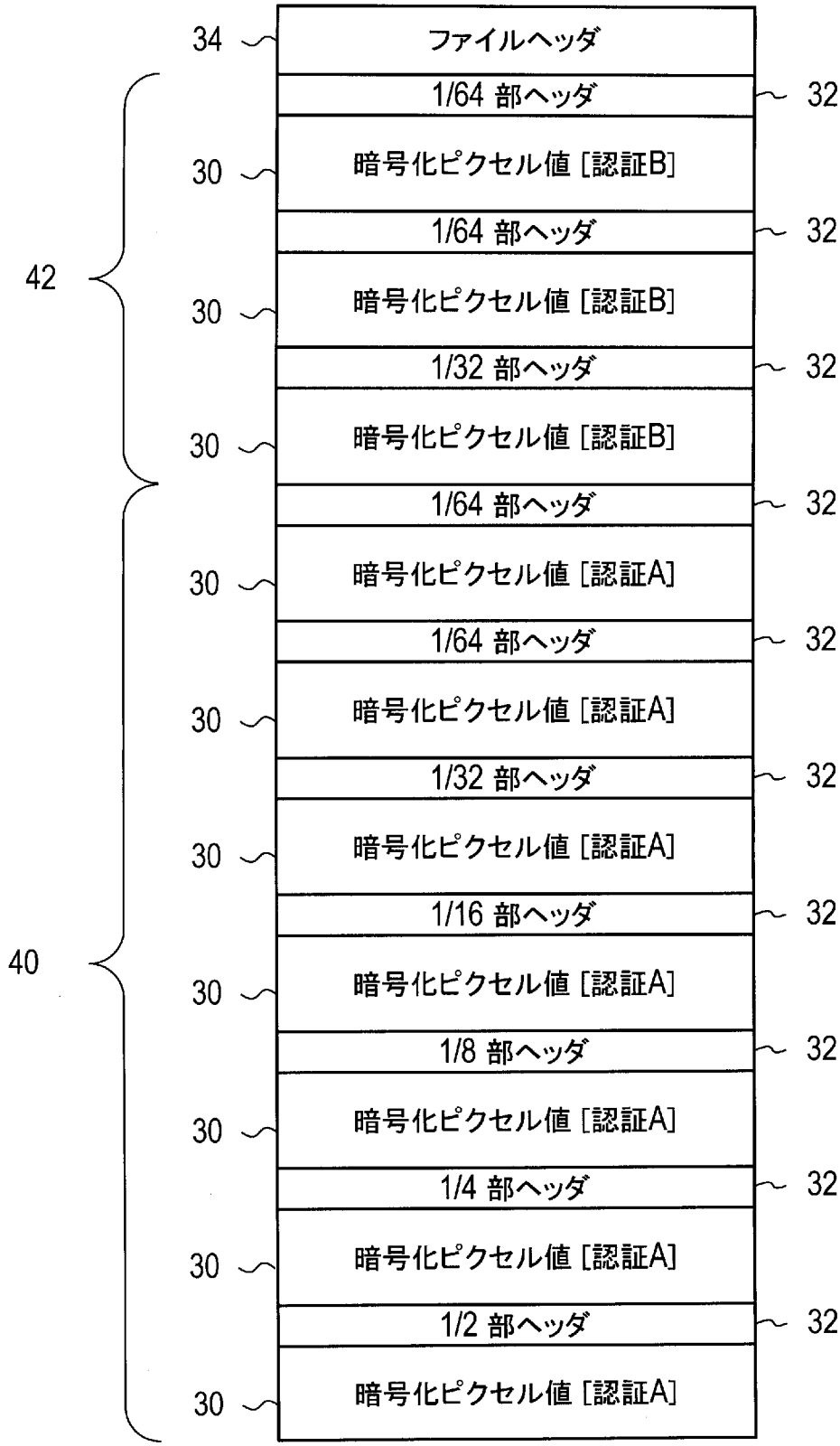
34
ファイルヘッダ
1/64 部ヘッダ
32
30
暗号化ピクセル値 [認証B]
1/64 部ヘッダ
32
42
30
暗号化ピクセル値 [認証B]
1/32 部ヘッダ
32
30
暗号化ピクセル値 [認証B]
1/64 部ヘッダ
32
30
暗号化ピクセル値 [認証A]
1/64 部ヘッダ
32
30
暗号化ピクセル値 [認証A]
1/32 部ヘッダ
32
30
暗号化ピクセル値 [認証A]
1/16 部ヘッダ
32
40
30
暗号化ピクセル値 [認証A]
1/8 部ヘッダ
32
30
暗号化ピクセル値 [認証A]
1/4 部ヘッダ
32
30
暗号化ピクセル値 [認証A]
1/2 部ヘッダ
32
30
暗号化ピクセル値 [認証A]

