(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4746004号
(P4746004)

(45)発行日　平成23年8月10日(2011.8.10)　(24)登録日　平成23年5月20日(2011.5.20)

(51)Int.Cl.　F I
G06F 21/20 (2006.01)　G06F 15/00 330F

請求項の数 4　(全 44 頁)

(21)出願番号　特願2007-128303(P2007-128303)
(22)出願日　平成19年5月14日(2007.5.14)
(62)分割の表示　特願2004-570164(P2004-570164)の分割
原出願日　平成15年3月31日(2003.3.31)
(65)公開番号　特開2007-234054(P2007-234054A)
(43)公開日　平成19年9月13日(2007.9.13)
審査請求日　平成19年5月14日(2007.5.14)

前置審査

(73)特許権者　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(74)代理人　100074099
弁理士　大菅　義之
(74)代理人　100133570
弁理士　▲徳▼永　民雄
(74)復代理人　100167483
弁理士　林　裕己
(72)発明者　福田　充昭
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

最終頁に続く

(54)【発明の名称】登録装置

(57)【特許請求の範囲】
【請求項１】
個人を確認する画像情報であって、個人に属するマルチメディア情報であり、画像の周波数に応じた複数の種類の要素からなる、複数人の個人情報を取得する取得手段と、
複数人の前記個人情報をそれぞれ、前記画像の周波数に応じて、該個人情報の要素の種類別に、周波数成分の低い順に段階的に分割する分割手段と、
該分割手段により複数に分割された個人情報である分割個人情報のそれぞれを、当該分割個人情報に対応する個人とは異なる個人の分割個人情報と組み合わせて、複数の複数人の分割個人情報の組とする組み合わせ手段と、
該組み合わせ手段により組み合わされた複数の複数人の分割個人情報の組をそれぞれ、異なる格納手段に格納する格納制御手段と、
を備え、
前記分割手段は、前記個人情報を情報量の少ない低周波成分の要素の種類を有する分割個人情報から情報量の多い高周波成分の要素の種類を有する分割個人情報へ段階的に分割し、前記組み合わせ手段は、前記情報量により段階的に分割された複数人の分割個人情報を組み合わせて、前記複数の複数人の分割個人情報の組とし、前記格納制御手段は、前記複数の複数人の分割個人情報の組をそれぞれ異なる前記格納手段に格納する
ことを特徴とする登録装置。
【請求項２】
前記登録装置は、さらに、前記分割手段により分割された、前記格納手段に格納される

分割個人情報を暗号化する暗号化手段と、
を備えることを特徴とする請求項１に記載の登録装置。
【請求項３】
前記格納制御手段は、前記複数の複数人の分割個人情報の組をそれぞれ異なる前記格納手段に格納することにより、同一人の複数の前記分割個人情報をそれぞれ異なる前記格納手段へ格納する
ことを特徴とする請求項１に記載の登録装置。
【請求項４】
可搬型記憶媒体の読み取りが可能な登録装置と、該登録装置とネットワークで接続されたサーバ装置とからなる登録システムの登録装置において、
個人を確認する画像情報であって、個人に属するマルチメディア情報であり、画像の周波数に応じた複数の種類の要素からなる、複数人の個人情報を取得する取得手段と、
複数人の前記個人情報をそれぞれ、前記画像の周波数に応じて、該個人情報の要素の種類別に、周波数成分の低い順に段階的に分割する分割手段と、
該分割手段により複数に分割された個人情報である分割個人情報のそれぞれを、当該分割個人情報に対応する個人とは異なる個人の分割個人情報と組み合わせて、複数の複数人の分割個人情報の組とする組み合わせ手段と、
該組み合わせ手段により組み合わされた複数の複数人の分割個人情報の組を、前記登録装置内蔵の格納手段、前記可搬型記憶媒体、及び前記サーバ装置内蔵の格納手段のうちの少なくとも２つの格納手段に分けて格納する格納制御手段と、
を備え、
前記分割手段は、前記個人情報を情報量の少ない低周波成分の要素の種類を有する分割個人情報から情報量の多い高周波成分の要素の種類を有する分割個人情報へ段階的に分割し、前記組み合わせ手段は、前記情報量により段階的に分割された複数人の分割個人情報を組み合わせて、前記複数の複数人の分割個人情報の組とし、前記格納制御手段は、前記複数の複数人の分割個人情報の組をそれぞれ、前記登録装置内蔵の格納手段、前記可搬型記憶媒体、及び前記サーバ装置内蔵の格納手段のうちの異なる前記格納手段に格納する
ことを特徴とする登録装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、予め記憶装置に記録した個人を確認する情報と提示された個人情報とを照合するための照合装置に関する。
【背景技術】
【０００２】
情報化社会における様々な局面において、セキュリティの確保や利用者の利便性向上のために、個人を確認する情報、すなわち個人に属するマルチメディア情報を利用する照合技術の開発が進められている。
【０００３】
マルチメディア情報を用いて照合処理をおこなうためには、個人に属するマルチメディア情報を予め記憶装置に登録しておき、照合が必要になった際に、照合の対象となる人の所持するマルチメディア情報を取得して、前記の記憶装置に登録されているマルチメディア情報と比較することによって同一性の照合をおこなう。
【０００４】
従来の手法では、この照合に必要な個人のマルチメディア情報は１ヶ所の記憶装置にまとまって記憶している。また、照合に用いるマルチメディア情報を可搬型記憶部と照合記憶部に分割して格納し、照合時にはこれら分割して記憶したデータを合成し、その合成したデータと利用者のマルチメディア情報を比較して照合する手法もある（例えば、特許文献１）。
【特許文献１】特開２００１－６７１３７号公報

【発明の開示】
【発明が解決しようとする課題】
【０００５】
ところが、従来技術では、予め記憶装置に記憶したマルチメディア情報が盗まれてしまった場合、そのマルチメディア情報を使って他人になりすまして照合処理を通過されてしまう危険性がある。また、個人に属するマルチメディア情報の中には変更が不可能であり、その情報がいったん盗まれてしまうと、取り返しがつかないものがある。
【０００６】
また、特許文献１では、個人に属するマルチメディア情報を分割率Ｍによって２分割し、分割した情報を異なる記憶装置に格納させている。しかしながら、特許文献１では、分割した情報の格納場所が２箇所に限定されており、一方はＩＣカード等の可搬型記憶媒体に格納し、他方は照合装置内部の記憶装置に格納するというように格納形態が限られていた。また、分割した情報を照合に用いる場合には、分割した情報を一度合成しなければならず、照合処理が始まるまでに余分な時間がかかっていた。
【０００７】
また、精度の高い照合処理をおこなう場合には処理速度が問題となる。特に、多くの登録者の中から１人を選び出す１：Ｎ照合の際には、全ての登録者のマルチメディア情報との照合を行うために処理に要する時間が増大してしまう。照合のために必要なマルチメディア情報の情報量も多くなるため、サーバ／クライアント型のシステム構成での情報転送路における情報伝送量も多くなり、ネットワークに多大な負荷がかかることになる。
【０００８】
上記の課題に鑑み、本発明では、セキュリティの向上、照合処理の高速化、個人を確認する情報を伝送する通信路の負荷軽減を図ることができる照合装置を提供する。
【課題を解決するための手段】
【０００９】
本発明にかかる登録装置は、個人を確認する情報である個人情報を取得する取得手段と、前記個人情報を分割する分割手段と、該分割手段により複数に分割された個人情報である分割個人情報を、前記照合装置の前記複数の格納手段にそれぞれ格納する格納制御手段と、を備え、前記分割手段は、前記個人情報を情報量の少ない分割個人情報から情報量の多い分割個人情報へ段階的に分割し、前記格納制御手段は該分割個人情報をそれぞれ異なる前記格納手段に格納することを特徴とする。
【００１０】
このように構成することによって、個人を確認する情報を別々の記憶装置に格納することができ、記憶装置の盗難などの際のリスクを分散することができ、個人を確認する情報の照合処理に要する平均時間を従来の手法よりも高速に処理を行うことができる。また、ネットワークの負荷も抑えることができる。
【００１１】
また、前記登録装置は、さらに、前記分割手段により分割された、前記格納手段に格納される分割個人情報を暗号化する暗号化手段と、を備えることを特徴とする。
このように構成することによって、分割保存するマルチメディア情報に暗号化を施すことによって、セキュリティが向上する。
【００１２】
また、前記登録装置において、前記分割手段は、複数人の前記個人情報をそれぞれ分割して、該分割した個人情報それぞれを該分割した個人情報以外の分割した個人情報と組み合わせて複数の組とし、前記格納制御手段は、該組み合わせた個人情報をそれぞれ異なる前記格納手段へ格納することを特徴とする。
【００１３】
このように構成することによって、特定個人の情報を取り出すことが困難となり、安全性を向上させることができる。
【発明の効果】

【００１４】
本発明を用いることにより、セキュリティの向上、照合処理の高速化、マルチメディア情報を伝送する通信路の負荷軽減を図ることができる。
【発明を実施するための最良の形態】
【００１５】
（実施例１）
図１は、本実施例における照合システムを示す。本実施例では個人に属するマルチメディア情報を３ヶ所の記憶部に分散記憶する例を示すが、本発明における記憶部の数は３ヶ所に限定されるものではない。
【００１６】
図１において、マルチメディア情報を格納する記憶装置は、個人照合装置２に内蔵されたハードディスク（第１の記憶装置２３）と、一般のメモリカードやセキュリティ保護されたＩＣカードなどの可搬型の記憶媒体３（可搬記憶媒体３に第２の記憶部３１を備える）と、ネットワークで接続されたサーバ４内の記憶装置（第３の記憶部４１）に分散配置されている。なお、本発明における記憶装置の分散配置形態はこの図１の形態に限定されず、記憶部の数や配置先は任意に決定することができる。
【００１７】
また、照合装置２は、マルチメディア情報取得部２１、マルチメディア情報照合部２２を備え、マルチメディア情報照合部２２では、照合処理Ｐ１，Ｐ２，Ｐ３を行う。
図１において照合対象者１を照合する場合、まず、照合対象者１を確認するための情報であるマルチメディア情報Ａ１をマルチメディア情報取得部２１で取得し、その取得したマルチメディア情報Ａ１はマルチメディア情報照合部２２に送られる。マルチメディア情報照合部２２に送られたマルチメディア情報Ａ１は、照合処理Ｐ１，Ｐ２，Ｐ３で、複数の場所に分散配置された記憶部２３，３１，４１の中に予め格納されている照合用のマルチメディア情報のそれぞれと段階的に照合される。
【００１８】
マルチメディア情報照合部２２では、マルチメディア情報Ａ１に対して照合処理Ｐ１，Ｐ２，Ｐ３を順番に行い、予め決めておいた条件に合致した場合に照合成功あるいは照合失敗の結果を出力する。
【００１９】
図２は、本実施例におけるマルチメディア情報照合部２２での照合処理の詳細なフロー（例１）を示す。また、図３は、照合に用いるある種のマルチメディア画像情報の一例を示す図である。図３（１）で、Ａ１は大きさの異なる３種類の枝Ａａ，Ａｂ，Ａｃから構成される。Ｄ１（図３（４）），Ｄ２（図３（５）），Ｄ３（図３（６））は、図３（１）のＡ１の構成要素である枝Ａａ，Ａｂ，Ａｃをそれぞれ、その種類別に分解（分割）したものである。本実施例において、Ｄ１（図３（４）），Ｄ２（図３（５）），Ｄ３（図３（６））はそれぞれ、第１の記憶部２３、第２の記憶部、第３の記憶部に格納されている。それでは、この図３を参照しながら、図２のフローを説明する。
【００２０】
まず、マルチメディア情報照合部２２は、マルチメディア情報取得部２１から送出された照合対象者１のマルチメディア情報Ａ１（図３（１））を取得する（ステップＳ１、以下ステップをＳと略する）。次に、第１の記憶部２３から登録済みマルチメディア情報Ｄ１（図３（４））を取得する（Ｓ２）。
【００２１】
次に、照合処理Ｐ１を行う（Ｓ３）。この照合処理Ｐ１では、マルチメディア情報Ａ１とマルチメディア情報Ｄ１とを照合し、その照合結果に基づいて類似度Ｒ１が設定される。さらに具体的にいえば、例えば、マルチメディア情報Ａ１とマルチメディア情報Ｄ１とをパターンマッチング等の照合手法を用いて、特徴点が互いに一致しているか否かに基づいて、類似度Ｒ１が設定される。例えば、特徴点の一致の度合いが大きければ類似度Ｒ１として５が設定され、特徴点の一致の度合いが小さければ類似度Ｒ１として１が設定され

る。
【００２２】
次に、Ｓ３で算出した類似度Ｒ１がしきい値Ｔ１を超えているか否かを判定する（Ｓ４）。ここで、しきい値Ｔ１は、予め決められた値である。類似度Ｒ１≦しきい値Ｔ１の場合、照合失敗となり、本処理は終了する。
【００２３】
類似度Ｒ１＞しきい値Ｔ１の場合、照合処理Ｐ２に渡すマルチメディア情報Ａ２（図３（２））を作成する（Ｓ５）。ここでは、マルチメディア情報Ａ１からマルチメディア情報Ｄ１を差し引いた差分の情報であるマルチメディア情報Ａ２を求める。次に、第２の記憶部３１から登録済みマルチメディア情報Ｄ２（図３（５））を取得する（Ｓ６）。
【００２４】
次に、照合処理Ｐ２を行う（Ｓ７）。この照合処理Ｐ２では、マルチメディア情報Ａ２とマルチメディア情報Ｄ２とを照合し、この照合結果に基づいて類似度Ｒ２が設定される。照合手法としては、Ｓ３と同様である。
【００２５】
次に、Ｓ７で算出した類似度Ｒ２がしきい値Ｔ２を超えているか否かを判定する（Ｓ８）。ここで、しきい値Ｔ２は、予め決められた値である。類似度Ｒ２≦しきい値Ｔ２の場合、照合失敗となり、本処理は終了する。
【００２６】
類似度Ｒ２＞しきい値Ｔ２の場合、照合処理Ｐ３に渡すマルチメディア情報Ａ３（図３（３））を作成する（Ｓ９）。ここでは、マルチメディア情報Ａ２からマルチメディア情報Ｄ２を差し引いた差分の情報であるマルチメディア情報Ａ３を求める。次に、第３の記憶部４１から登録済みマルチメディア情報Ｄ３（図３（６））を取得する（Ｓ１０）。
【００２７】
次に、照合処理Ｐ３を行う（Ｓ１１）。この照合処理Ｐ３では、マルチメディア情報Ａ３とマルチメディア情報Ｄ３とを照合し、この照合結果に基づいて類似度Ｒ３が設定される。照合手法としては、Ｓ３と同様である。
【００２８】
次に、Ｓ１１で算出した類似度Ｒ３がしきい値Ｔ３を超えているか否かを判定する（Ｓ１２）。ここで、しきい値Ｔ３は、予め決められた値である。類似度Ｒ３≦しきい値Ｔ３の場合、照合失敗となり、本処理は終了する。
【００２９】
類似度Ｒ３＞しきい値Ｔ３の場合、照合成功となり、本フローは終了する。
マルチメディア情報照合部における照合処理は、上記の図２のフローに限定されず、例えば、図４のようなフローであってもよい。
【００３０】
図４は、本実施例におけるマルチメディア情報照合部２２での照合処理の詳細なフロー（例２）を示す。まず、照合処理で案出される類似度の累計を格納するための変数である類似度累計Ｘを、例えばＸ＝０として、初期化する（Ｓ２１）。次に、マルチメディア情報照合部２２は、マルチメディア情報取得部２１から送出された照合対象者１のマルチメディア情報Ａ１を取得する（Ｓ２２）。次に、第１の記憶部２３から登録済みマルチメディア情報Ｄ１を取得する（Ｓ２３）。
【００３１】
次に、照合処理Ｐ１を行う（Ｓ２４）。この照合処理Ｐ１では、マルチメディア情報Ａ１とマルチメディア情報Ｄ１とを照合し、図２のＳ３と同様にして、類似度Ｒ１を算出する。この算出した類似度Ｒ１を類似度累計Ｘに格納する（類似度累計Ｘに類似度Ｒ１を加えた値を類似度累計Ｘに格納する）。
【００３２】
次に、Ｓ２４で算出した類似度累計Ｘがしきい値Ｔ１を超えているか否かを判定する（Ｓ２５）。ここで、しきい値Ｔ１は、予め決められた値である。類似度累計Ｘ≦しきい値

Ｔ１の場合、照合失敗となり、本処理は終了する。

【００３３】

類似度累計Ｘ＞しきい値Ｔ１の場合、照合処理Ｐ２に渡すマルチメディア情報Ａ３を作成する（Ｓ２６）。ここでは、マルチメディア情報Ａ１からマルチメディア情報Ｄ１を差し引いた差分の情報であるマルチメディア情報Ａ２を求める。次に、第２の記憶部３１から登録済みマルチメディア情報Ｄ２を取得する（Ｓ２７）。

【００３４】

次に、照合処理Ｐ２を行う（Ｓ２８）。この照合処理Ｐ２では、マルチメディア情報Ａ２とマルチメディア情報Ｄ２とを照合し、Ｓ２４と同様にして、類似度Ｒ２を算出する。そして、類似度累計Ｘに類似度Ｒ２を加えた値を類似度累計Ｘに格納する。

【００３５】

次に、Ｓ２８で算出した類似度累計Ｘがしきい値Ｔ２を超えているか否かを判定する（Ｓ２９）。類似度累計Ｘ≦しきい値Ｔ２の場合、照合失敗となり、本処理は終了する。

類似度累計Ｘ＞しきい値Ｔ２の場合、照合処理Ｐ３に渡すマルチメディア情報Ａ３を作成する（Ｓ３０）。ここでは、マルチメディア情報Ａ２からマルチメディア情報Ｄ２を差し引いた差分の情報であるマルチメディア情報Ａ３を求める。次に、第３の記憶部４１から登録済みマルチメディア情報Ｄ３を取得する（Ｓ３１）。

【００３６】

次に、照合処理Ｐ３を行う（Ｓ３２）。この照合処理Ｐ３では、マルチメディア情報Ａ３とマルチメディア情報Ｄ３とを照合し、Ｓ２４と同様にして、類似度Ｒ３を算出する。そして、類似度累計Ｘに類似度Ｒ３を加えた値を類似度累計Ｘに格納する。

【００３７】

次に、Ｓ３２で算出した類似度累計Ｘがしきい値Ｔ３を超えているか否かを判定する（Ｓ３３）。類似度累計Ｘ≦しきい値Ｔ３の場合、照合失敗となり、本処理は終了する。

類似度累計Ｘ＞しきい値Ｔ３の場合、照合成功となり、本フローは終了する。なお、しきい値Ｔ１，Ｔ２，Ｔ３は、Ｔ１＜Ｔ２＜Ｔ３の関係にある。

【００３８】

照合処理Ｐ１，Ｐ２，Ｐ３で照合成功に至る条件の例としては、図２に示すように、照合処理Ｐ１，Ｐ２，Ｐ３それぞれが出力するマルチメディア情報の類似度が、それぞれの照合段階に対して予め決めておいたしきい値を全ての照合処理Ｐ１，Ｐ２，Ｐ３において上回った場合に適用できる。また、図４に示すように、照合処理Ｐ１，Ｐ２，Ｐ３それぞれが出力するマルチメディア情報の類似度の累積が、あらかじめ決めておいたしきい値を上回った場合などにも照合成功に至る条件の例として適用することができる。

【００３９】

また、１：Ｎ照合（複数の登録者の中から照合対象者が誰であるかを確認する照合手法）では、この照合処理を登録されている全ての人に属するマルチメディア情報に対して繰り返し、マルチメディア情報の類似度が最も高い登録者の情報を照合結果として出力する。

【００４０】

分割したマルチメディア情報を記憶する複数の記憶部は、本実施例のように別々の装置の中に配置することができる。また、そのように分散配置することによって装置の盗難などの際のリスクを分散することができる。

【００４１】

また、本実施例では、全ての照合処理を１つのマルチメディア情報照合部の中で行っているが、それぞれの照合処理を複数のマルチメディア情報照合部で分割照合する構成も可能である。

【００４２】

また、各照合処理が次の段階の照合処理に渡すマルチメディア情報は、記憶部から取り出して照合に用いたマルチメディア情報によって変換を施されたものとすることができる。既に照合処理を施した情報を削減することによって、次の段階の照合処理を高速化する

