(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7626558号
(P7626558)

(45)発行日　令和7年2月4日(2025.2.4)

(24)登録日　令和7年1月27日(2025.1.27)

(51)国際特許分類
Ｇ０９Ｃ　1/00　(2006.01)

ＦＩ
Ｇ０９Ｃ　1/00　６２０Ｚ

請求項の数　25　（全29頁）

(21)出願番号　特願2022-548236(P2022-548236)
(86)(22)出願日　令和3年2月2日(2021.2.2)
(65)公表番号　特表2023-512725(P2023-512725A)
(43)公表日　令和5年3月28日(2023.3.28)
(86)国際出願番号　PCT/IB2021/050816
(87)国際公開番号　WO2021/161131
(87)国際公開日　令和3年8月19日(2021.8.19)
審査請求日　令和5年7月21日(2023.7.21)
(31)優先権主張番号　16/787,211
(32)優先日　令和2年2月11日(2020.2.11)
(33)優先権主張国・地域又は機関
米国(US)

(73)特許権者　390009531
インターナショナル・ビジネス・マシーンズ・コーポレーション
ＩＮＴＥＲＮＡＴＩＯＮＡＬ　ＢＵＳＩＮＥＳＳ　ＭＡＣＨＩＮＥＳ　ＣＯＲＰＯＲＡＴＩＯＮ
アメリカ合衆国１０５０４　ニューヨーク州　アーモンク　ニュー　オーチャード　ロード
Ｎｅｗ　Ｏｒｃｈａｒｄ　Ｒｏａｄ，　Ａｒｍｏｎｋ，　Ｎｅｗ　Ｙｏｒｋ　１０５０４，　Ｕｎｉｔｅｄ　Ｓｔａｔｅｓ　ｏｆ　Ａｍｅｒｉｃａ
(74)代理人　100112690
弁理士　太佐 種一

最終頁に続く

(54)【発明の名称】　パターンの安全な照合および識別

(57)【特許請求の範囲】
【請求項１】
第１のコンピュータ・システムが、暗号化されたクエリの実体の表現と１つまたは複数の暗号化されたギャラリーの実体の表現とを比較することであって、前記暗号化されたクエリの実体の前記表現と前記１つまたは複数の暗号化されたギャラリーの実体の前記表現との比較が、対応する比較された表現間の指標の二重に暗号化された値をもたらし、前記暗号化されたクエリの実体の前記表現が、第１の秘密鍵を使用する準同型暗号方式を用いて準同型に暗号化され、前記１つまたは複数の暗号化されたギャラリーの実体の前記表現が、第２の秘密鍵を使用する準同型暗号方式を用いて準同型に暗号化され、前記いずれの表現も復号せずに、暗号化された領域内で前記比較が実行される、前記比較することと、
前記第１のコンピュータ・システムが、前記指標の前記１つまたは複数の二重に暗号化された値のうちの選択された１つまたは複数を出力することと
を含む、方法。
【請求項２】
前記出力することが、前記指標の前記１つまたは複数の二重に暗号化された値のうちの単一の選択された１つ、および対応する単一の選択された二重に暗号化されたインデックスを出力することを含む、請求項１に記載の方法。
【請求項３】
前記第１のコンピュータ・システムが、前記値に基づいて複数の選択された二重に暗号化された値を並べ替えることと、

前記第１のコンピュータ・システムが、二重に暗号化されたしきい値Ｔを使用することと、
前記第１のコンピュータ・システムが、前記並べ替えられた複数の選択された二重に暗号化された値のうちの特定の値を、出力する前に、前記指標に基づく選択された値に変更することと
をさらに含む、請求項１に記載の方法。
【請求項４】
前記出力することが、前記並べ替えられた前記複数の選択された二重に暗号化された値のうちの特定の値およびそれらに対応する二重に暗号化されたインデックスの両方を出力することをさらに含む、
請求項３に記載の方法。
【請求項５】
前記出力することが、前記並べ替えられた複数の選択された二重に暗号化された値のうちの特定の値の一部のみを出力することをさらに含む、請求項３に記載の方法。
【請求項６】
前記第１のコンピュータ・システムが、前記値に基づいて複数の選択された二重に暗号化された値を並べ替えることをさらに含み、
前記出力することが、前記並べ替えられた複数の選択された二重に暗号化された値のサブセットを出力することを含む、
請求項１に記載の方法。
【請求項７】
前記出力することが、前記複数の選択された二重に暗号化された値の前記サブセットおよびそれらに対応する二重に暗号化されたインデックスの両方を出力することをさらに含む、
請求項６に記載の方法。
【請求項８】
前記第１のコンピュータ・システムが、第２のコンピュータ・システムからクエリを受信することをさらに含み、
前記クエリが、前記暗号化されたクエリの実体の前記表現を含み、
前記二重に暗号化された値のうちの前記選択された値を前記出力することが、前記第１のコンピュータ・システムから前記第２のコンピュータ・システムに向かって実行され、
前記出力することが、前記第１のコンピュータ・システムによって、第３のコンピュータ・システムに向かって、前記指標の前記１つまたは複数の二重に暗号化された値のうちの前記選択された値を出力することをさらに含む、
請求項１に記載の方法。
【請求項９】
前記比較して出力することが、前記暗号化されたクエリの実体の前記表現に対して実行される、請求項１に記載の方法。
【請求項１０】
１つまたは複数の暗号化されたギャラリーの実体の前記表現が、顔を含んでいる画像に対応する、請求項１に記載の方法。
【請求項１１】
１つまたは複数の暗号化されたギャラリーの実体の前記表現が、画像内の顔情報の特徴ベクトルに対応する、請求項１に記載の方法。
【請求項１２】
前記指標が、コサイン距離に基づく距離指標を含む、請求項１に記載の方法。
【請求項１３】
前記指標が類似性指標を含む、請求項１に記載の方法。
【請求項１４】
第１のコンピュータ・システムによって、暗号化されたクエリの実体の表現を含んでいるクエリを第２のコンピュータ・システムに送信することであって、前記暗号化されたク