FIG. 10

[図11A]

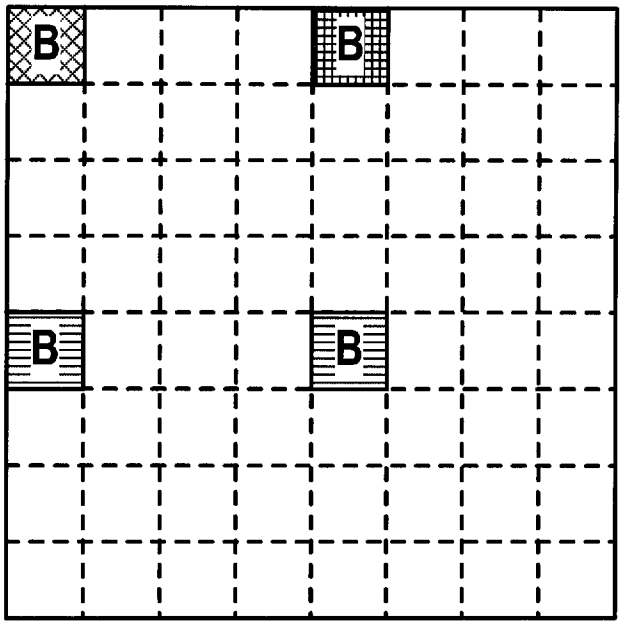

FIG. 11A

[図11B]

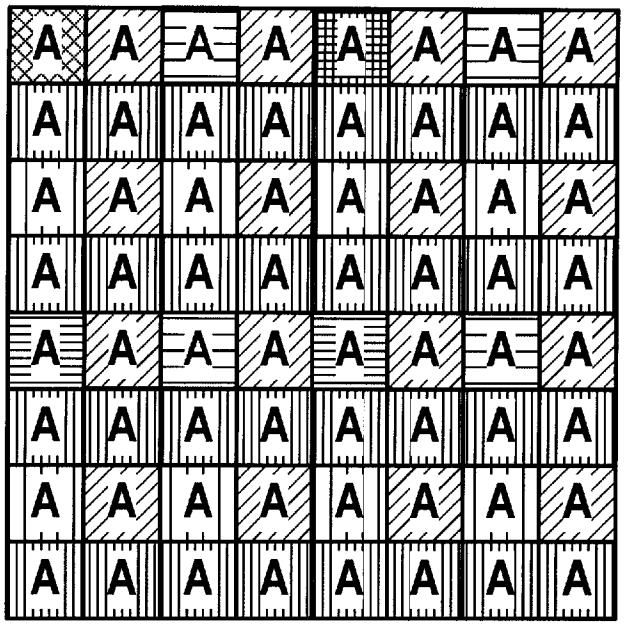

FIG. 11B

[図12]