ことができる。

【００４３】

以上より、マルチメディア情報を複数の記憶装置に分割して記憶する構成によって、一部の記憶装置からマルチメディア情報が盗まれても、残りの記憶装置に登録されているマルチメディア情報が無事であれば、その盗まれたマルチメディア情報だけを用いても照合処理を通過することが不可能であるため、セキュリティを向上することが可能となる。

【００４４】

また、複数分割したマルチメディア情報を合成してから照合するのではなく、各分割マルチメディア情報毎に段階的に複数回の照合を繰り返す構成にすることで、分割後のマルチメディア情報から元のマルチメディア情報を復元することが困難になる。複数の記憶装置のマルチメディア情報が同時に盗難に遭った場合でも、それを用いて元のマルチメディア情報を復元することが困難であれば、照合処理を通過することが困難であり、セキュリティを向上することができる。特許文献１のように分割して記憶しておいたマルチメディア情報を合成してから照合する方式では、その合成の方法が分かってしまった場合、照合処理を通過するためのマルチメディア情報を復元することが可能となり、リスクが高い。

【００４５】

（実施例２）

本実施例では、マルチメディア情報の分散・格納について説明する。照合にあたって、予め照合対象者（正規のユーザ）の情報を照合装置の記憶部（第１の記憶部、第２の記憶部、第３の記憶部）に格納しておかなければならない。本実施例は、その登録について説明する。

【００４６】

図５は、本実施例における登録装置の内部の概要を示す。登録時において、まず、マルチメディア取得部５１により登録対象者のマルチメディア情報Ｂが取得され、そのマルチメディア情報Ｂがマルチメディア情報分割部５２へ送出される。マルチメディア情報分割部５２では、受け取ったマルチメディア情報Ｂを複数に分割して（本実施例では、３つに分割しているがこれに限定されない）、格納制御部５４によって、その分割した各情報を第１の記憶部５３、第２の記憶部３１、第３の記憶部４１へ格納する。

【００４７】

図６は、マルチメディア情報分割部５２により３つに分割したマルチメディア情報を格納制御部５４によって各記憶部に格納する概要を示す。図１において、第１の記憶部５３、第２の記憶部３１、第３の記憶部４１にそれぞれ記憶するマルチメディア情報を、図６に示すように、情報量が少なく粗いマルチメディア情報から、情報量が多く詳細なマルチメディア情報へと分割する。そして、その分割したそれぞれのマルチメディア情報を各記憶部に格納する。ここで、分割処理は、例えば画像の周波数の高低により分割する手法等がある。この場合、画像の低周波数成分を抽出した画像が粗い分割マルチメディア情報Ｄ１に相当し、画像の高周波数成分を抽出した画像が詳細な分割マルチメディア情報Ｄ３に相当し、画像のそれらの間の周波数成分を抽出した画像が分割マルチメディア情報Ｄ２に相当する。

【００４８】

実施例１（図２）において、最初に照合される、すなわち照合処理Ｐ１で照合される分割マルチメディア情報をより粗い情報とし、後から照合される分割マルチメディア情報をより詳細な情報とすることで、早い段階の照合処理をより情報量の少ないマルチメディア情報で処理することができ、この段階で照合に合致しないデータを高速にふるい落とすことで、平均的な照合処理時間を短縮することができる。

【００４９】

なお、本実施例では、登録装置５に内蔵されている第１の記憶部５３に分割したマルチメディア情報を格納したが、ネットワーク経由等で照合装置２の第１の記憶部２３に格納するようにしてもよい。また、登録装置５の第１の記憶部５３に格納した情報を可搬型記憶媒体等に一度格納し、その可搬型記憶媒体を照合装置２に読み取らせて、その可搬型記

憶媒体に格納した情報を照合装置２の第１の記憶部２３に格納するようにしてもよい。また、実施例１，２では、照合装置１と登録装置５とを分離して構成したが、これに限定されるものではなく、同一の装置内に照合装置と登録装置を共存させてもよい。このことより、これより以下では、第１の記憶部５１に格納した情報と同一の情報が、第１の記憶部２３に格納されているものとする。したがって、格納時では第１の記憶部に５３を用い、照合時には第１の記憶部に２３を用いることとする。

【００５０】

以上より、一般に、少量の情報を用いた粗い照合処理は、多量の情報を用いた詳細な照合処理に比べ高速に処理することができる。そこで、実施例１において個人に属するマルチメディア情報を分割する際に、粗い照合処理のための情報から詳細な照合処理のための情報へ段階的に分割して別々の記憶部に記録し、照合時には粗い照合処理を行ってから徐々により詳細な照合処理へ進むようにすることで、粗い照合処理で合致しない場合は全ての照合処理を最後までおこなう必要がなく、その段階で処理を終了することができる。これによって、個人に属するマルチメディア情報の照合処理に要する平均時間を従来の手法よりも高速に処理をおこなうことができる。

【００５１】

また特許文献１は、個人に属するマルチメディア情報を分割率Ｍで単純に２分割する手法であるが、照合の際には２分割したマルチメディア情報を合成してから照合をおこなうため、この手法では従来技術に比べて速度向上は望めない。むしろ分割したマルチメディア情報を合成するための処理時間が増加する。

【００５２】

さらに本実施例では、可搬記憶媒体には特定の個人に属する詳細なマルチメディア情報を記憶し、サーバには粗いマルチメディア情報を記憶することにより、可搬記憶媒体が無い場合は精度の低い照合、可搬記憶媒体が有る場合には精度の高い照合が可能となり、可搬記憶媒体の有無で提供するサービスを変化させることが可能となる。

【００５３】

その逆に、可搬記憶媒体や照合装置に内蔵の記憶部には特定の個人に属する粗いマルチメディア情報を記憶し、サーバには詳細なマルチメディア情報を記憶することにより、可搬記憶媒体や照合装置に内蔵の記憶部のマルチメディア情報だけで照合した場合は精度の低い照合、サーバに接続して照合した場合には精度の高い照合が可能となり、ローカルで利用する場合とサーバに接続する場合で提供するサービスを変化させることが可能となる。

【００５４】

（実施例３）

本実施例は、実施例２で説明した粗い情報から詳細な情報まで段階的に分割したマルチメディア情報をさらに複数の部分に再分割し、再分割した部分を任意に組み合わせて、それを複数の異なる記憶部に記憶するものである。

【００５５】

図７は、本実施例における分割・組み合わせの概念を示す。同図では、３つに分割したマルチメディア情報Ｄ１，Ｄ２，Ｄ３をさらに３つの部分に再分割し（（Ｄ１１，Ｄ１２，Ｄ１３）、（Ｄ２１，Ｄ２２，Ｄ２３），（Ｄ３１，Ｄ３２，Ｄ３３））、９つの再分割された各情報を３つずつ組み合わせて（Ｅ１，Ｅ２，Ｅ３）、Ｅ１，Ｅ２，Ｅ３をそれぞれ第１の記憶部５３、第２の記憶部３１、第３の記憶部４１に記憶する。

【００５６】

ここで、９つの再分割された各情報を３つずつ組み合わせることについて説明する。Ｄ１に着目すると、Ｄ１は再分割され、Ｄ１１、Ｄ１２、Ｄ１３になるが、組み合わせる場合には、できるだけこれらの情報が同一組にならないようにする。Ｄ２、Ｄ３についても同様である。このようにして組み合わせると、Ｅ１（Ｄ１１，Ｄ２１，Ｄ３１）、Ｅ２（Ｄ１２，Ｄ２２，Ｄ３２）、Ｅ３（Ｄ１３，Ｄ２３，Ｄ３３）の３組のマルチメディア情報が作成され、これらをそれぞれ第１の記憶部、第２の記憶部、第３の記憶部に記憶する

。

【００５７】

本実施例における登録装置５は、図５に示す登録装置と同様であり、上記の分割・組み合わせはマルチメディア情報分割部５２で実行される。まず、マルチメディア情報取得部２１により取得した登録対象者のマルチメディア情報は、マルチメディア情報分割部５２に送出され、マルチメディア情報分割部５２において上記の手順でマルチメディア情報は、分割・再分割され、格納制御部５４で各記憶部５３，３１，４１に格納される。

【００５８】

図８は、図７で再分割・組み合わせを行ったマルチメディア情報を照合する場合の処理を示す。照合処理は実施例１と同様である。このとき、照合処理Ｐ１においてマルチメディア情報Ｄ１を取得する場合（図２のＳ２に相当する処理）、第１の記憶部２３、第２の記憶部３１、第３の記憶部４１からそれぞれ、Ｅ１，Ｅ２，Ｅ３を取得する。マルチメディア情報合成部２５では、Ｅ１からはＤ１１を取り出し、Ｅ２からはＤ１２を取り出し、Ｅ３からはＤ１３を取り出し、これからＤ１を再構成する。

【００５９】

照合処理Ｐ２，Ｐ３を行う場合も、同様にしてマルチメディア情報Ｄ２，Ｄ３を取得する。

このようにして、各記憶部から取り出したマルチメディア情報を再構成して、再構成した後に各段の照合処理に適用することができる。

【００６０】

以上より、実施例２の構成の場合、第一段目の照合に用いる粗いマルチメディア情報を盗まれた場合、それを用いることによって第一段目の照合処理だけは通過されてしまうリスクがあった。それに対し、粗い照合処理のための情報から詳細な照合処理のための情報へ段階的に分割したマルチメディア情報をさらに分割して組み合わせて別々の記憶部に格納することにより、もし何れかの記憶部に格納した分割マルチメディア情報が盗まれても、その盗まれたマルチメディア情報だけを用いたのでは、照合処理を１段でも通過することは不可能となる。

【００６１】

（実施例４）

本実施例では、分割して記憶したマルチメディア情報を照合処理に用いる場合に、照合装置の要求仕様に応じて、必要な記憶部を選択して用いる構成とする。また、照合処理は実施例１と同様である。

【００６２】

図９は、本実施例における必要な記憶部を選択して構成された照合装置のパターンの１例を示す。同図において、照合装置２ａは、マルチメディア情報照合部２２ａの照合処理で用いるマルチメディア情報を第１の記憶部２３ａと可搬記憶装置３の第２の記憶部３１とから取得する構成である。照合装置２ｂは、マルチメディア情報照合部２２ｂの照合処理で用いるマルチメディア情報を第１の記憶部２３ｂとサーバ装置４の第３の記憶部４１とから取得する構成である。照合装置２ｃは、マルチメディア情報照合部２２ｃの照合処理で用いるマルチメディア情報を可搬記憶装置３の第２の記憶部３１とサーバ装置４の第３の記憶部４１とから取得する構成である。

【００６３】

また、必要な記憶部を選択して用いる構成であるので、セキュリティ制御をすることができる。クライアント装置とサーバ装置とを比較した場合、一般にサーバ装置外部側（クライアント装置側へ近づくほど）ほどセキュリティは低くなる。よって、図９では、最もセキュリティが高いのは、クライアント装置内蔵の記憶部から情報を取得していない照合装置２ｃであり、次にセキュリティが高いのは、照合装置２ｂであり、セキュリティが最も低いのは、サーバ装置の記憶部から情報を取得していない照合装置２ａである。

【００６４】

一方、マルチメディア情報の取得時間について考えてみる。一般に、ネットワークを介

して情報を取得しなければならないサーバ装置の記憶部から情報を取得する場合と比較して、ユーザ側の使用する端末、即ちクライアント装置により近いほうの記憶装置から情報を取得する場合の方が、取得時間は短い。

【００６５】

したがって、セキュリティ重視か、データの取得時間（即ち、照合処理時間の短縮）重視かという様々な用途に基いて、マルチメディア情報を取得する記憶部を選択し、照合装置を構成することができる。

【００６６】

このようにして、分割して記憶したマルチメディア情報を照合処理に用いる場合に、必要な記憶部を選択して用いる構成とする。記憶部に記憶する内容を変えずに様々な要求に応じることが可能となる。

【００６７】

また、分割する際に各々の記憶部に記憶する分割情報には冗長性を持たせてもよい。図９では、例えば第１の記憶部２３ａと第２の記憶部２３ｂに同じ情報を冗長的に記憶することができる。情報通信路に負荷をかけずに照合処理をおこなうことができる。

【００６８】

以上より、実施例１で個人に属するマルチメディア情報を複数の記憶部に分割保存し、この分割されたマルチメディア情報を利用して照合処理を行う場合に、照合精度や処理速度や情報転送量などの要求水準が異なる状況において、分割保存したマルチメディア情報の中からその状況の要求水準を満たすために必要なマルチメディア情報だけを選択して、照合処理を行うことで、分割して記憶した情報を変えることなく、様々な状況に対応することができる。

【００６９】

照合処理の高速性や情報転送量の削減が要求される状況では、少数の記憶部からの情報を利用して照合を行ったり、あるいは、粗い情報を記憶した記憶部を用いて照合を行うことで、速度向上や転送量の削減を行うことができる。

精度の高い照合が必要な状況では、多くの記憶部からの情報を利用して照合を行ったり、より詳細な情報を記憶した記憶部を利用して照合を行うことで、精度の高い照合を実現することができる。

【００７０】

（実施例５）

本実施例では、記憶部に記憶された情報のうち優先的に処理する分割マルチメディア情報を変更する。つまり、各記憶部からマルチメディア情報を取得する場合、その取得する順序を任意に変更する。

【００７１】

図１０は、本実施例における照合情報選択制御部２６を設けた照合装置２を示す。照合処理は実施例１と同様である。このとき、図２のＳ２，Ｓ６，Ｓ１０に相当する処理で第１の記憶部２３、第２の記憶部３１、第３の記憶部４１からマルチメディア情報を取得する場合、照合情報選択制御部２６の制御によって、この取得順序を変更することができる。例えば、ある場合には、第３の記憶部４１，第１の記憶部２３，第２の記憶部３１の順で各記憶部からマルチメディア情報を取得し、またある場合には、第２の記憶部３１，第３の記憶部４１，第１の記憶部２３の順で各記憶部からマルチメディア情報を取得することができる。

【００７２】

このように、取得する順番を変える利点として、各記憶部に異なる属性の情報が格納されている場合、ある属性の情報を優先的に照合することが挙げられる。例えば、第１の記憶部には音声情報、第２の記憶部には顔画像情報、第３の記憶部には、指紋情報が格納されている場合において、優先的に指紋照合を行うことができる。また、例えば、同じ種類の情報であって異なる部位の情報（同じ指紋情報でも、親指のものと中指のもの）を各記憶部に格納しておいて優先的に親指の指紋照合を行うことができる。

【００７３】
このような構成にすることによって、照合対象者の状況や照合環境によって、照合順序を変えることが可能となり、柔軟性の高い照合が可能となる。人によって、あるいは、環境によっては、分割保存したマルチメディア情報のどれを優先的に適用するかを変更することによって、処理速度の向上や利便性を向上することが可能となる。
【００７４】
（実施例６）
本実施例では、実施例２で説明した各分割マルチメディア情報をそれぞれ暗号化し、その暗号化を解除するための復号化キーを暗号化した分割マルチメディア情報とは異なる記憶部に格納する。
【００７５】
図１１は、本実施例における登録装置５を示す。まず、マルチメディア情報取得部５１により登録対象者のマルチメディア情報Ｂが取得され、そのマルチメディア情報Ｂがマルチメディア情報分割部５２へ送出される。マルチメディア情報分割部５２では、受け取ったマルチメディア情報Ｂを実施例２と同様の手法で分割し、分割したマルチメディア情報群を暗号部５５へ送出する。暗号部５５では、受け取った分割マルチメディア情報群を暗号化し、格納制御部５４では暗号化した分割マルチメディア情報をそれぞれ各記憶部２３，３１，４１へ格納する。
【００７６】
図１２は、本実施例における照合装置を示す。マルチメディア情報取得部２１により照合対象者１のマルチメディア情報Ａが取得され、そのマルチメディア情報Ａがマルチメディア情報照合部２２へ送出される。マルチメディア情報照合部２２で、照合処理Ｐ１，Ｐ２，Ｐ３を行う。それぞれの照合処理Ｐ１，Ｐ２，Ｐ３においてマルチメディア情報Ａと照合するための情報を各記憶部から取得する。このとき、各記憶部２３，３１，４１から取り出した暗号化された分割マルチメディア情報は復号部２７で復号化され、各照合処理Ｐ１，Ｐ２，Ｐ３で用いられる。
【００７７】
図１３は、本実施例におけるマルチメディア情報Ｂを記憶部に格納する場合の暗号化のフローを示す。まず、分割・合成部でマルチメディア情報Ｂを分割し（Ｓ４０）、分割マルチメディア情報Ｄ１，Ｄ２，Ｄ３を作成する。次に分割マルチメディア情報Ｄ１，Ｄ２，Ｄ３は、暗号部５５で以下に説明する手法で暗号化される。
【００７８】
まず、分割マルチメディア情報Ｄ１は暗号化キーＫ１で暗号化され（Ｓ４１）、暗号化済み分割マルチメディア情報Ｄ１ａとなる。分割マルチメディア情報Ｄ２は暗号化キーＫ２で暗号化され（Ｓ４２）、暗号化済み分割マルチメディア情報Ｄ２ａとなる。分割マルチメディア情報Ｄ３は暗号化キーＫ３で暗号化され（Ｓ４３）、暗号化済み分割マルチメディア情報Ｄ３ａとなる。ここで、暗号化には共通鍵方式を採用する。したがって、暗号化キーと復号化キーは同一である。
【００７９】
それから、分割マルチメディア情報Ｄ１ａは、復号化キーＫ２ａ（すなわち、暗号化キーＫ２のことである）と共に第１の記憶部５３に格納される。また、分割マルチメディア情報Ｄ２ａは、復号化キーＫ３ａ（すなわち、暗号化キーＫ３のことである）と共に第２の記憶部３１に格納される。また、分割マルチメディア情報Ｄ３ａは、復号化キーＫ１ａ（すなわち、暗号化キーＫ１のことである）と共に第３の記憶部４１に格納される。
【００８０】
このように、各分割マルチメディア情報をそれぞれ暗号化し、その暗号化を解除するための復号化キーを暗号化した分割マルチメディア情報とは異なる記憶部に格納する。
図１４は、本実施例における暗号化した分割マルチメディア情報の復号化のフローを示す。まず、照合処理Ｐ１が実行されると、復号部２７は第１の記憶部２３から暗号化済み分割マルチメディア情報Ｄ１ａと復号化キーＫ２ａとを取得し、第３の記憶部から暗号化

済み分割マルチメディア情報Ｄ３ａと復号化キーＫ１ａを取得する。復号化キーＫ１ａで暗号化済み分割マルチメディア情報Ｄ１ａを復号化し（Ｓ５０）、分割マルチメディア情報Ｄ１を得る。そして、この分割マルチメディア情報Ｄ１が照合処理Ｐ１で用いられる。

【００８１】

次に、照合処理Ｐ２が実行されると、復号部２７は第２の記憶部３１から暗号化済み分割マルチメディア情報Ｄ２ａと復号化キーＫ３ａとを取得する。暗号化済み分割マルチメディア情報Ｄ２ａを復号化するための複合化キーＫ２ａは、照合処理Ｐ１実行時に既に取得しているので、この復号化キーＫ２ａを用いて暗号化済み分割マルチメディア情報Ｄ２ａを復号化し（Ｓ５１）、分割マルチメディア情報Ｄ２を得る。そして、この分割マルチメディア情報Ｄ２が照合処理Ｐ２で用いられる。

【００８２】

次に、照合処理Ｐ３が実行されると、復号部２７は、照合処理Ｐ１，Ｐ２実行時で既に取得している暗号化済み分割マルチメディア情報Ｄ３ａと復号化キーＫ３ａを用いて、上記と同様に復号化を行い（Ｓ５２）、分割マルチメディア情報Ｄ３を得る。そして、この分割マルチメディア情報Ｄ３が照合処理Ｐ３で用いられる。

【００８３】

このように、照合時には、異なる記憶部に格納されている復号化キーを用いて暗号化された情報を復号化して、その後に実施例１における照合処理を行う。このように構成することで、各照合処理をおこなう際に、次の段階の照合処理で用いる分割マルチメディア情報を復号化するための復号化キーを同時に取得することができ、次の照合処理のための分割マルチメディア情報を直ちに復号処理することができ、効率良く照合処理を進めることが可能となる。