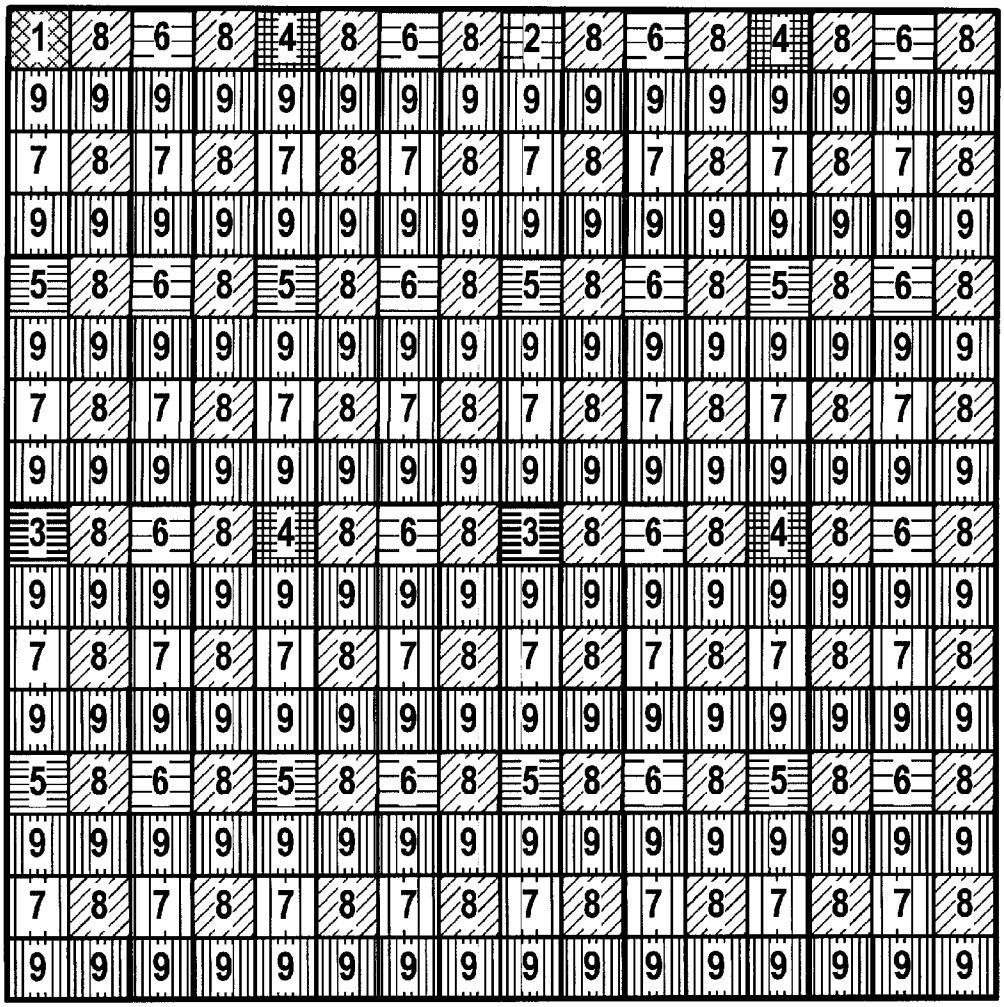
1 8 6 8 4 8 6 8 2 8 6 8 4 8 6 8
9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9
7 8 7 8 7 8 7 8 7 8 7 8 7 8 7 8
9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9
5 8 6 8 5 8 6 8 5 8 6 8 5 8 6 8
9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9
7 8 7 8 7 8 7 8 7 8 7 8 7 8 7 8
9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9
3 8 6 8 4 8 6 8 3 8 6 8 4 8 6 8
9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9
7 8 7 8 7 8 7 8 7 8 7 8 7 8 7 8
9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9
5 8 6 8 5 8 6 8 5 8 6 8 5 8 6 8
9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9
7 8 7 8 7 8 7 8 7 8 7 8 7 8 7 8
9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9

FIG. 12

[図13]