【００８４】

以上より、分割保存するマルチメディア情報に暗号化を施すことによって、セキュリティが向上する。その際に、暗号化したマルチメディア情報を復元するキーとなる情報を、暗号化したマルチメディア情報を記憶する記憶部とは異なる記憶部に保存することで、暗号化されたマルチメディア情報が盗難に遭っても、その暗号化を解除するキーは別の記憶部に格納されているので、暗号化を解除することができない。

【００８５】

（実施例７）

本実施例では、実施例２で説明した各分割マルチメディア情報をそれぞれ暗号化し、その暗号化をおこなうための暗号化キーを暗号化した分割マルチメディア情報とは異なる分割マルチメディア情報を基にして生成する。本実施例では、図１１と同様の登録装置、図１２と同様の照合装置を用いる。また、本実施例での照合処理は実施例１と同様である。

【００８６】

図１５は、本実施例におけるマルチメディア情報を記憶部に格納する場合の暗号化のフローを示す。まず、登録対象者のマルチメディア情報Ｂをマルチメディア情報取得部５１により取得し、マルチメディア情報分割部５２でマルチメディア情報を分割し（Ｓ６０）、分割マルチメディア情報Ｄ１，Ｄ２，Ｄ３を作成する。次に暗号化関数（例えば、ハッシュ関数等）を用いて、分割マルチメディア情報Ｄ１から暗号化キーＫ２を作成する（Ｓ６１）。分割マルチメディア情報Ｄ２，Ｄ３も同様にして、それぞれ暗号化キーＫ３，Ｋ１を作成する（Ｓ６２，Ｓ６３）。

【００８７】

分割マルチメディア情報Ｄ１は暗号化キーＫ１で暗号化され（Ｓ６４）、暗号化済み分割マルチメディア情報Ｄ１ａとなる。分割マルチメディア情報Ｄ２は暗号化キーＫ２で暗号化され（Ｓ６５）、暗号化済み分割マルチメディア情報Ｄ２ａとなる。分割マルチメディア情報Ｄ３は暗号化キーＫ３で暗号化され（Ｓ６６）、暗号化済み分割マルチメディア情報Ｄ３ａとなる。ここで、暗号化には共通鍵方式を採用する。したがって、暗号化キーと復号化キーは同一である。

【００８８】

それから、分割マルチメディア情報Ｄ１ａは格納制御部５４によって第１の記憶部５３に格納され、分割マルチメディア情報Ｄ２ａは第２の記憶部３１に格納される。また、分割マルチメディア情報Ｄ３ａは、復号化キーＫ１ａ（すなわち、暗号化キーＫ１のことである）と共に第３の記憶部４１に格納される。

【００８９】

図１６は、本実施例における暗号化した分割マルチメディア情報の復号化のフローを示す。まず、照合処理Ｐ１が実行されると、復号部２７は第１の記憶部２３から暗号化済み分割マルチメディア情報Ｄ１ａを取得し、第３の記憶部から暗号化済み分割マルチメディア情報Ｄ３ａと復号化キーＫ１ａを取得する。復号化キーＫ１ａで暗号化済み分割マルチメディア情報Ｄ１ａを復号化し（Ｓ７０）、分割マルチメディア情報Ｄ１を得る。そして、この分割マルチメディア情報Ｄ１が照合処理Ｐ１で用いられる。

【００９０】

次に、照合処理Ｐ２が実行されると、復号部２７は第２の記憶部３１から暗号化済み分割マルチメディア情報Ｄ２ａを取得する。また、暗号化関数を用いて、照合処理Ｐ１実行時に取得した分割メディア情報Ｄ１から復号化キーＫ２ａを取得する。この復号化キーＫ２ａを用いて暗号化済み分割マルチメディア情報Ｄ２ａを復号化し（Ｓ５１）、分割マルチメディア情報Ｄ２を得る。そして、この分割マルチメディア情報Ｄ２が照合処理Ｐ２で用いられる。

【００９１】

次に、照合処理Ｐ３が実行されると、復号部２７は、暗号化関数を用いて、照合処理Ｐ２実行時に取得した分割メディア情報Ｄ２から復号化キーＫ３ａを取得する。この復号化キーＫ３ａを用いて、照合処理Ｐ１実行時に取得した暗号化済み分割マルチメディア情報Ｄ３ａを復号化し（Ｓ５１）、分割マルチメディア情報Ｄ３を得る。そして、この分割マルチメディア情報Ｄ３が照合処理Ｐ３で用いられる。

【００９２】

このように、照合時には、異なる記憶部に格納されている分割マルチメディア情報から暗号化を解除するための復号化キーを生成し、その復号化キーを用いて暗号化を解除して、その後に実施例１における照合処理を行う。このように構成することで、各照合処理を行う際に次の段階の照合処理の分割マルチメディア情報を復号化するための復号化キーを同時に生成することができ、次の照合処理のための分割マルチメディア情報を直ちに復号化することができ、効率良く照合処理を進めることが可能となる。

【００９３】

ところが、このままでは全てのマルチメディア情報が暗号化されているため、いずれの復号化キーも生成することができず暗号化を解除することが不可能であるので、いずれか一つの複合化キーは何らかの手段で別に取得する必要がある。本実施例では、第３の記憶部に暗号化済み分割マルチメディア情報Ｄ３ａを復号化するための復号化キーを暗号化を施さずに記憶する構成としている。このように構成することによっても、記憶部１と記憶部３の情報が同時に盗まれない限り、暗号化されたマルチメディア情報を復号化することはできずセキュリティを高く保つことができる。

【００９４】

以上より、実施例６と同様に、分割保存するマルチメディア情報に暗号化を施すことによって、セキュリティが向上する。その際に、暗号化したマルチメディア情報を復元するキーとなる情報を、暗号化したマルチメディア情報を記憶する記憶部とは異なる記憶部に保存する別のマルチメディア情報を元に作成することで、暗号化されたマルチメディア情報が盗難に遭っても、その暗号化を解除するキーは別の記憶部に格納されているマルチメディア情報が元になっているので、暗号化を解除することができない。

【００９５】

（実施例８）

本実施例では、実施例２で説明した各分割マルチメディア情報をそれぞれ暗号化し、その暗号化をおこなうための暗号化キーを暗号化した分割マルチメディア情報とは異なる分

割マルチメディア情報を基にして生成する。本実施例では、図１１と同様の登録装置、図１２と同様の照合装置を用いる。また、本実施例での照合処理は実施例１と同様である。

【００９６】

図１７は、本実施例におけるマルチメディア情報を記憶部に格納する場合の暗号化のフロー（例１）を示す。まず、登録対称者のマルチメディア情報Ｂをマルチメディア情報取得部５１で取得し、マルチメディア情報分割部５２でこのマルチメディア情報を分割し（Ｓ８０）、分割マルチメディア情報Ｄ１，Ｄ２，Ｄ３を作成する。分割マルチメディア情報Ｄ１は暗号部５５で分割マルチメディア情報Ｄ３によって暗号化され（Ｓ８１）、暗号化済み分割マルチメディア情報Ｄ１ａを得る。ここでの暗号化処理は、分割マルチメディア情報Ｄ１を構成しているビット情報と分割マルチメディア情報Ｄ３を構成しているビット情報との論理演算（ＡＮＤ演算、ＯＲ演算、排他的論理和演算等）である。Ｓ８１で得られた暗号化済み分割マルチメディア情報Ｄ１ａを格納制御部５４により第１の記憶部５３へ格納する。

【００９７】

マルチメディア情報Ｄ２についても上記と同様であり、分割マルチメディア情報Ｄ２は分割マルチメディア情報Ｄ１によって暗号化され（Ｓ８２）、暗号化済み分割マルチメディア情報Ｄ２ａを得る。Ｓ８２で得られた暗号化済み分割マルチメディア情報Ｄ２ａを第２の記憶部３１へ格納する。

【００９８】

マルチメディア情報Ｄ３については、暗号化をせずに、そのまま第３の記憶部４１へ格納する。

このように、各分割マルチメディア情報をそれぞれ暗号化し、その暗号化を行うための暗号化キーとして暗号化した分割マルチメディア情報とは異なる分割マルチメディア情報を利用する。

【００９９】

図１８は、本実施例における暗号化した分割マルチメディア情報の復号化のフロー（例１）を示す。まず、照合処理Ｐ１が実行されると、復号部２７は第１の記憶部２３から暗号化済み分割マルチメディア情報Ｄ１ａを取得し、第３の記憶部から分割マルチメディア情報Ｄ３を取得する。暗号化済み分割マルチメディア情報Ｄ１ａは、分割マルチメディア情報Ｄ３を復号化キーＫ１ａとして用いることで復号化され（Ｓ９０）、分割マルチメディア情報Ｄ１を得る。

【０１００】

次に、照合処理Ｐ２が実行されると、復号部２７は第２の記憶部３１から暗号化済み分割マルチメディア情報Ｄ２ａを取得する。暗号化済み分割マルチメディア情報Ｄ２ａは、分割マルチメディア情報Ｄ１を復号化キーＫ２ａとして用いることで復号化され（Ｓ９１）、分割マルチメディア情報Ｄ２を得る。

【０１０１】

次に、照合処理Ｐ３が実行されると、復号部２７は、既に取得している分割マルチメディア情報Ｄ３を照合処理Ｐ３へ渡す。

このように、照合時には、異なる記憶部に格納されている分割マルチメディア情報を暗号化を解除するための復号化キーとして利用して暗号化を解除し、その後に実施例１における照合処理を行う。このように構成することで、各照合処理を行う際に次の段階の照合処理のための分割マルチメディア情報を復号化するための復号キーを得ることができ、次の照合処理のための分割マルチメディア情報を直ちに復号処理することができ、効率良く照合処理を進めることが可能となる。

【０１０２】

ところが、このまま全てのマルチメディア情報を暗号化した状態で保存すると、いずれの暗号化も解除することが不可能であるので、いずれか一つのマルチメディア情報は暗号化しない状態で保存しておく必要がある。本実施例では、第３の記憶部に記憶する分割マルチメディア情報Ｄ３は暗号化を施さずに記憶する構成としている。このように構成する

ことによっても、第１の記憶部と第３の記憶部の情報が同時に盗まれない限り、暗号化されたマルチメディア情報を復号化することはできず、セキュリティを高く保つことができる。

【０１０３】

また、本実施例のフローは以下に示す図１９、図２０のようにしてもよい。

図１９は、本実施例におけるマルチメディア情報を記憶部に格納する場合の暗号化のフロー（例２）を示す。まず、マルチメディア情報分割部５２で登録対象者のマルチメディア情報Ｂを分割し（Ｓ１００）、分割マルチメディア情報Ｄ１，Ｄ２，Ｄ３を作成する。分割マルチメディア情報Ｄ２は暗号部５５で分割マルチメディア情報Ｄ１によって暗号化され（Ｓ１０２）、暗号化済み分割マルチメディア情報Ｄ２ａを得る。ここでの暗号化処理は、図１８で説明したものと同様である。Ｓ１０２で得られた暗号化済み分割マルチメディア情報Ｄ２ａを第２の記憶部３１へ格納する。

【０１０４】

マルチメディア情報Ｄ３についても上記と同様であり、分割マルチメディア情報Ｄ３は分割マルチメディア情報Ｄ２によって暗号化され（Ｓ１０３）、暗号化済み分割マルチメディア情報Ｄ３ａを得る。Ｓ１０３で得られた暗号化済み分割マルチメディア情報Ｄ３ａを第３の記憶部４１へ格納する。

【０１０５】

マルチメディア情報Ｄ１については、Ｓ１０３で暗号化処理された暗号化済み分割マルチメディア情報Ｄ３ａを暗号化キーＫ１として、暗号化され（Ｓ１０１）、暗号化済み分割マルチメディア情報Ｄ１ａを得る。Ｓ１０１で得られた暗号化済み分割マルチメディア情報Ｄ１ａを第１の記憶部５３へ格納する。

【０１０６】

図２０は、本実施例における暗号化した分割マルチメディア情報の復号化のフロー（例２）を示す。まず、照合処理Ｐ１が実行されると、復号部２７は第１の記憶部２３から暗号化済み分割マルチメディア情報Ｄ１ａを取得し、第３の記憶部から暗号化済み分割マルチメディア情報Ｄ３ａを取得する。暗号化済み分割マルチメディア情報Ｄ１ａは、暗号化済み分割マルチメディア情報Ｄ３ａを復号化キーＫ１ａとして用いることで復号化され（Ｓ１１０）、分割マルチメディア情報Ｄ１を得る。

【０１０７】

次に、照合処理Ｐ２が実行されると、復号部２７は第２の記憶部３１から暗号化済み分割マルチメディア情報Ｄ２ａを取得する。暗号化済み分割マルチメディア情報Ｄ２ａは、分割マルチメディア情報Ｄ１を復号化キーＫ２ａとして用いることで復号化され（Ｓ１１１）、分割マルチメディア情報Ｄ２を得る。

【０１０８】

次に、照合処理Ｐ３が実行されると、分割マルチメディア情報Ｄ２を復号化キーＫ３ａとして用いることで、暗号化済み分割マルチメディア情報Ｄ３ａは復号化され（Ｓ１１２）、分割マルチメディア情報Ｄ３を得る。

【０１０９】

したがって、図１９、図２０のように、暗号化を施した分割マルチメディア情報を暗号化／復号化キーとして用いることにより、分割マルチメディア情報を安全に保つことも可能である。

【０１１０】

以上より、実施例６と同様に、分割保存するマルチメディア情報に暗号化を施すことによって、セキュリティが向上する。その際に、暗号化したマルチメディア情報を復元するキーとなる情報を、暗号化したマルチメディア情報を記憶する記憶部とは異なる記憶部に保存する別のマルチメディア情報自体とすることで、暗号化されたマルチメディア情報が盗難に遭っても、その暗号化を解除するには別の記憶部に格納されているマルチメディア情報が必要となるので、暗号化を解除することができない。

【０１１１】

（実施例９）
本実施例は、複数の個人に属する分割マルチメディア情報を組み合わせて合成し、複数の記憶部に記憶する。
【０１１２】
図２１は、本実施例における複数の個人に属する分割マルチメディア情報を組み合わせて合成する概要を示す。登録対象者１ａに属するマルチメディア情報Ａ１ａを分割したものをＤ１－１ａ、Ｄ２－１ａ、Ｄ３－１ａとし、登録対象者１ｂに属するマルチメディア情報Ａ１ｂを分割したものをＤ１－１ｂ、Ｄ２－１ｂ、Ｄ３－１ｂとし、登録対象者１ｃに属するマルチメディア情報Ａ１ｃを分割したものをＤ１－１ｃ、Ｄ２－１ｃ、Ｄ３－１ｃとする。
【０１１３】
次に分割したこれらのマルチメディア情報を他人のマルチメディア情報と組み合わせて各記憶部に格納する。ここで、９つの分割された各情報を３つずつ組み合わせることについて説明する。Ａ１ａに着目すると、分割したＤ１－１ａ、Ｄ２－１ａ、Ｄ３－１ａを組み合わせる場合には、これらの情報ができるだけ同一組にならないようにする。Ａ１ｂ、Ａ１ｃについても同様である。このようにして組み合わせると、合成情報Ｇ１（Ｄ１－１ａ，Ｄ１－１ｂ，Ｄ１－１ｃ）、合成情報Ｇ２（Ｄ２－１ａ，Ｄ２－１ｂ，Ｄ２－１ｃ）、合成情報Ｇ３（Ｄ３－１ａ，Ｄ３－１ｂ，Ｄ３－１ｃ）の３組のマルチメディア情報が作成され、これらをそれぞれ第１の記憶部５３、第２の記憶部３１、第３の記憶部４１に記憶する。本実施例における登録装置の概要は、図５と同様である。図５において、マルチメディア情報取得部５１により取得した複数の登録対象者のマルチメディア情報は、マルチメディア情報分割部５２に送出され、上記の手順でマルチメディア情報は、分割・組み合わされ、各記憶部に格納される。
【０１１４】
図２２は、図２１で分割・組み合わされたマルチメディア情報を照合する場合の処理を示す。照合処理は実施例１と同様である。照合対象者が１ａの場合、照合処理Ｐ１において照合対象者１ａに属するマルチメディア情報Ｄ１－１ａを取得しなければならない。よって、マルチメディア情報合成部２５は、第１の記憶部２３に格納した合成情報Ｇ１（Ｄ１－１ａ，Ｄ１－１ｂ，Ｄ１－１ｃ）を取得し、情報抽出処理Ｐ２５１で合成情報Ｇ１からＤ１－１ａを取得し、照合処理Ｐ１へ渡す。また、マルチメディア情報合成部２５は、第２の記憶部３１に格納した合成情報Ｇ２（Ｄ２－１ａ，Ｄ２－１ｂ，Ｄ２－１ｃ）を取得し、情報抽出処理Ｐ２５２で合成情報Ｇ２からＤ２－１ａを取得し、照合処理Ｐ２へ渡す。また、マルチメディア情報合成部２５は、第２の記憶部４１に格納した合成情報Ｇ３（Ｄ３－１ａ，Ｄ３－１ｂ，Ｄ３－１ｃ）を取得し、情報抽出処理Ｐ２５３で合成情報Ｇ３からＤ３－１ａを取得し、照合処理Ｐ３へ渡す。
【０１１５】
このように複数の個人に属する分割マルチメディア情報を合成したものを利用して照合処理を行う。このように構成することで特定個人の情報を取り出すことが困難となり、安全性を向上させることができる。また、合成処理の段階でデータの圧縮処理をおこなうことも可能である。データを圧縮することによって情報の転送量の削減も可能となる。
【０１１６】
以上より、複数の個人に属するマルチメディア情報を合成して保存することで、分割保存したマルチメディア情報が盗難に遭った場合でも、特定の個人のマルチメディア情報を取り出すことが困難となる。
【０１１７】
（実施例１０）
本実施例は、図２３に示すように各記憶部に登録する対象者の人数を変えた場合である。分割処理は、実施例９と同様であるが、実施例９と異なるのは分割したマルチメディア情報を組み合わせて記憶部に格納するだけでなく、様々なパターンで記憶部に格納することになる。

【０１１８】
同図において、Ｄ１－１ａ，Ｄ１－１ｂ，Ｄ１－１ｃ，Ｄ２－１ｃは、それぞれ単体で可搬媒体３ａの記憶部３１ａ，可搬媒体３ｂの記憶部３１ｂ，可搬媒体３ｃの記憶部３１ｃ，登録装置５ｂの記憶部５３に格納される。また、Ｄ２－１ａ，Ｄ２－１ｂは組み合わされて、合成情報Ｇ４として登録装置５ａの記憶部５３ａに格納される。また、Ｄ３－１ａ，Ｄ３－１ｂ，Ｄ３－１ｃは組み合わされて、合成情報Ｇ５としてサーバ装置４の記憶部４１に格納される。
【０１１９】
図２４は、本実施例における照合を行う際にどの記憶部から情報を取り出すかの処理概要を示す。照合対象者１ａを照合する場合、可搬記憶媒体３ａの記憶部３１ａと照合装置２ａの記憶部２３ａとサーバ装置４の記憶部４１とから照合対象者１ａに属するマルチメディア情報を取得する。また、照合対象者１ｂを照合する場合、可搬記憶媒体３ｂの記憶部３１ｂと照合装置２ａの記憶部２３ａとサーバ装置４の記憶部４１とから照合対象者１ｂに属するマルチメディア情報を取得する。照合対象者１ｃを照合する場合、可搬記憶媒体３ｃの記憶部３１ｃと照合装置２ｂの記憶部２３ｂとサーバ装置４の記憶部４１とから照合対象者１ｃに属するマルチメディア情報を取得する。
【０１２０】
このように構成することによって、例えば可搬型記憶媒体にはその可搬型記憶媒体を保持する個人に属するマルチメディア情報を分割したものだけを格納することによって、可搬型記憶媒体の記憶容量を節約することが可能となる。照合装置の記憶部にも、その装置で照合する対象者の情報だけを記憶することで記憶容量を節約することができる。
【０１２１】
以上より、記憶容量の少ない可搬記憶媒体などには特定の個人に属するマルチメディア情報を分割したものを記憶し、記憶容量の大きなサーバには複数の個人に属するマルチメディア情報を分割したものを記憶することによって、記憶容量の少ない記憶媒体を用いた場合でも有効に照合をおこなうことが可能となる。
【０１２２】
なお、以上の実施例１～１０で本発明についてその詳細を説明したが、この照合装置は当然一般的なコンピュータシステムとして構成することが可能である。
図２５はそのようなコンピュータシステム、すなわちハードウエア環境の構成ブロック図である。同図においてコンピュータシステムは中央処理装置（ＣＰＵ）６２、リードオンリメモリ（ＲＯＭ）６３、ランダムアクセスメモリ（ＲＡＭ）６６、通信インタフェース（Ｉ／Ｆ）６４、記憶装置６７、出力Ｉ／Ｆ６１、入力Ｉ／Ｆ６５、可搬型記憶媒体の読み取り装置６８、およびこれらの全てが接続されたバス６９、出力Ｉ／Ｆ６１に接続している出力装置７０、入力Ｉ／Ｆ６５に接続している入力装置７１によって構成されている。
【０１２３】
記憶装置６７としてはハードディスク、磁気ディスクなど様々な形式の記憶装置を使用することができ、このような記憶装置６７、またはＲＯＭ６３に図２，図４で示したフローチャートに示されたプログラム（マルチメディア情報照合部２２）や、マルチメディア情報分割部５２のプログラムや、マルチメディア情報合成部２５のプログラムや、照合情報選択制御部２６のプログラムなどや、暗号部５５、復号部２７のプログラムなどが格納され、そのようなプログラムがＣＰＵ６２によって実行されることにより、本実施形態における個人を確認するためのマルチメディア情報の照合や、個人を確認するためのマルチメディア情報を予め格納するときの分割や、その情報の暗号化・復号化などが可能となる。
【０１２４】
このようなプログラムは、プログラム提供者側からネットワーク７２、および通信Ｉ／Ｆ６４を介して、例えば記憶装置６７に格納されることも、また市販され、流通している可搬型記憶媒体３に格納され、読み取り装置６８にセットされて、ＣＰＵ６２によって実

行されることも可能である。可搬型記憶媒体３としてはＣＤ－ＲＯＭ、フレキシブルディスク、光ディスク、光磁気ディスク、ＩＣカードなど様々な形式の記憶媒体を使用することができ、このような記憶媒体に格納されたプログラムが読み取り装置６８によって読み取られる。

【０１２５】

また、入力装置７１には、マルチメディア情報取得部２１に該当し、キーボード、マウス、またはマルチメディア情報を入力するためのカメラ、マイク、スキャナ、センサー、タブレットなどを用いることが可能である。また、出力装置７０には、ディスプレイ、プリンタ、スピーカなどを用いることが可能である。

【０１２６】

また、ネットワーク７２は、インターネット、ＬＡＮ、ＷＡＮ、専用線、有線、無線等の通信網であってよい。

本発明を用いることにより、セキュリティの向上、照合処理の高速化、マルチメディア情報を伝送する通信路の負荷軽減を図ることができる。

【図面の簡単な説明】

【０１２７】

【図１】実施例１における照合装置を示す図である。

【図２】実施例１におけるマルチメディア情報照合部での照合処理の詳細なフロー（例１）を示す図である。

【図３】実施例１におけるマルチメディア画像情報の一例として、草花の葉脈を用いる例を示す図である。

【図４】実施例１におけるマルチメディア情報照合部での照合処理の詳細なフロー（例２）を示す図である。

【図５】実施例２における登録装置を示す図である。

【図６】実施例２におけるマルチメディア情報分割部により３つに分割したマルチメディア情報を各記憶部に格納する概要を示す図である。

【図７】実施例３における分割・組み合わせの概念を示す図である。

【図８】実施例３における照合装置を示す図である。

【図９】実施例４における照合装置を示す図である。

【図１０】実施例５における照合装置を示す図である。

【図１１】実施例６における登録装置を示す図である。

【図１２】実施例６における照合装置を示す図である。

【図１３】実施例６における暗号化のフローを示す図である。

【図１４】実施例６における復号化のフローを示す図である。

【図１５】実施例７における暗号化のフローを示す図である。

【図１６】実施例７における復号化のフローを示す図である。

【図１７】実施例８における暗号化のフロー（例１）を示す図である。

【図１８】実施例８における復号化のフロー（例１）を示す図である。

【図１９】実施例８における暗号化のフロー（例２）を示す図である。

【図２０】実施例８における復号化のフロー（例２）を示す図である。

【図２１】実施例９における複数の個人に属する分割マルチメディア情報を組み合わせて合成する概要を示す図である。

【図２２】実施例９における照合装置を示す図である。

【図２３】実施例１０における、各記憶部に記憶する対象者の人数を変えた場合の記憶装置の格納例を示す。

【図２４】実施例１０における照合を行う際にどの記憶部から情報を取り出すかの処理概要を示す図である。

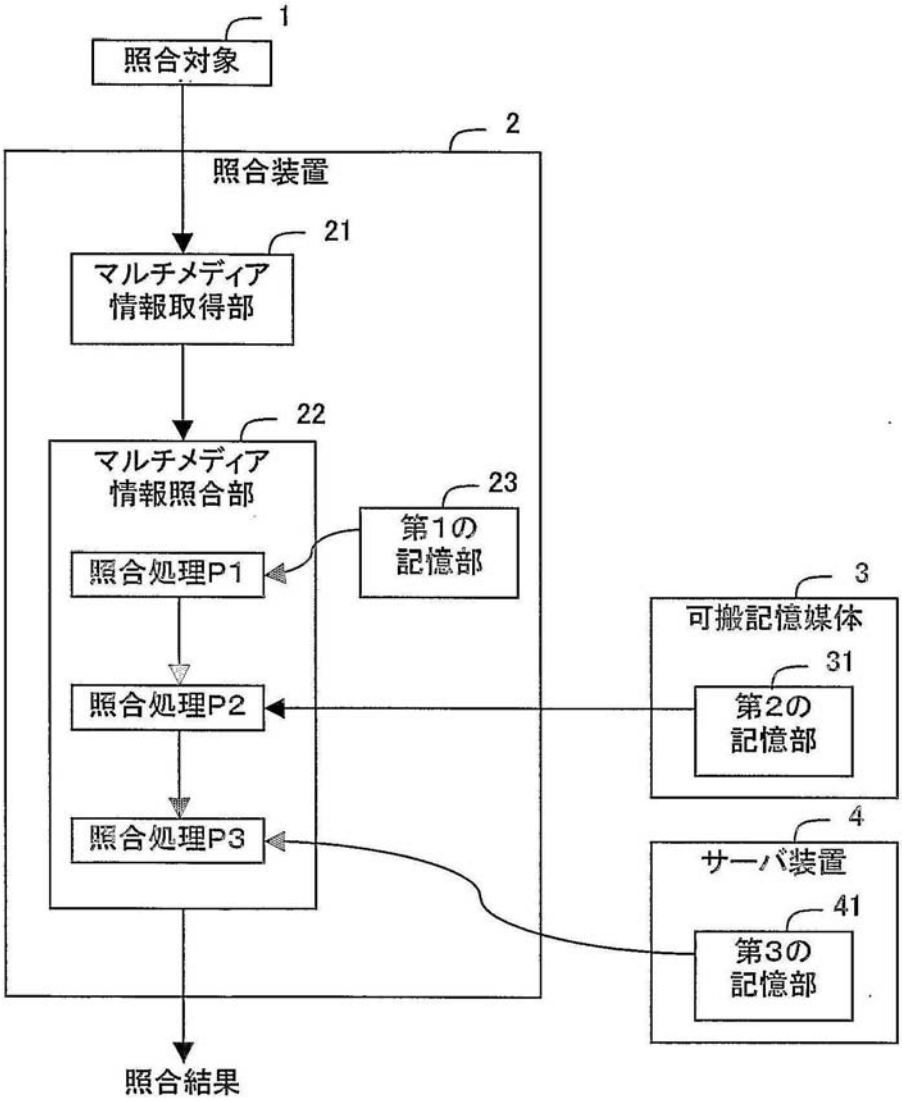
【図２５】本発明におけるハードウエア環境の構成ブロック図である。

【符号の説明】

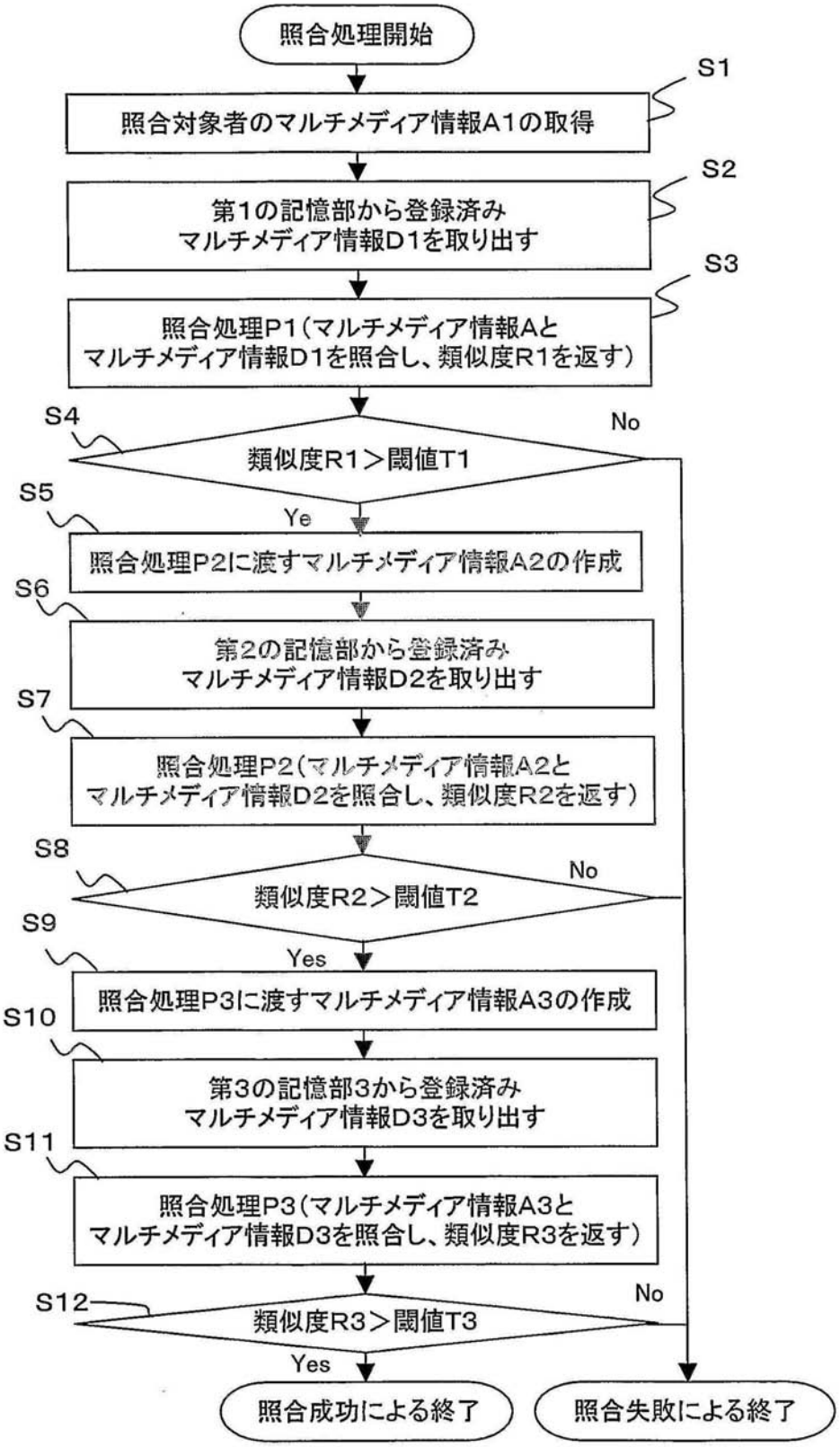
【０１２８】

２　照合装置
２１　マルチメディア情報取得部
２２　マルチメディア情報照合部
２３　第１の記憶部
２５　マルチメディア情報合成部
２６　照合情報選択制御部
２７　復号部
３　可搬記憶媒体
３１　第２の記憶部
４　サーバ装置
４１　第３の記憶部
５　登録装置
５１　マルチメディア取得部
５２　マルチメディア分割部
５３　第１の記憶部
５４　格納制御部
５５　暗号部
６１　出力Ｉ／Ｆ
６２　ＣＰＵ
６３　ＲＯＭ
６４　通信Ｉ／Ｆ
６５　入力Ｉ／Ｆ
６６　ＲＡＭ
６７　記憶装置
６８　可搬型記憶媒体の読み取り装置
６９　バス
７０　出力装置
７１　入力装置
７２　ネットワーク

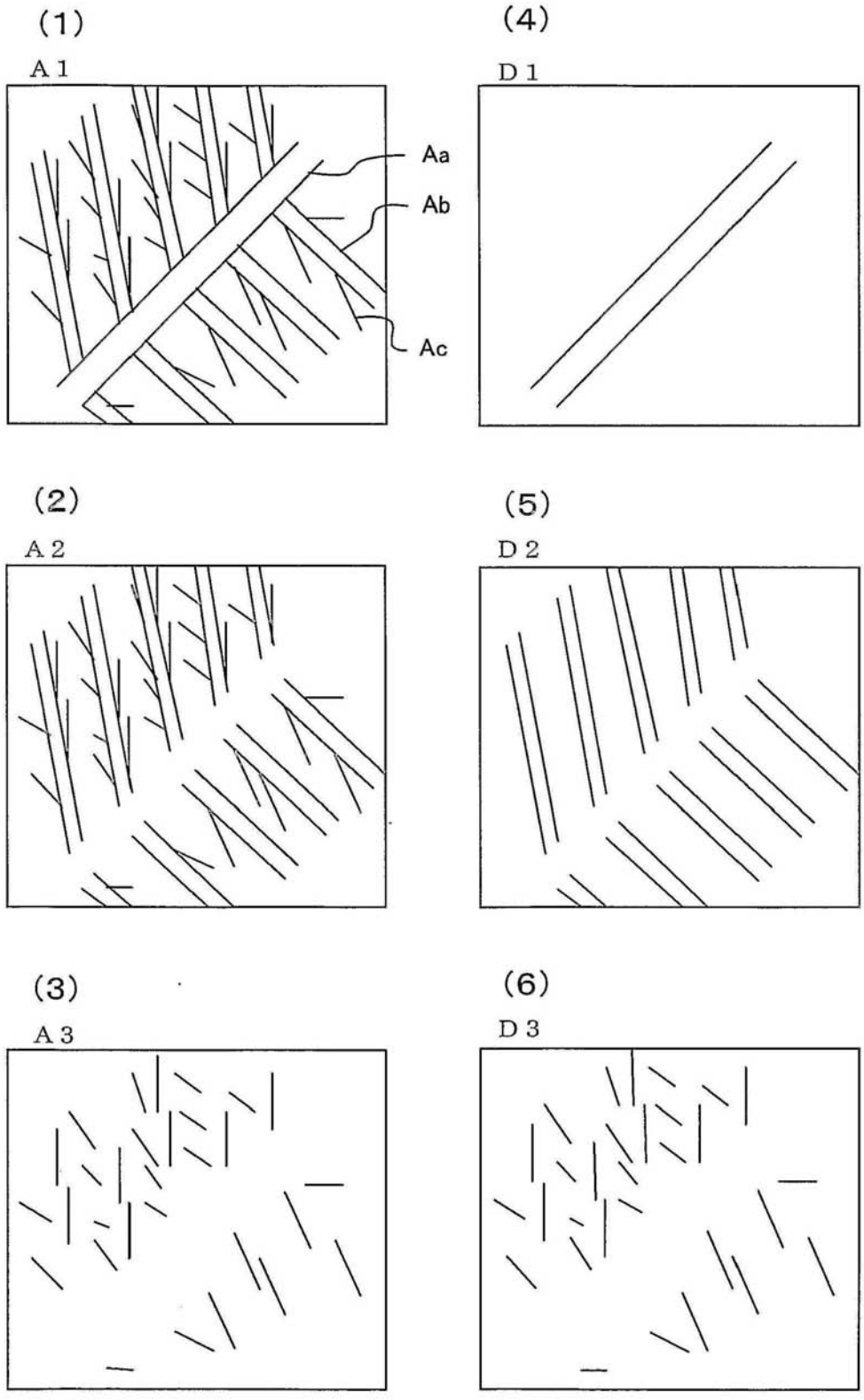
【図１】


1
照合対象
2
照合装置
21
マルチメディア
情報取得部
22
マルチメディア
情報照合部
23
第1の
記憶部
照合処理P1
照合処理P2
照合処理P3
3
可搬記憶媒体
31
第2の
記憶部
4
サーバ装置
41
第3の
記憶部
照合結果

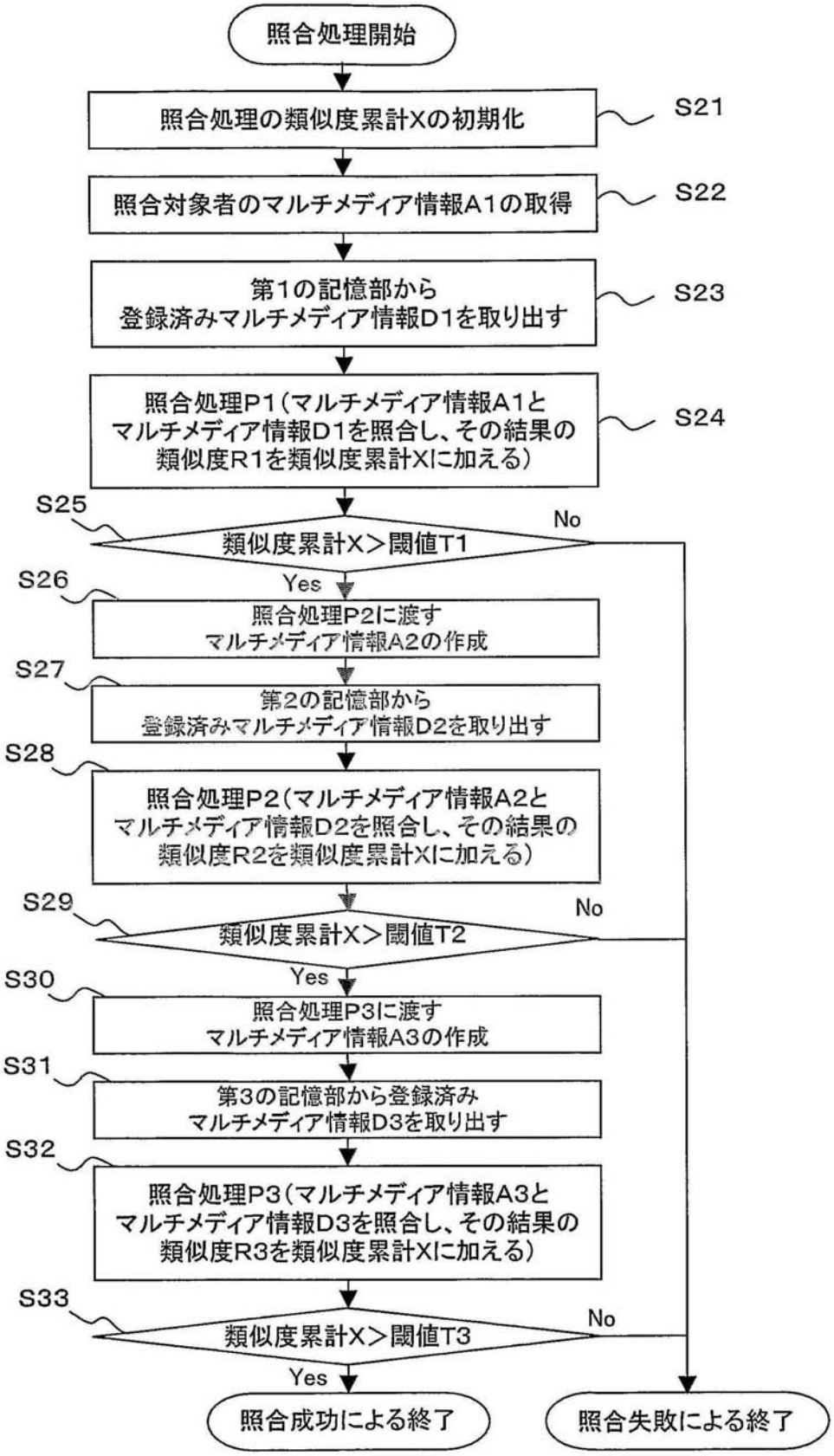
【図２】


照合処理開始
S1
照合対象者のマルチメディア情報A1の取得
S2
第1の記憶部から登録済み
マルチメディア情報D1を取り出す
S3
照合処理P1（マルチメディア情報Aと
マルチメディア情報D1を照合し、類似度R1を返す）
S4
類似度R1＞閾値T1
No
Ye
S5
照合処理P2に渡すマルチメディア情報A2の作成
S6
第2の記憶部から登録済み
マルチメディア情報D2を取り出す
S7
照合処理P2（マルチメディア情報A2と
マルチメディア情報D2を照合し、類似度R2を返す）
S8
類似度R2＞閾値T2
No
S9
Yes
照合処理P3に渡すマルチメディア情報A3の作成
S10
第3の記憶部3から登録済み
マルチメディア情報D3を取り出す
S11
照合処理P3（マルチメディア情報A3と
マルチメディア情報D3を照合し、類似度R3を返す）
S12
類似度R3＞閾値T3
No
Yes
照合成功による終了
照合失敗による終了