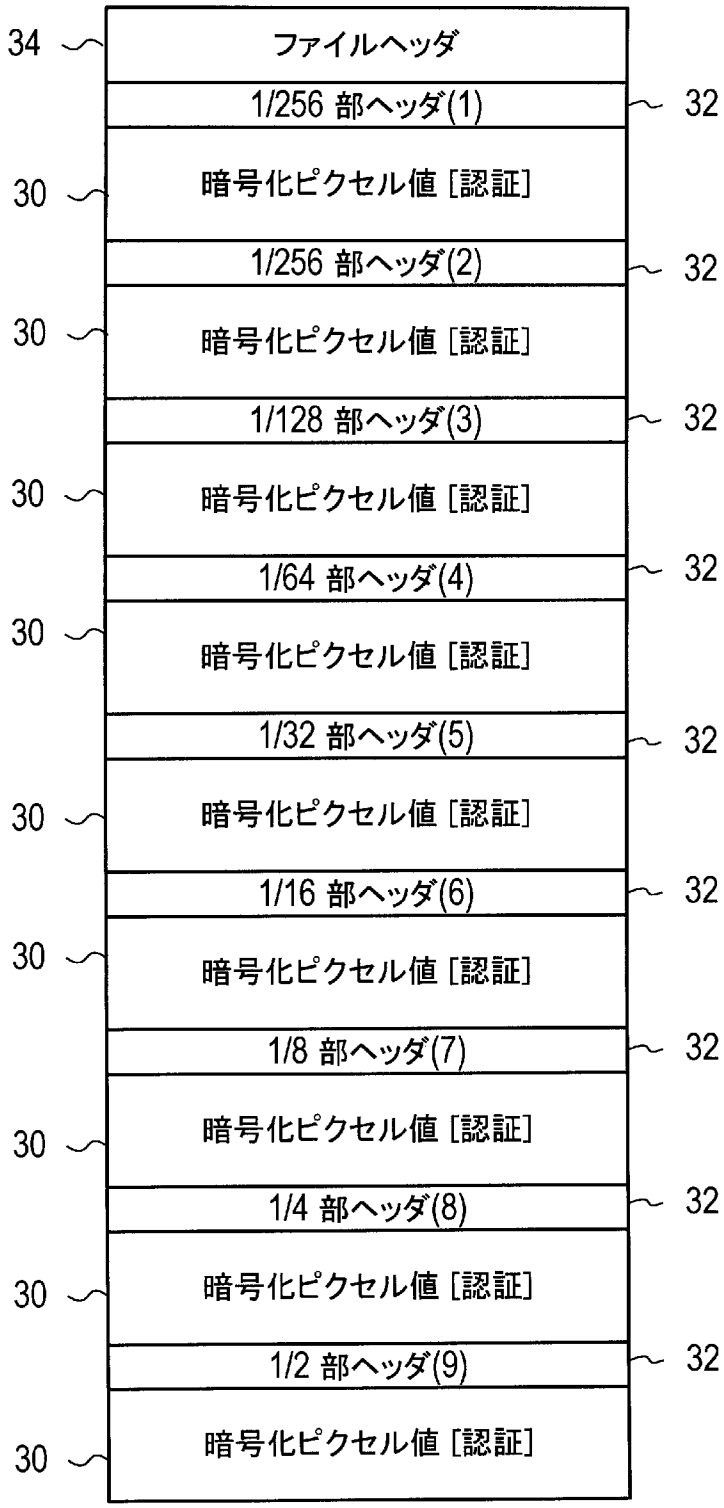
34
ファイルヘッダ
1/256 部ヘッダ(1)
32
30
暗号化ピクセル値 [認証]
1/256 部ヘッダ(2)
32
30
暗号化ピクセル値 [認証]
1/128 部ヘッダ(3)
32
30
暗号化ピクセル値 [認証]
1/64 部ヘッダ(4)
32
30
暗号化ピクセル値 [認証]
1/32 部ヘッダ(5)
32
30
暗号化ピクセル値 [認証]
1/16 部ヘッダ(6)
32
30
暗号化ピクセル値 [認証]
1/8 部ヘッダ(7)
32
30
暗号化ピクセル値 [認証]
1/4 部ヘッダ(8)
32
30
暗号化ピクセル値 [認証]
1/2 部ヘッダ(9)
32
30
暗号化ピクセル値 [認証]

FIG. 13

[図14A]

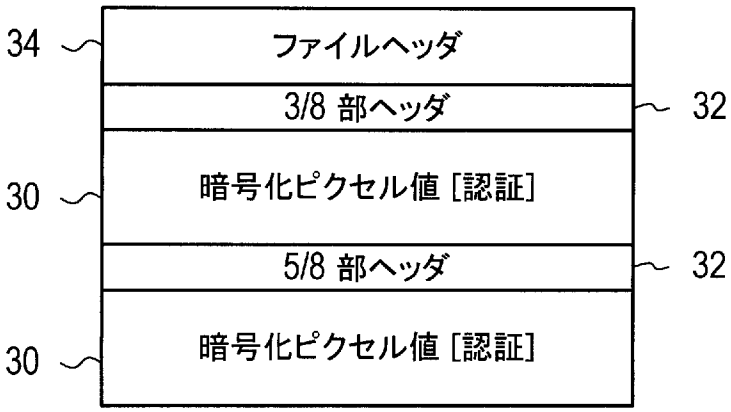

FIG. 14A

[図14B]

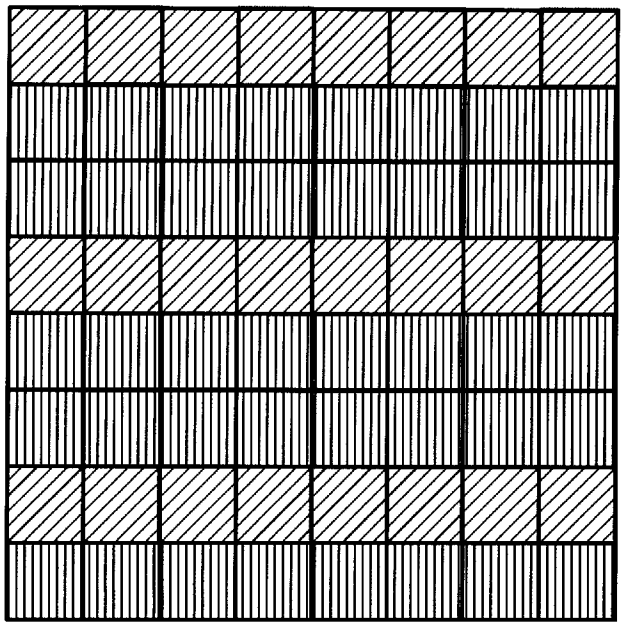

FIG. 14B

[図15A]