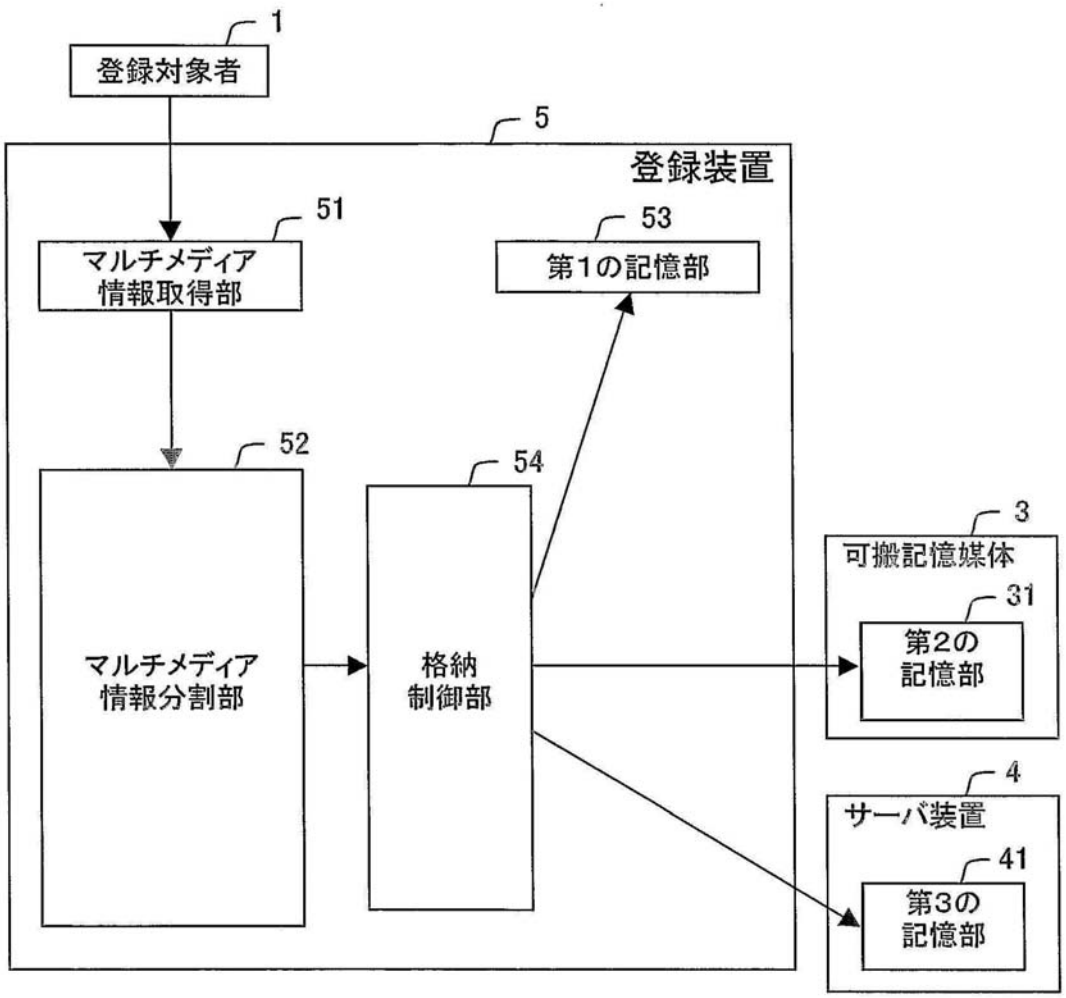
【図３】



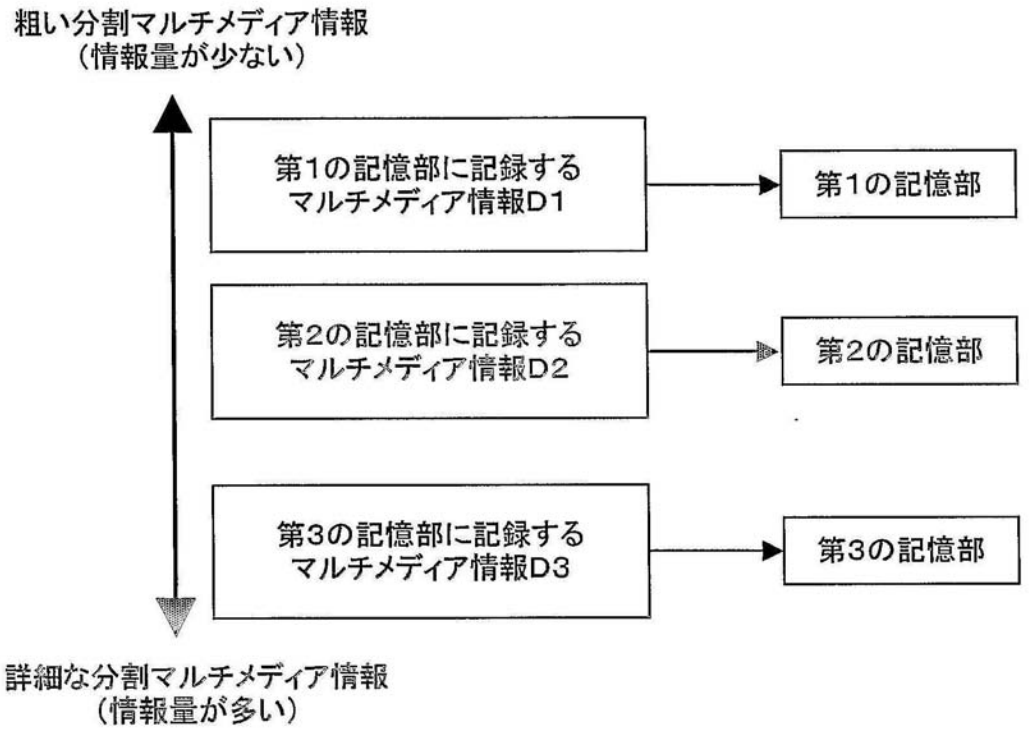
【図４】


照合処理開始
照合処理の類似度累計Xの初期化
S21
照合対象者のマルチメディア情報A1の取得
S22
第1の記憶部から
登録済みマルチメディア情報D1を取り出す
S23
照合処理P1（マルチメディア情報A1と
マルチメディア情報D1を照合し、その結果の
類似度R1を類似度累計Xに加える）
S24
S25
類似度累計X＞閾値T1
No
Yes
S26
照合処理P2に渡す
マルチメディア情報A2の作成
S27
第2の記憶部から
登録済みマルチメディア情報D2を取り出す
S28
照合処理P2（マルチメディア情報A2と
マルチメディア情報D2を照合し、その結果の
類似度R2を類似度累計Xに加える）
S29
類似度累計X＞閾値T2
No
Yes
S30
照合処理P3に渡す
マルチメディア情報A3の作成
S31
第3の記憶部から登録済み
マルチメディア情報D3を取り出す
S32
照合処理P3（マルチメディア情報A3と
マルチメディア情報D3を照合し、その結果の
類似度R3を類似度累計Xに加える）
S33
類似度累計X＞閾値T3
No
Yes
照合成功による終了
照合失敗による終了

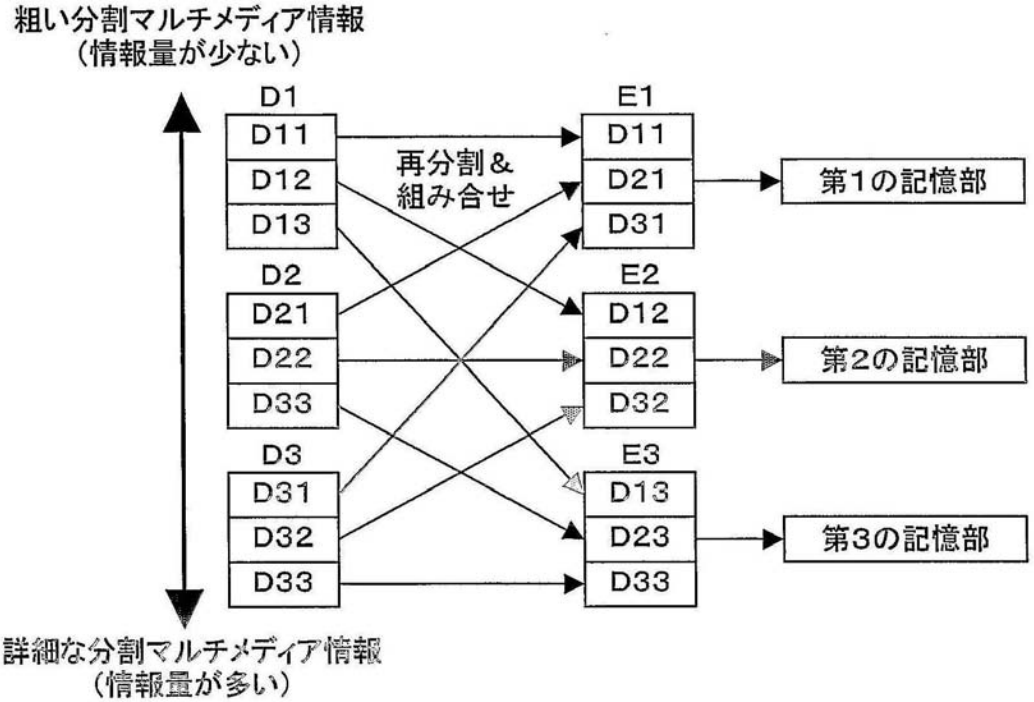
【図５】


1
登録対象者
5
登録装置
51
マルチメディア
情報取得部
53
第1の記憶部
52
マルチメディア
情報分割部
54
格納
制御部
3
可搬記憶媒体
31
第2の
記憶部
4
サーバ装置
41
第3の
記憶部

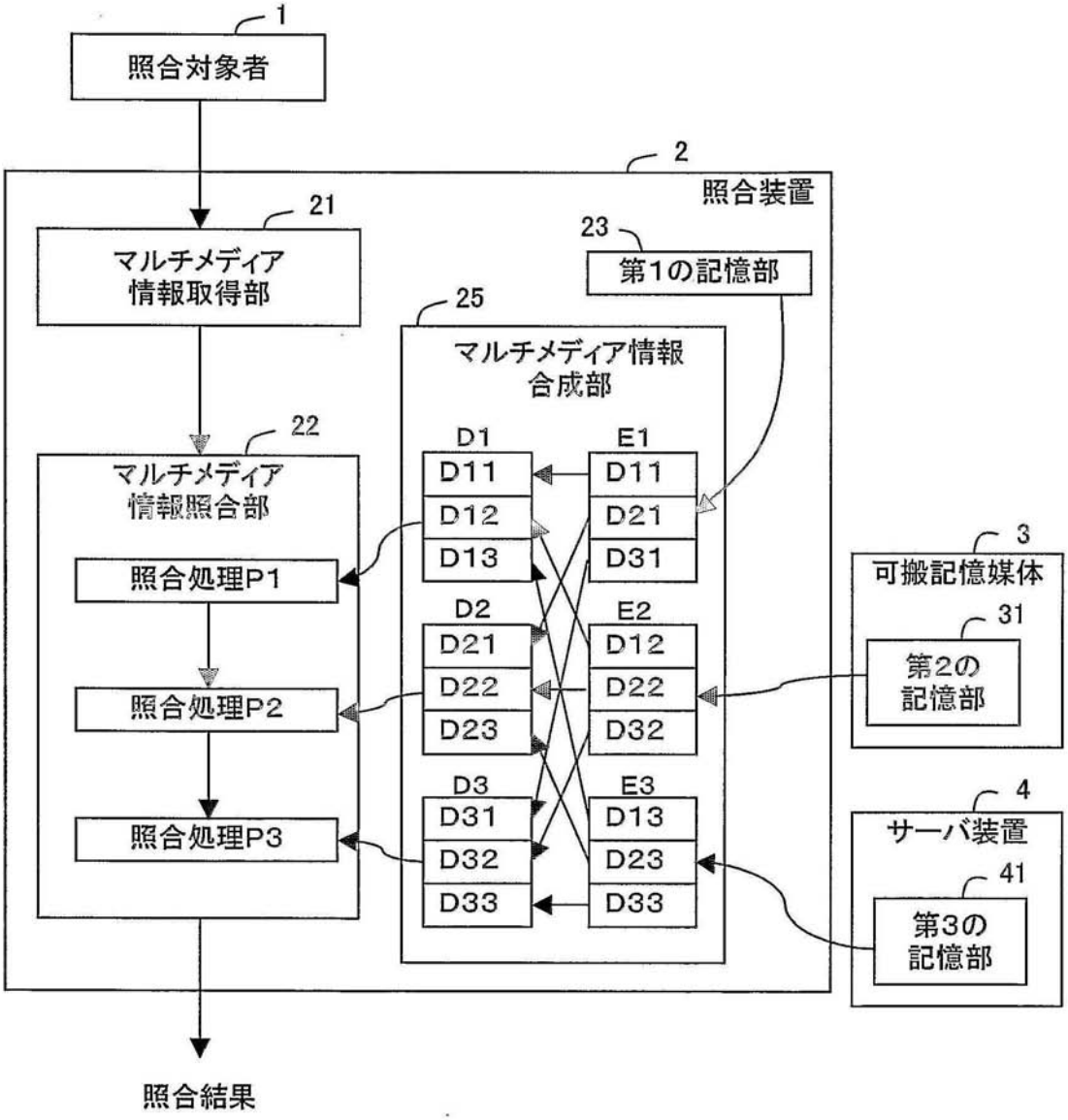
【図６】


粗い分割マルチメディア情報
（情報量が少ない）
第1の記憶部に記録する
マルチメディア情報D1
第1の記憶部
第2の記憶部に記録する
マルチメディア情報D2
第2の記憶部
第3の記憶部に記録する
マルチメディア情報D3
第3の記憶部
詳細な分割マルチメディア情報
（情報量が多い）

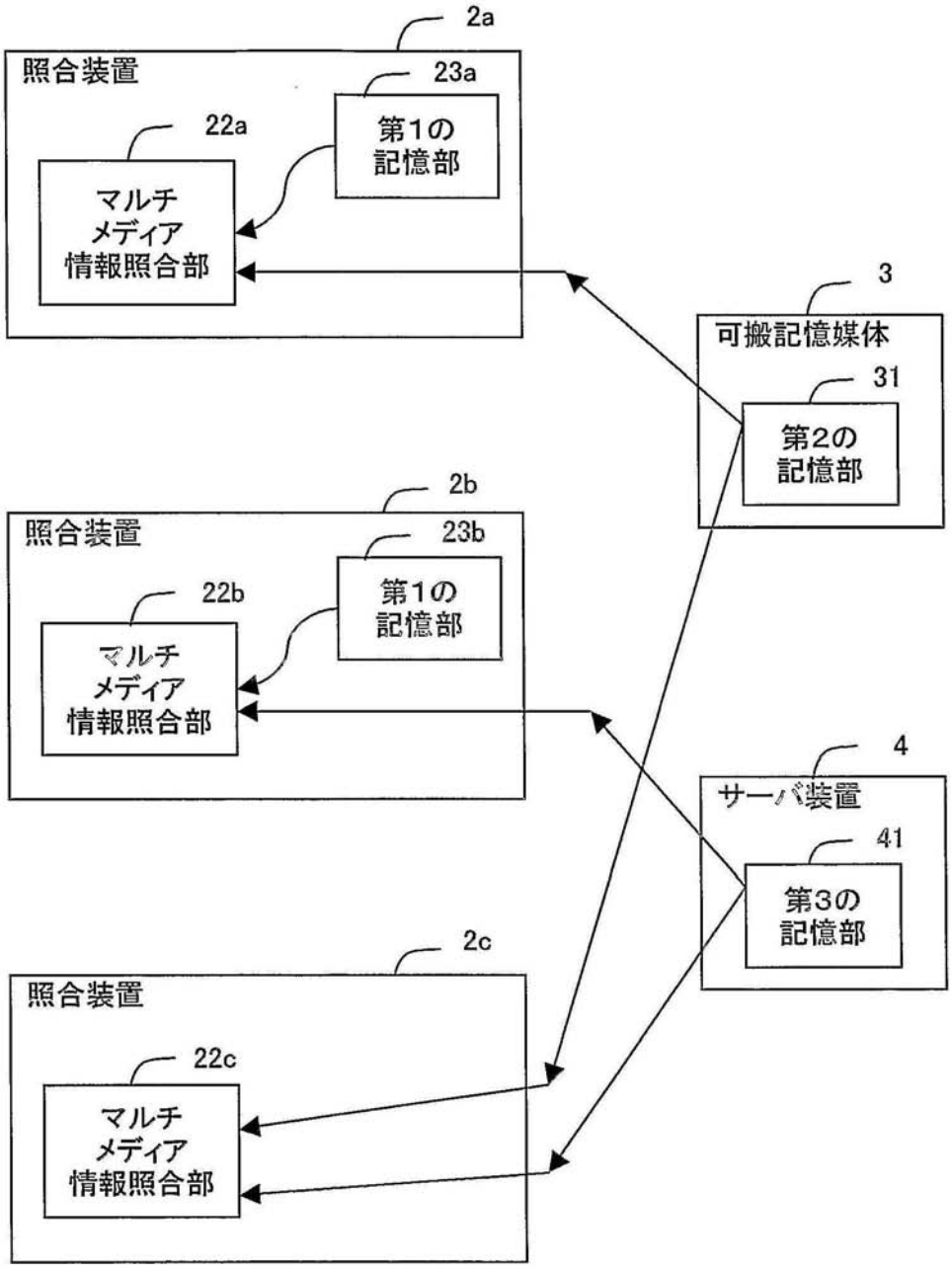
【図７】


粗い分割マルチメディア情報
（情報量が少ない）
D1
D11
D12
D13
D2
D21
D22
D33
D3
D31
D32
D33
再分割＆
組み合せ
E1
D11
D21
D31
E2
D12
D22
D32
E3
D13
D23
D33
第1の記憶部
第2の記憶部
第3の記憶部
詳細な分割マルチメディア情報
（情報量が多い）

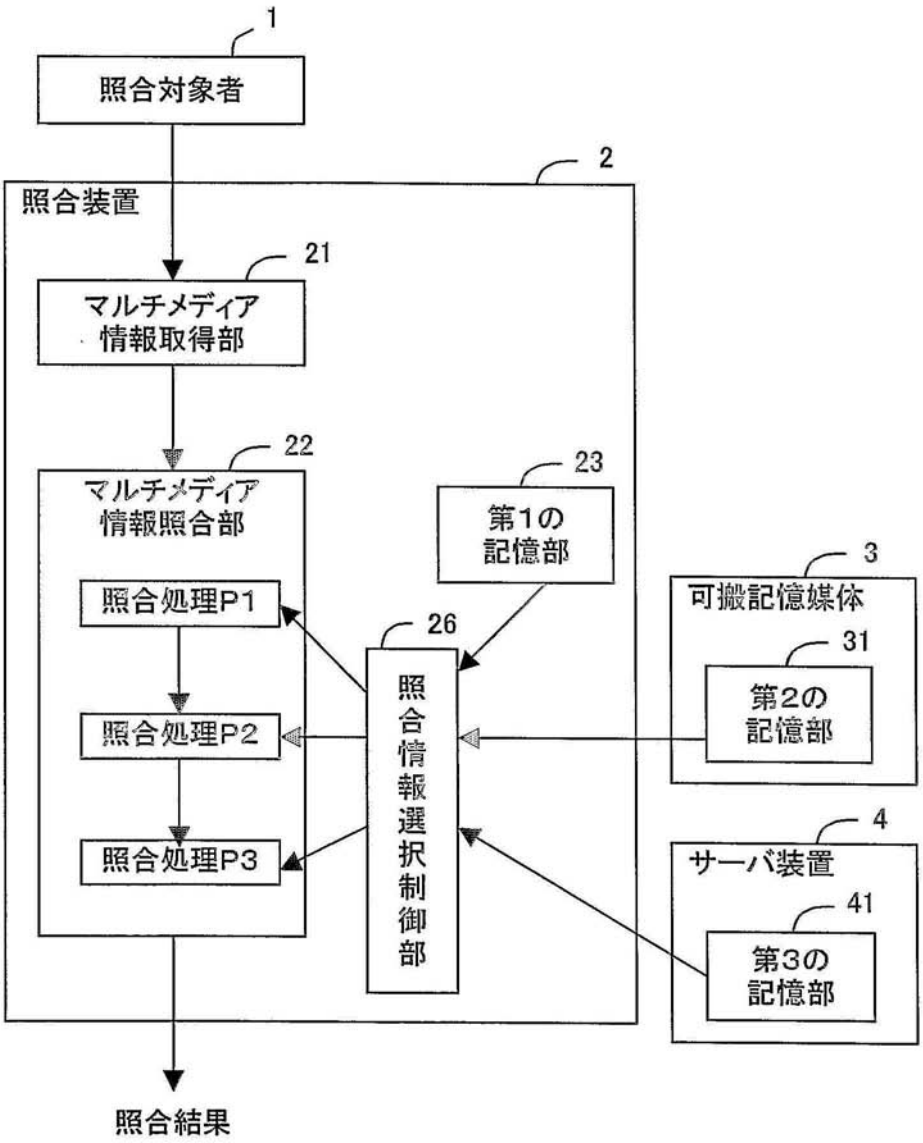
【図８】


1
照合対象者
2
照合装置
21
マルチメディア
情報取得部
23
第1の記憶部
25
マルチメディア情報
合成部
22
マルチメディア
情報照合部
D1
D11
D12
D13
E1
D11
D21
D31
照合処理P1
照合処理P2
照合処理P3
D2
D21
D22
D23
E2
D12
D22
D32
D3
D31
D32
D33
E3
D13
D23
D33
3
可搬記憶媒体
31
第2の
記憶部
4
サーバ装置
41
第3の
記憶部
照合結果

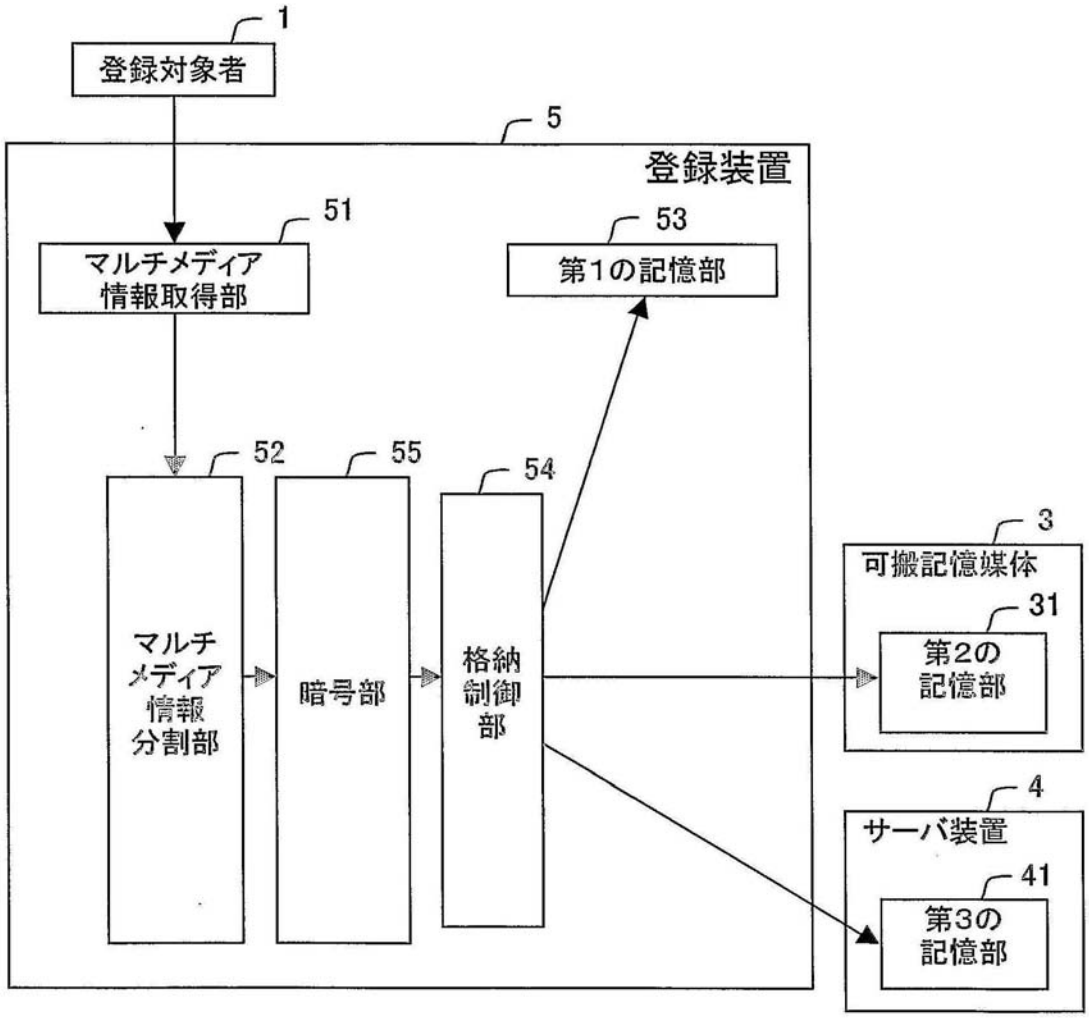
【図９】


2a
照合装置
23a
第1の
記憶部
22a
マルチ
メディア
情報照合部
3
可搬記憶媒体
31
第2の
記憶部
2b
照合装置
23b
第1の
記憶部
22b
マルチ
メディア
情報照合部
4
サーバ装置
41
第3の
記憶部
2c
照合装置
22c
マルチ
メディア
情報照合部

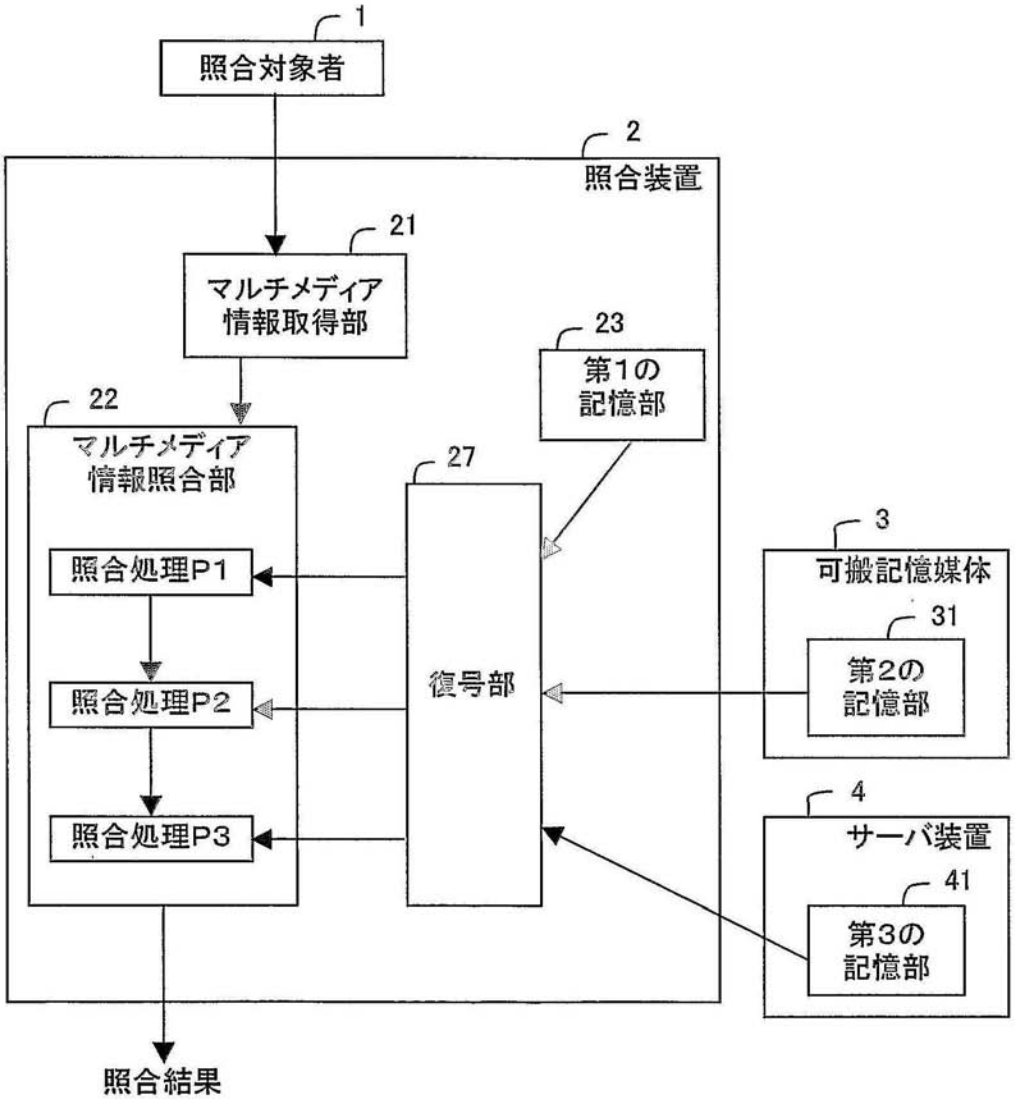
【図１０】


1
照合対象者
2
照合装置
21
マルチメディア
情報取得部
22
マルチメディア
情報照合部
照合処理P1
照合処理P2
照合処理P3
23
第1の
記憶部
26
照合情報選択制御部
3
可搬記憶媒体
31
第2の
記憶部
4
サーバ装置
41
第3の
記憶部
照合結果

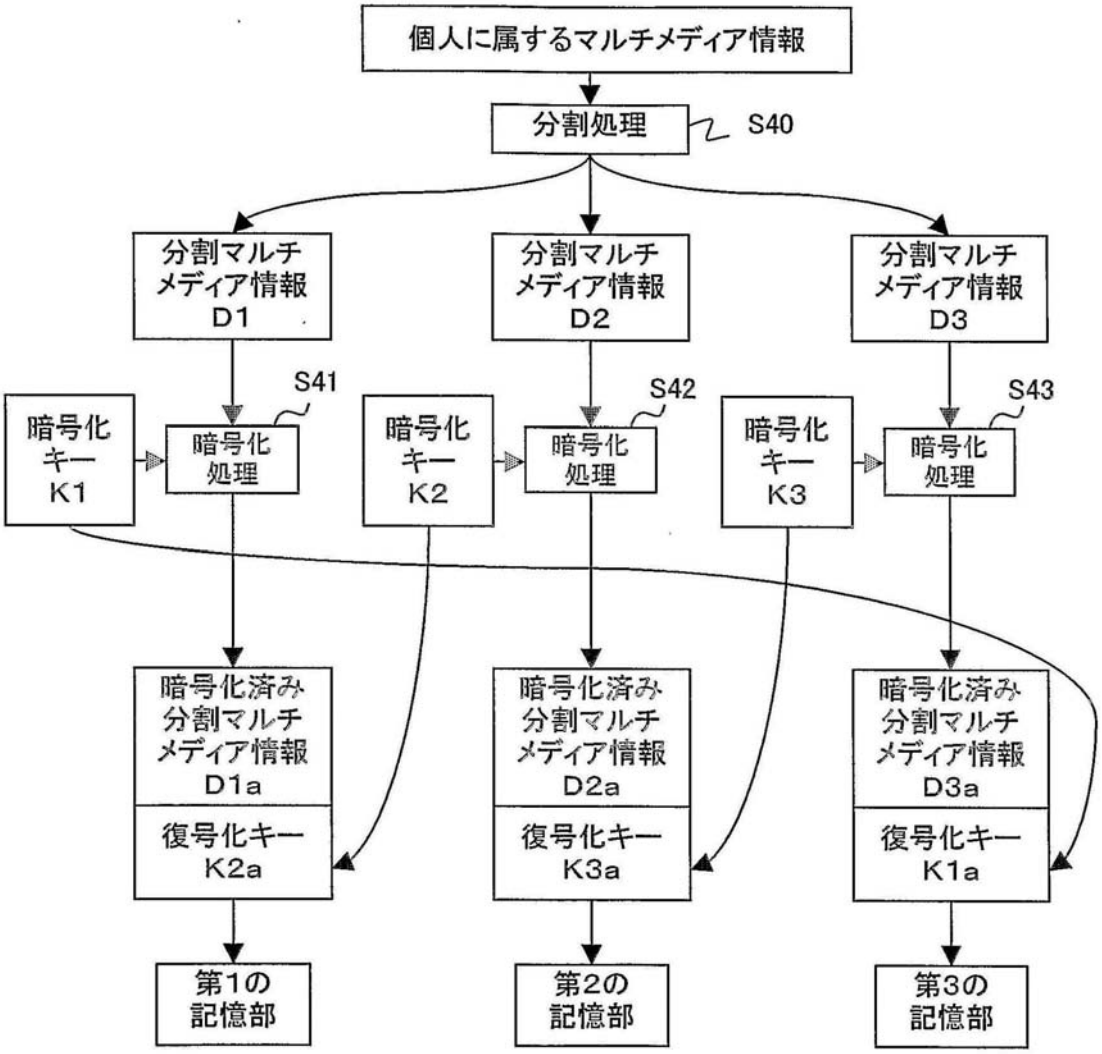
【図１１】


1
登録対象者
5
登録装置
51
マルチメディア
情報取得部
53
第1の記憶部
52
55
54
マルチ
メディア
情報
分割部
暗号部
格納
制御
部
3
可搬記憶媒体
31
第2の
記憶部
4
サーバ装置
41
第3の
記憶部

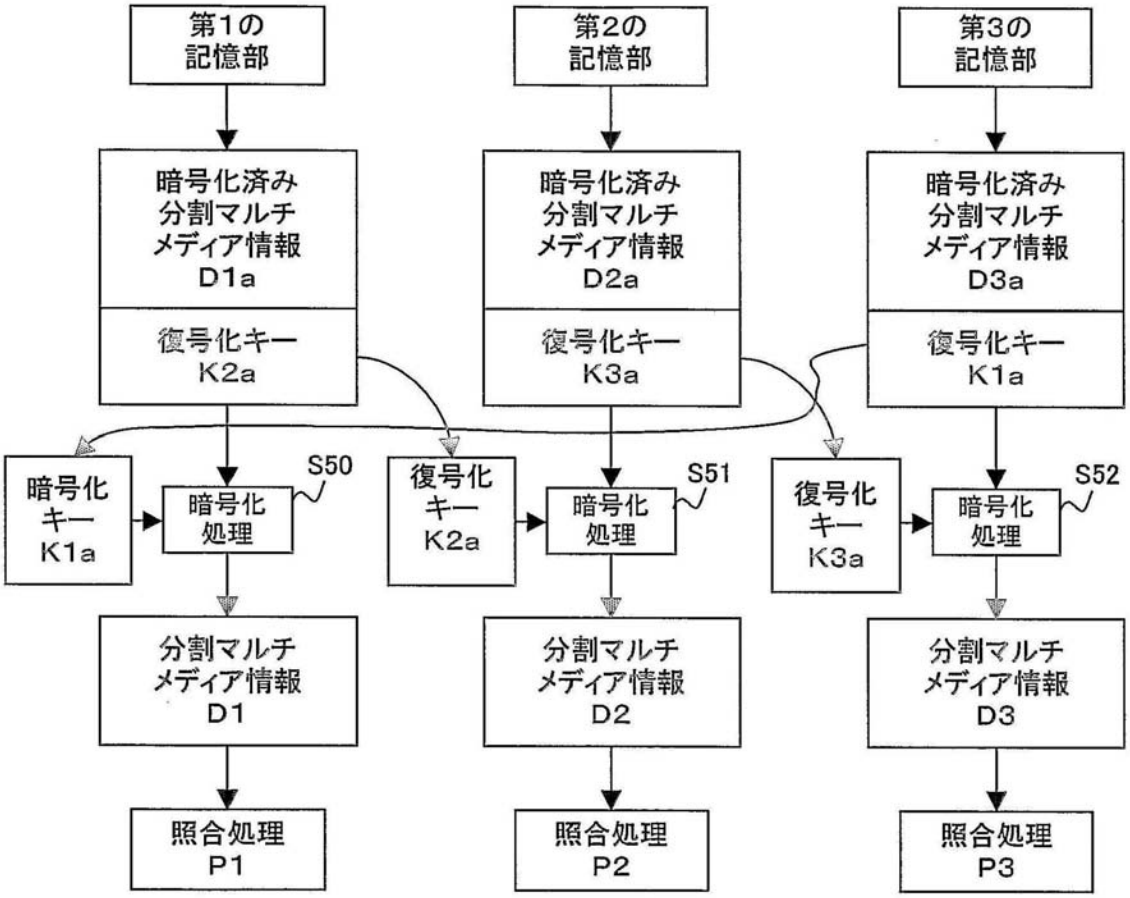
【図１２】


1
照合対象者
2
照合装置
21
マルチメディア
情報取得部
23
第1の
記憶部
22
マルチメディア
情報照合部
27
照合処理P1
照合処理P2
照合処理P3
復号部
3
可搬記憶媒体
31
第2の
記憶部
4
サーバ装置
41
第3の
記憶部
照合結果

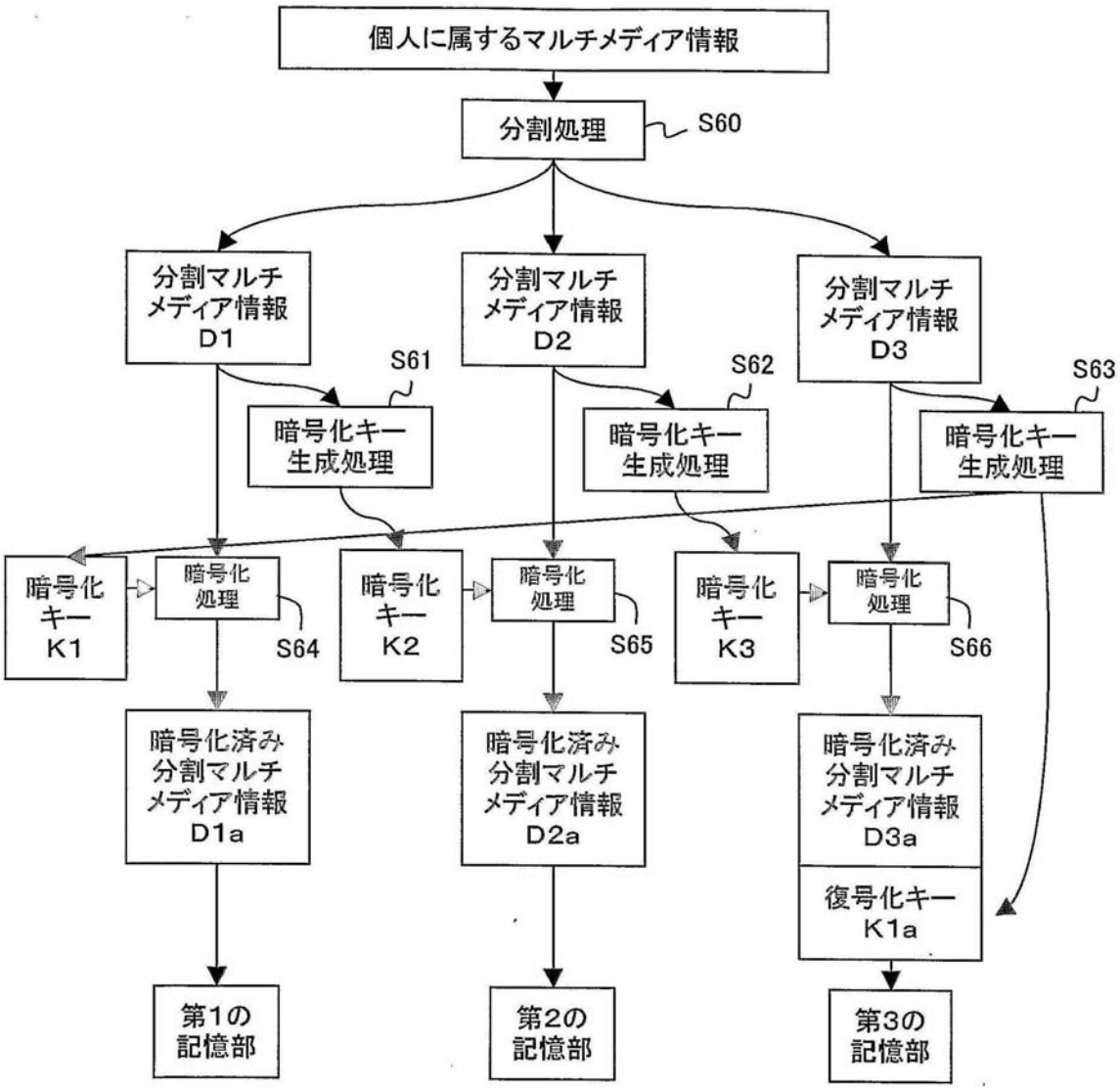
【図１３】


個人に属するマルチメディア情報
分割処理
S40
分割マルチメディア情報D1
分割マルチメディア情報D2
分割マルチメディア情報D3
S41
S42
S43
暗号化キーK1
暗号化キーK2
暗号化キーK3
暗号化処理
暗号化処理
暗号化処理
暗号化済み分割マルチメディア情報D1a
暗号化済み分割マルチメディア情報D2a
暗号化済み分割マルチメディア情報D3a
復号化キーK2a
復号化キーK3a
復号化キーK1a
第1の記憶部
第2の記憶部
第3の記憶部