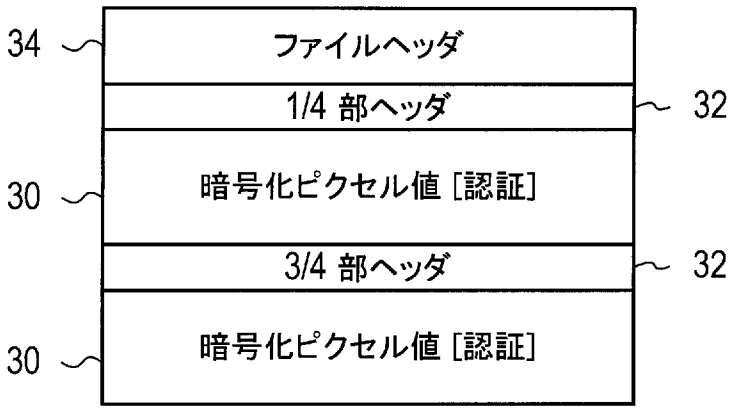

FIG. 15A

[図15B]

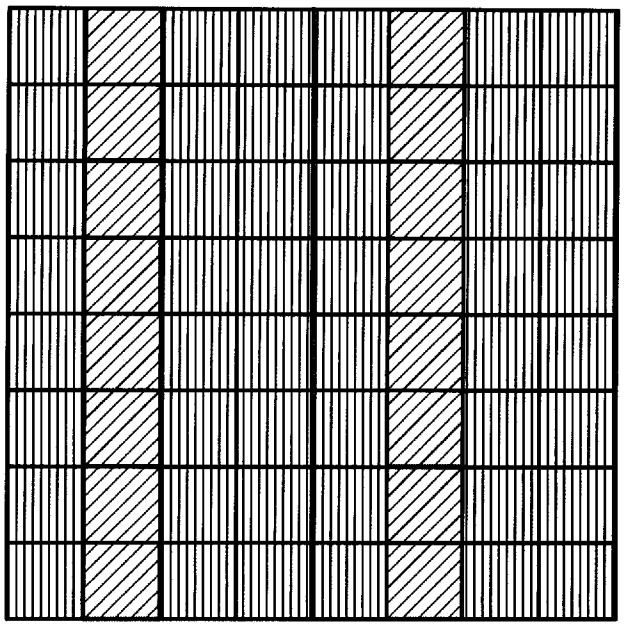

FIG. 15B

[図16A]

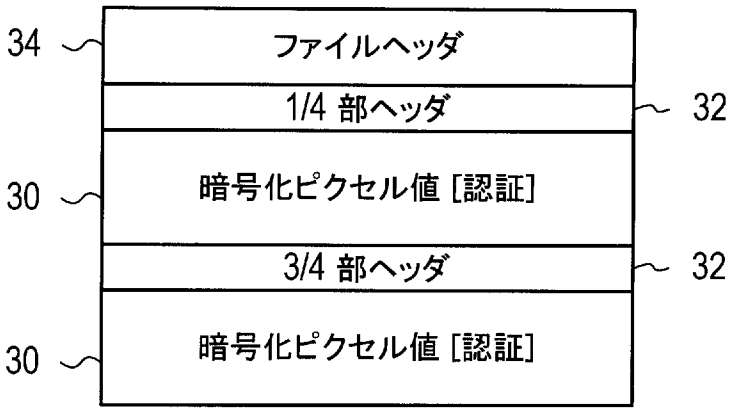

FIG. 16A

[図16B]