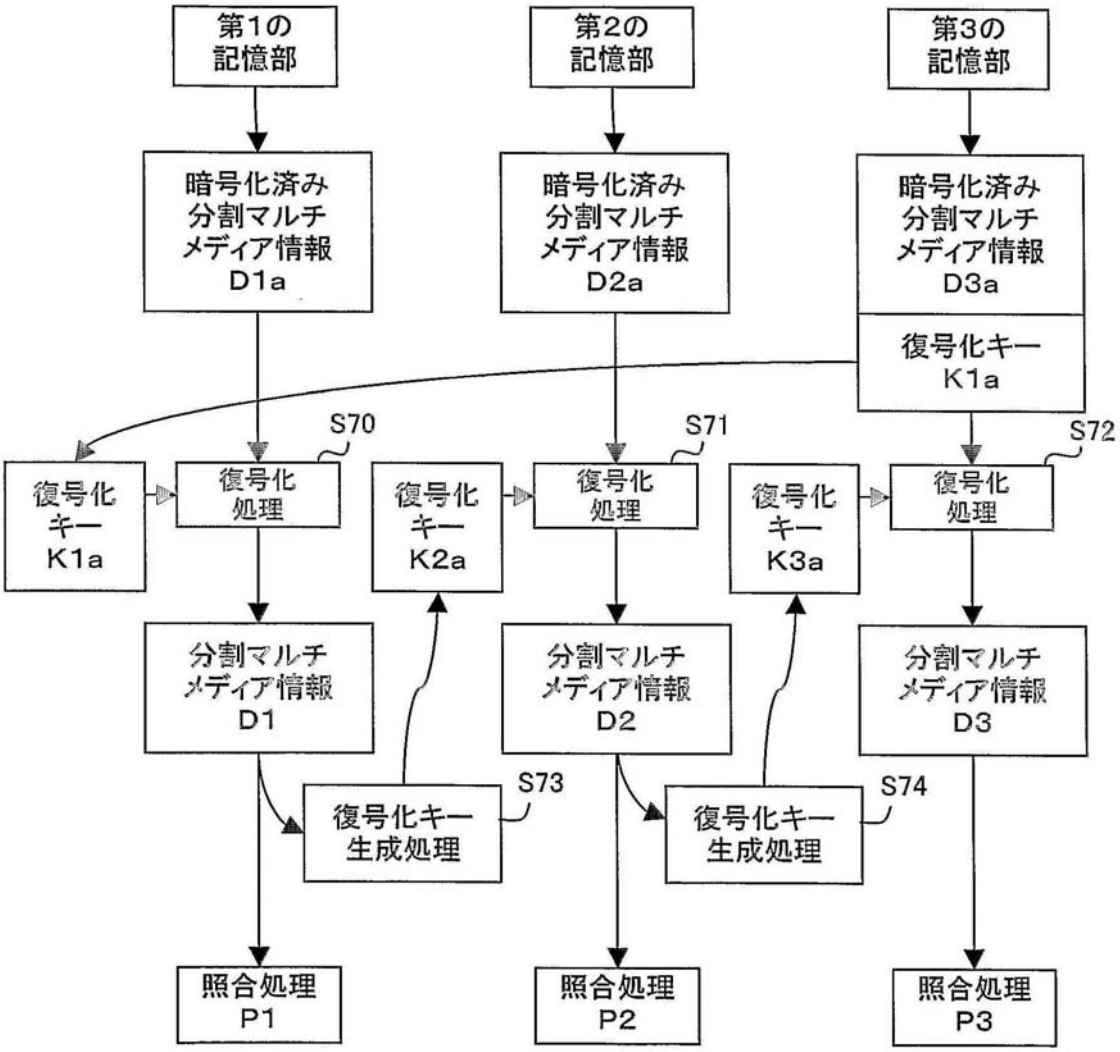
【図１４】


第1の
記憶部
第2の
記憶部
第3の
記憶部
暗号化済み
分割マルチ
メディア情報
D1a
暗号化済み
分割マルチ
メディア情報
D2a
暗号化済み
分割マルチ
メディア情報
D3a
復号化キー
K2a
復号化キー
K3a
復号化キー
K1a
暗号化
キー
K1a
暗号化
処理
S50
復号化
キー
K2a
暗号化
処理
S51
復号化
キー
K3a
暗号化
処理
S52
分割マルチ
メディア情報
D1
分割マルチ
メディア情報
D2
分割マルチ
メディア情報
D3
照合処理
P1
照合処理
P2
照合処理
P3

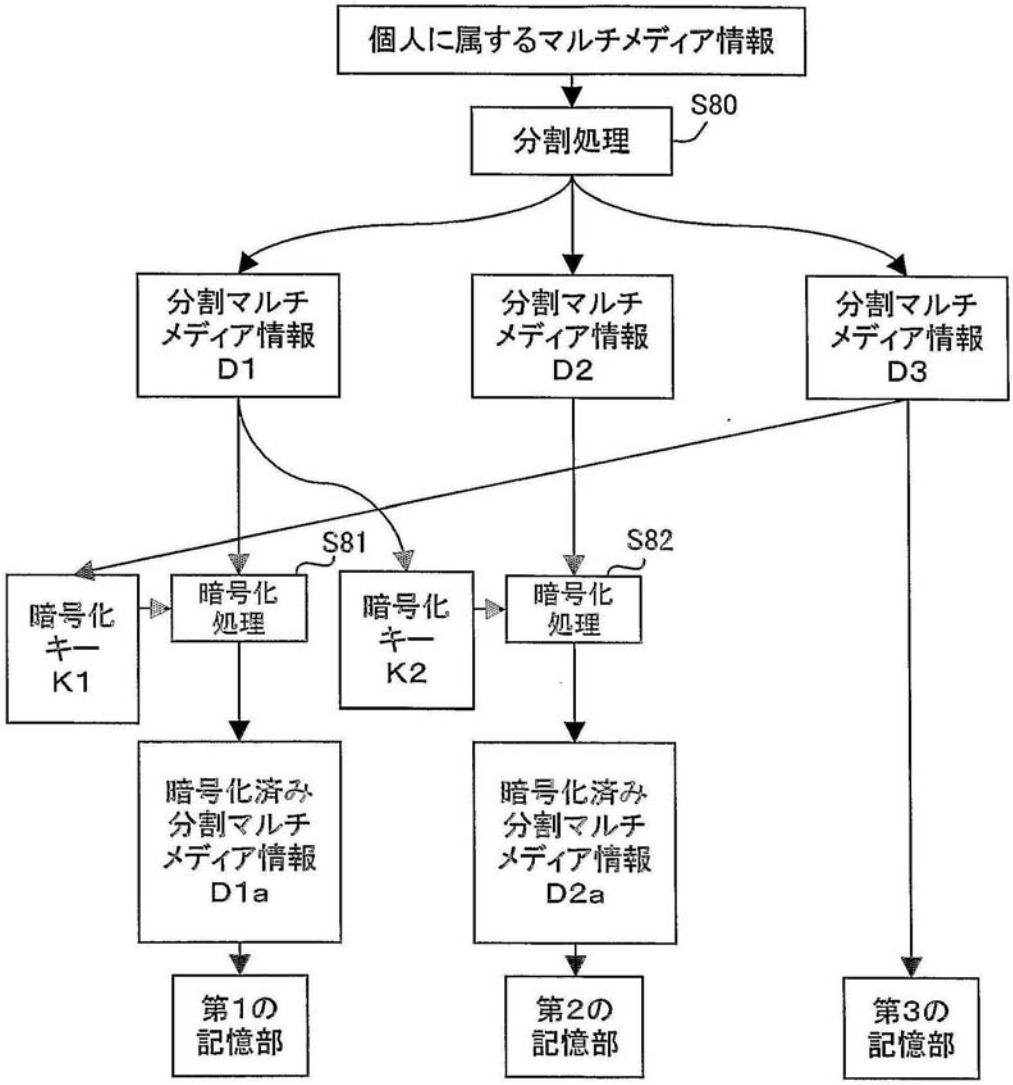
【図１５】


個人に属するマルチメディア情報
分割処理
S60
分割マルチメディア情報D1
分割マルチメディア情報D2
分割マルチメディア情報D3
S61
S62
S63
暗号化キー生成処理
暗号化キー生成処理
暗号化キー生成処理
暗号化キーK1
暗号化処理
S64
暗号化キーK2
暗号化処理
S65
暗号化キーK3
暗号化処理
S66
暗号化済み分割マルチメディア情報D1a
暗号化済み分割マルチメディア情報D2a
暗号化済み分割マルチメディア情報D3a
復号化キーK1a
第1の記憶部
第2の記憶部
第3の記憶部

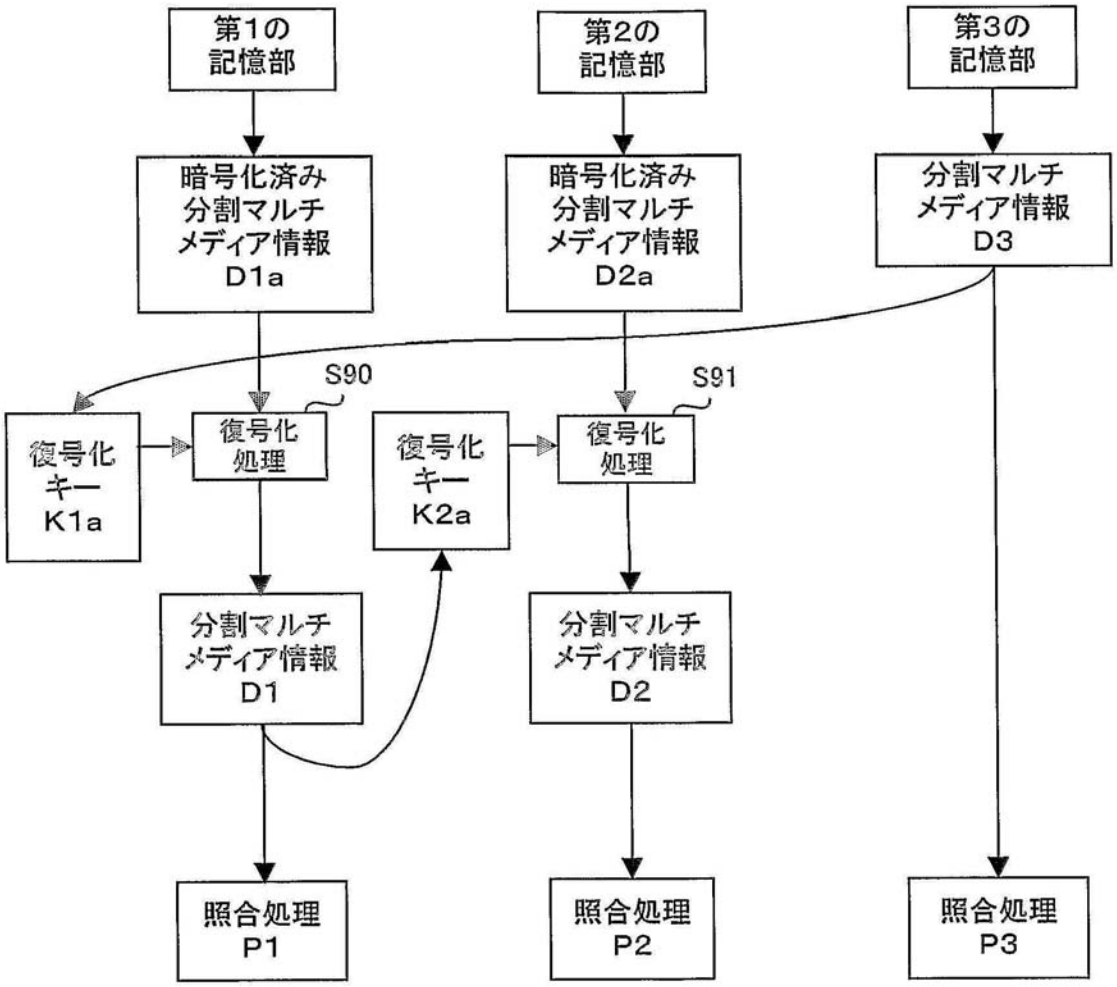
【図１６】


第1の
記憶部
第2の
記憶部
第3の
記憶部
暗号化済み
分割マルチ
メディア情報
D1a
暗号化済み
分割マルチ
メディア情報
D2a
暗号化済み
分割マルチ
メディア情報
D3a
復号化キー
K1a
S70
S71
S72
復号化
キー
K1a
復号化
処理
復号化
キー
K2a
復号化
処理
復号化
キー
K3a
復号化
処理
分割マルチ
メディア情報
D1
分割マルチ
メディア情報
D2
分割マルチ
メディア情報
D3
S73
S74
復号化キー
生成処理
復号化キー
生成処理
照合処理
P1
照合処理
P2
照合処理
P3

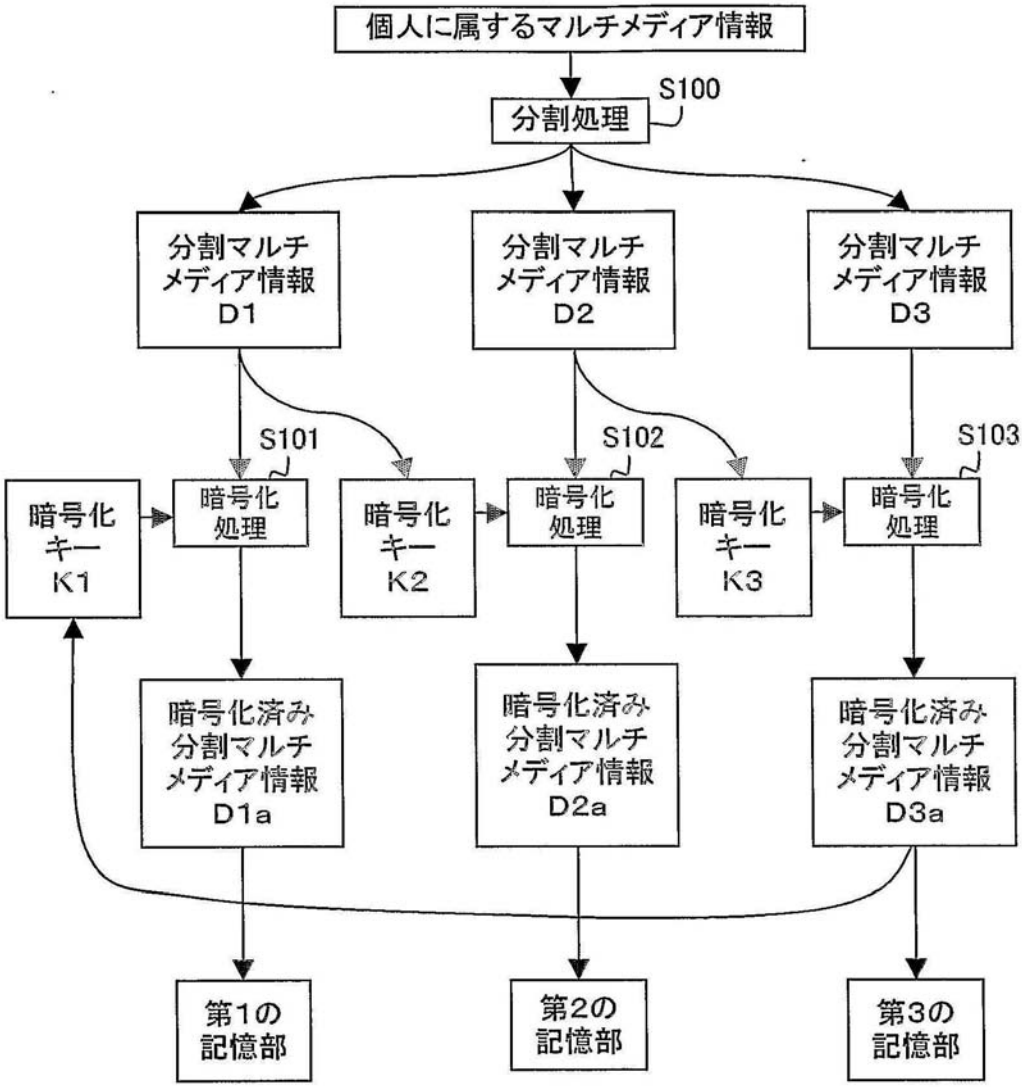
【図１７】


個人に属するマルチメディア情報
分割処理
S80
分割マルチメディア情報D1
分割マルチメディア情報D2
分割マルチメディア情報D3
S81
S82
暗号化キーK1
暗号化処理
暗号化キーK2
暗号化処理
暗号化済み分割マルチメディア情報D1a
暗号化済み分割マルチメディア情報D2a
第1の記憶部
第2の記憶部
第3の記憶部

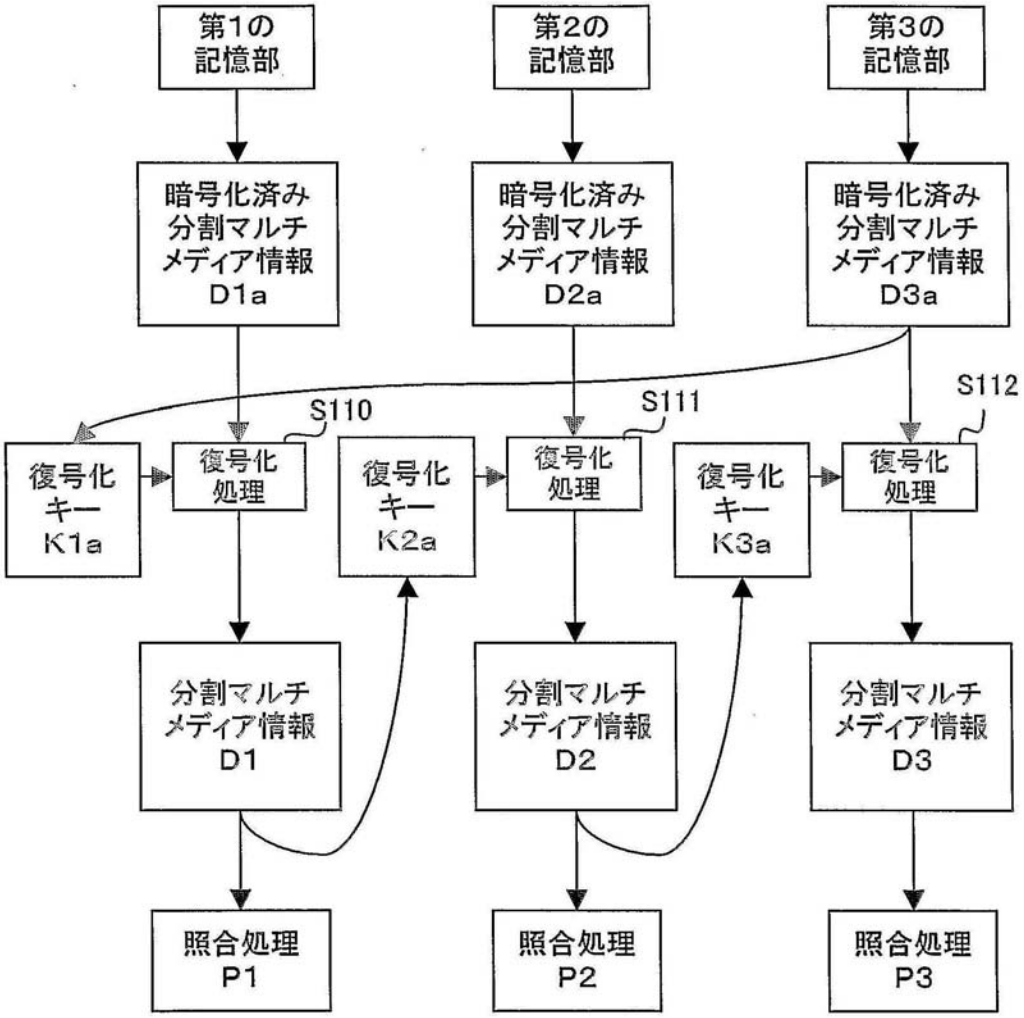
【図１８】


第1の
記憶部
第2の
記憶部
第3の
記憶部
暗号化済み
分割マルチ
メディア情報
D1a
暗号化済み
分割マルチ
メディア情報
D2a
分割マルチ
メディア情報
D3
S90
S91
復号化
キー
K1a
復号化
処理
復号化
キー
K2a
復号化
処理
分割マルチ
メディア情報
D1
分割マルチ
メディア情報
D2
照合処理
P1
照合処理
P2
照合処理
P3

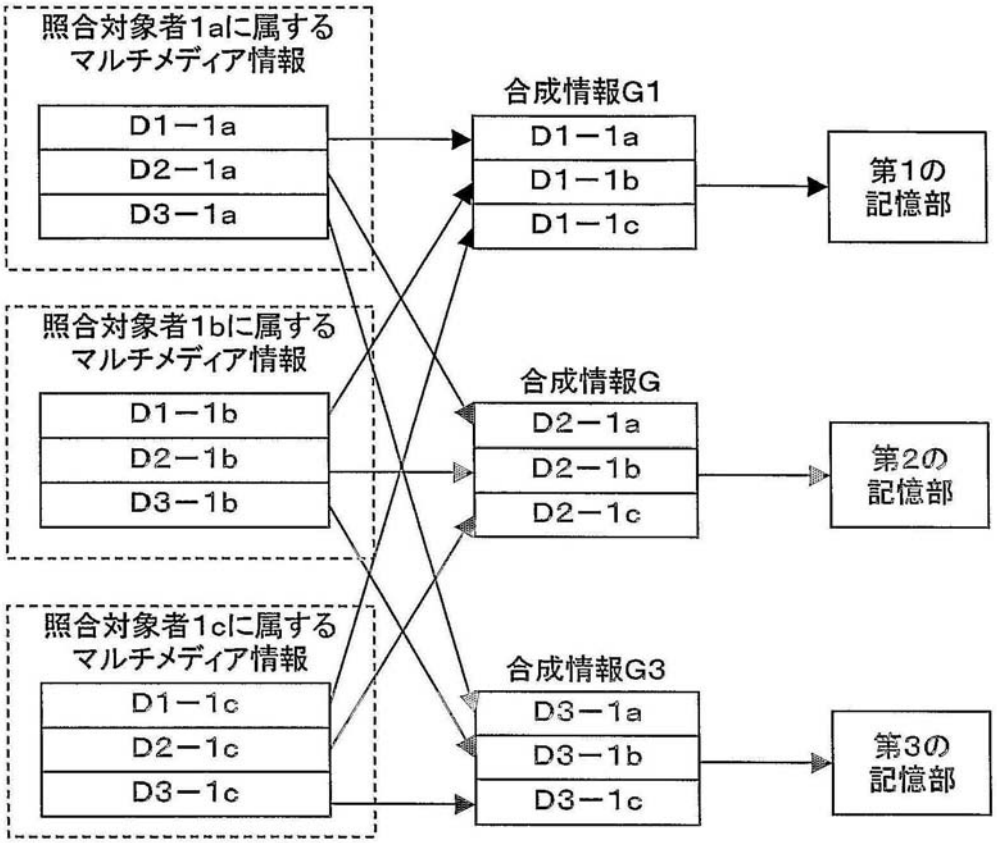
【図１９】


個人に属するマルチメディア情報
分割処理
S100
分割マルチメディア情報D1
分割マルチメディア情報D2
分割マルチメディア情報D3
S101
S102
S103
暗号化キーK1
暗号化処理
暗号化キーK2
暗号化処理
暗号化キーK3
暗号化処理
暗号化済み分割マルチメディア情報D1a
暗号化済み分割マルチメディア情報D2a
暗号化済み分割マルチメディア情報D3a
第1の記憶部
第2の記憶部
第3の記憶部

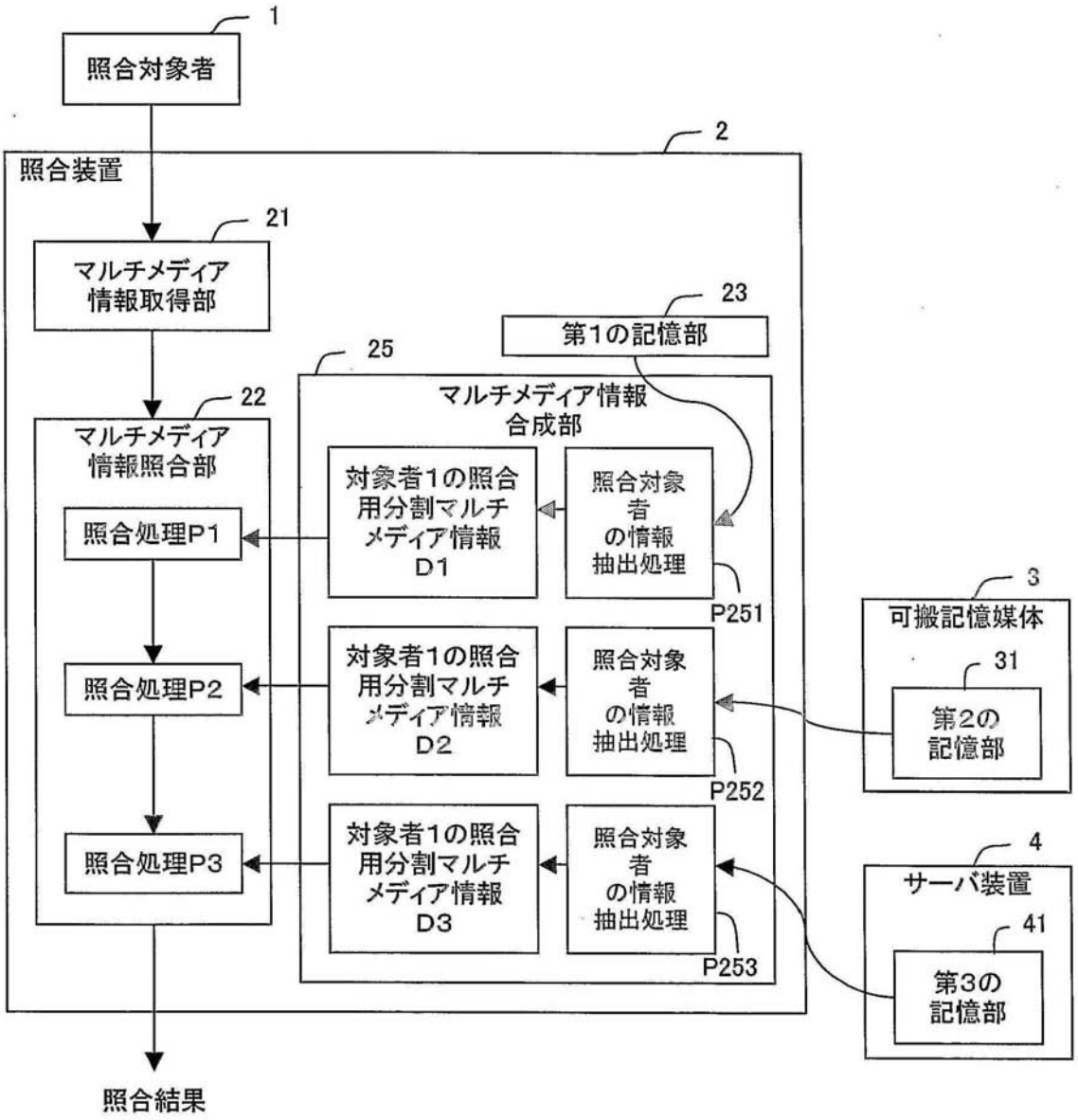
【図２０】


第1の
記憶部
第2の
記憶部
第3の
記憶部
暗号化済み
分割マルチ
メディア情報
D1a
暗号化済み
分割マルチ
メディア情報
D2a
暗号化済み
分割マルチ
メディア情報
D3a
S110
S111
S112
復号化
キー
K1a
復号化
処理
復号化
キー
K2a
復号化
処理
復号化
キー
K3a
復号化
処理
分割マルチ
メディア情報
D1
分割マルチ
メディア情報
D2
分割マルチ
メディア情報
D3
照合処理
P1
照合処理
P2
照合処理
P3

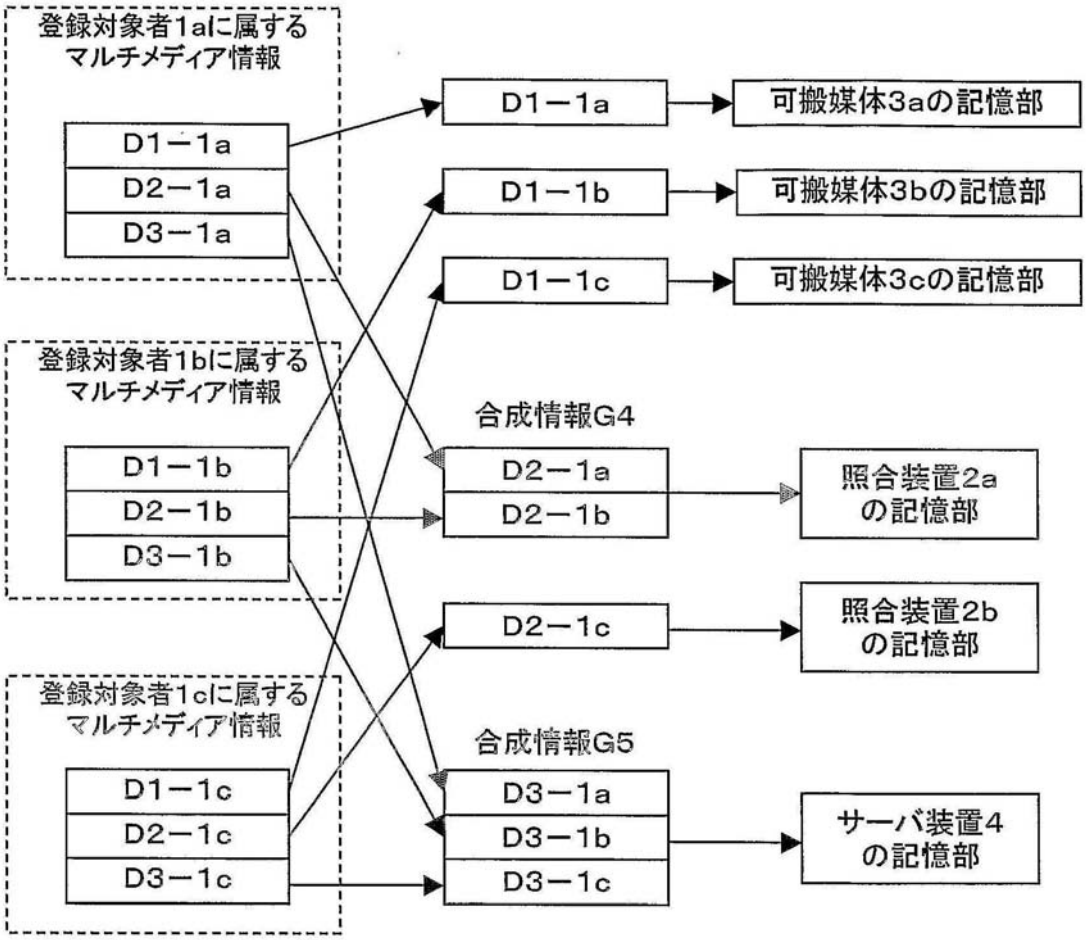
【図２１】


照合対象者1aに属する
マルチメディア情報
D1−1a
D2−1a
D3−1a
照合対象者1bに属する
マルチメディア情報
D1−1b
D2−1b
D3−1b
照合対象者1cに属する
マルチメディア情報
D1−1c
D2−1c
D3−1c
合成情報G1
D1−1a
D1−1b
D1−1c
合成情報G
D2−1a
D2−1b
D2−1c
合成情報G3
D3−1a
D3−1b
D3−1c
第1の
記憶部
第2の
記憶部
第3の
記憶部

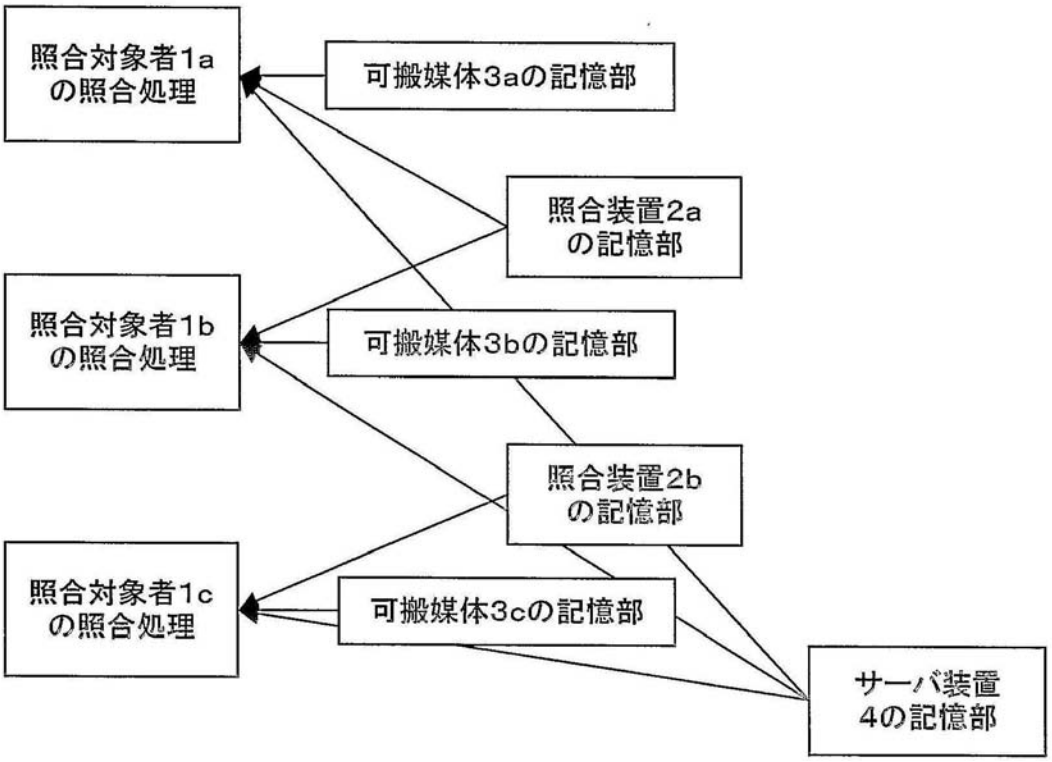
【図２２】


1
照合対象者
2
照合装置
21
マルチメディア
情報取得部
23
第1の記憶部
25
マルチメディア情報
合成部
22
マルチメディア
情報照合部
照合処理P1
照合処理P2
照合処理P3
対象者1の照合
用分割マルチ
メディア情報
D1
対象者1の照合
用分割マルチ
メディア情報
D2
対象者1の照合
用分割マルチ
メディア情報
D3
照合対象
者
の情報
抽出処理
P251
照合対象
者
の情報
抽出処理
P252
照合対象
者
の情報
抽出処理
P253
3
可搬記憶媒体
31
第2の
記憶部
4
サーバ装置
41
第3の
記憶部
照合結果

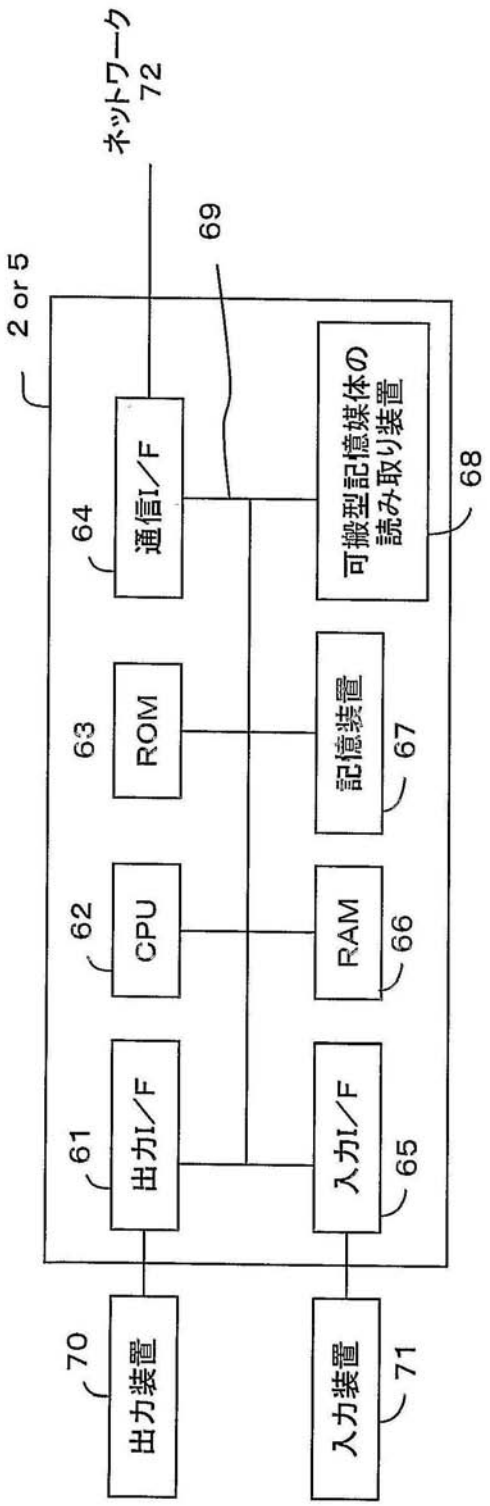
【図２３】


登録対象者1aに属する
マルチメディア情報
D1−1a
D2−1a
D3−1a
登録対象者1bに属する
マルチメディア情報
D1−1b
D2−1b
D3−1b
登録対象者1cに属する
マルチメディア情報
D1−1c
D2−1c
D3−1c
D1−1a
D1−1b
D1−1c
可搬媒体3aの記憶部
可搬媒体3bの記憶部
可搬媒体3cの記憶部
合成情報G4
D2−1a
D2−1b
照合装置2a
の記憶部
D2−1c
照合装置2b
の記憶部
合成情報G5
D3−1a
D3−1b
D3−1c
サーバ装置4
の記憶部

【図２４】


照合対象者1a
の照合処理
可搬媒体3aの記憶部
照合装置2a
の記憶部
照合対象者1b
の照合処理
可搬媒体3bの記憶部
照合装置2b
の記憶部
照合対象者1c
の照合処理
可搬媒体3cの記憶部
サーバ装置
4の記憶部

【図２５】


ネットワーク
72
69
2 or 5
64
通信I／F
63
ROM
62
CPU
61
出力I／F
可搬型記憶媒体の
読み取り装置
68
記憶装置
67
RAM
66
入力I／F
65
70
出力装置
71
入力装置

フロントページの続き

(72)発明者　遠藤　利生
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　渡辺　正規
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

審査官　間野　裕一

(56)参考文献　特開昭６２－２１２７８１（ＪＰ，Ａ）
特開２０００－２９３４９１（ＪＰ，Ａ）
国際公開第９９／０６０４８５（WO，Ａ１）
特開２００１－０６７１３７（ＪＰ，Ａ）
特開２００２－０３２７５６（ＪＰ，Ａ）
特開平１１－３３８８２６（ＪＰ，Ａ）
特開昭５７－０５５４６８（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／２０