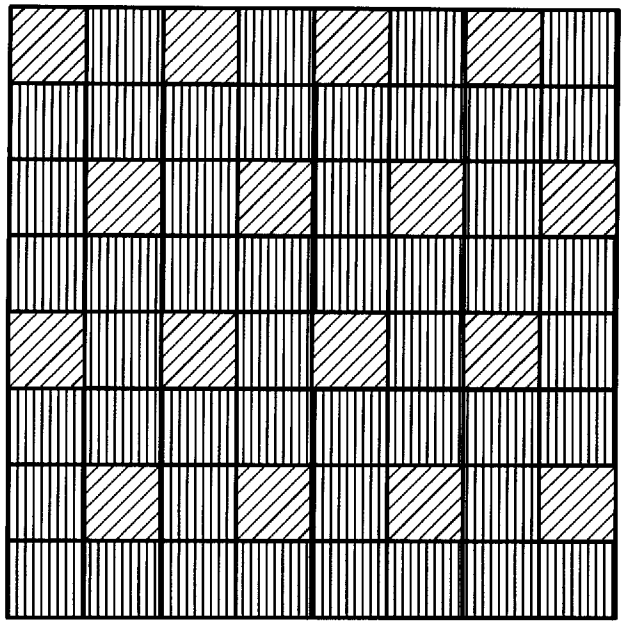

FIG. 16B

[図17]

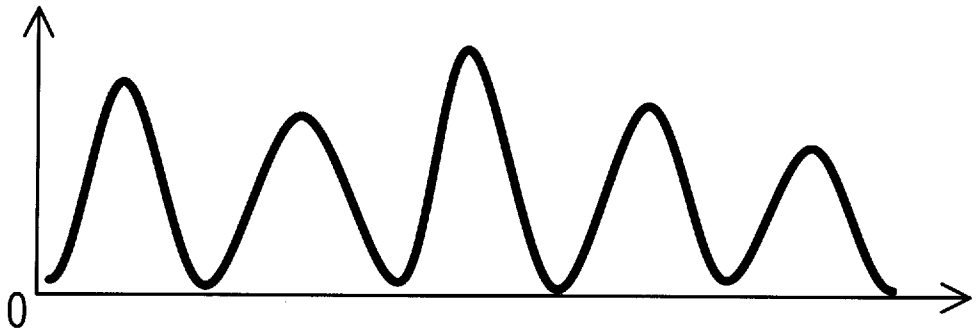

FIG. 17

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2017/004766

A. CLASSIFICATION OF SUBJECT MATTER
H04L9/14(2006.01)i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L9/14

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

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2017
Kokai Jitsuyo Shinan Koho	1971-2017	Toroku Jitsuyo Shinan Koho	1994-2017

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2003-319158 A (Toshiyuki TANI), 07 November 2003 (07.11.2003), paragraphs [0076] to [0088] (Family: none)	1-8
Y	JP 2007-243256 A (Dainippon Printing Co., Ltd.), 20 September 2007 (20.09.2007), paragraphs [0029] to [0035]; fig. 7, 8 (Family: none)	1-8
Y	JP 2001-216045 A (NEC Corp.), 10 August 2001 (10.08.2001), paragraphs [0041], [0042] & US 2001/0025342 A1 paragraph [0040] & KR 10-2001-0078320 A	4-6

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

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
01 May 2017 (01.05.17)	16 May 2017 (16.05.17)

Name and mailing address of the ISA/	Authorized officer
Japan Patent Office 3-4-3,Kasumigaseki,Chiyoda-ku, Tokyo 100-8915,Japan	Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2017/004766

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 61-264371 A (Ryoichi MORI), 22 November 1986 (22.11.1986), page 3, upper right, line 9 to lower left, line 5 (Family: none)	6

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１７／００４７６６

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　H04L9/14(2006.01)i

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.　H04L9/14

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２０１７年
日本国実用新案登録公報	１９９６－２０１７年
日本国登録実用新案公報	１９９４－２０１７年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
Y	JP 2003-319158 A (谷 俊行) 2003.11.07, 段落 [0076] － [0088] (ファミリーなし)	1-8
Y	JP 2007-243256 A (大日本印刷株式会社) 2007.09.20, 段落 [0029] － [0035], 図 7, 8 (ファミリーなし)	1-8

☑　Ｃ欄の続きにも文献が列挙されている。　　☐　パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
０１．０５．２０１７	１６．０５．２０１７

国際調査機関の名称及びあて先
日本国特許庁（ＩＳＡ／ＪＰ）
郵便番号１００－８９１５
東京都千代田区霞が関三丁目４番３号

特許庁審査官（権限のある職員）　５Ｓ　６３０４
行田　悦資
電話番号　０３－３５８１－１１０１　内線　３５４６

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
Y	JP 2001-216045 A (日本電気株式会社) 2001.08.10, 段落 [0041], [0042] & US 2001/0025342 A1, 段落 [0040] & KR 10-2001-0078320 A	4-6
Y	JP 61-264371 A (森 亮一) 1986.11.22, 3頁右上9行－左下5行 (ファミリーなし)	6