エリの実体の前記表現が、第１の秘密鍵を使用する第１の準同型暗号方式を使用して準同型に暗号化される、前記送信することと、
前記第１のコンピュータ・システムで、前記第２のコンピュータ・システムから、１つまたは複数の暗号化されたギャラリーの実体の表現を前記暗号化されたクエリの実体の前記表現と比較するために前記第２のコンピュータ・システムによって使用される指標の値を示す１つまたは複数の二重に暗号化された値を受信することであって、前記１つまたは複数の二重に暗号化された値が、前記第１の準同型暗号方式および第２の秘密鍵を使用する第２の準同型暗号方式の両方を使用して暗号化される、前記受信することと、
前記第１のコンピュータ・システムによって、前記１つまたは複数の二重に暗号化された値を復号し、前記第１の準同型暗号方式で復号される対応する１つまたは複数の第１の部分的に復号された値を作成することと、
前記第１のコンピュータ・システムで、第３のコンピュータ・システムから１つまたは複数の第２の部分的に復号された値を受信することであって、前記１つまたは複数の第２の部分的に復号された値が、前記二重に暗号化された値の個別の値に対応するが、前記第２の準同型暗号方式で復号される、前記受信することと、
前記第１のコンピュータ・システムによって、対応する第１および第２の部分的に復号された値の個別の値に対してマージを実行して、平文の値を形成することであって、前記平文の値が、前記指標に対応する値を提供し、暗号化されたギャラリーの実体の対応する表現が前記暗号化されたクエリの実体の表現とどの程度良く一致すると見なされるかを示す、前記形成することと
を含む、方法。
【請求項１５】
前記第１のコンピュータ・システムによって、前記第２のコンピュータ・システムに向かって、前記第１の準同型暗号方式に対応する公開鍵を送信することをさらに含む、請求項１４に記載の方法。
【請求項１６】
前記第１のコンピュータ・システムで１つまたは複数の二重に暗号化された値を前記受信することが、前記第１のコンピュータ・システムで前記二重に暗号化された値およびそれらに対応する二重に暗号化されたインデックスを受信することをさらに含む、請求項１４に記載の方法。
【請求項１７】
前記指標に基づいて、前記平文の値のうちの特定の１つを、前記暗号化されたクエリの実体の前記表現との一致であると見なすことであって、前記クエリの実体の前記表現がギャラリーの実体の暗号化されたバージョンに対応する、前記一致であると見なすことと、
前記第１の準同型暗号方式を使用して、前記特定の平文の値に対応する二重に暗号化されたインデックスを復号し、第１の部分的に復号されたインデックスを作成することと、
前記第１のコンピュータ・システムから、前記第３のコンピュータ・システムに向かって、前記第１の部分的に復号されたインデックスおよび前記第１の部分的に復号されたインデックスに対応する平文のギャラリーの実体に対する要求を送信することと
をさらに含む、請求項１６に記載の方法。
【請求項１８】
前記第１のコンピュータ・システムで、前記第３のコンピュータ・システムから、平文インデックスに対応する平文のギャラリーの実体を受信することと、前記ギャラリーの実体が前記平文のギャラリーの実体に対応するかどうかを判定することとをさらに含む、請求項１７に記載の方法。
【請求項１９】
第１のコンピュータ・システムが、第２のコンピュータ・システムから、１つまたは複数の暗号化されたギャラリーの実体の表現を暗号化されたクエリの実体の表現と比較するために前記第２のコンピュータ・システムによって使用される指標の値を示す１つまたは複数の二重に暗号化された値を受信することであって、前記１つまたは複数の二重に暗号

化された値が、第１の秘密鍵を使用する第１の準同型暗号方式および第２の秘密鍵を使用する第２の準同型暗号方式の両方を使用して暗号化される、前記受信することと、
前記第１のコンピュータ・システムが、前記１つまたは複数の二重に暗号化された値を復号し、前記第２の準同型暗号方式で復号される対応する１つまたは複数の第１の部分的に復号された値を作成することと、
前記第２の準同型暗号方式で復号される前記１つまたは複数の第１の部分的に復号された値を第３のコンピュータ・システムに出力することと
を含む、方法。
【請求項２０】
前記第１のコンピュータ・システムによって、前記第２のコンピュータ・システムに向かって、前記第２の準同型暗号方式に対応する公開鍵を送信することをさらに含む、請求項１９に記載の方法。
【請求項２１】
前記第１のコンピュータ・システムで１つまたは複数の二重に暗号化された値を前記受信することが、前記第１のコンピュータ・システムで前記１つまたは複数の二重に暗号化された値およびそれらに対応する二重に暗号化されたインデックスを受信することをさらに含む、請求項１９に記載の方法。
【請求項２２】
前記第１のコンピュータ・システムが、前記第２の準同型暗号方式を使用して、前記二重に暗号化されたインデックスのうちの選択された１つを部分的に復号し、第１の部分的に復号されたインデックスを作成することと、
前記第１のコンピュータ・システムが、前記第３のコンピュータ・システムから、前記第１の準同型暗号方式を使用して部分的に復号された、前記第１の部分的に復号されたインデックスに対応する第２の部分的に復号されたインデックスを受信することと、
前記第１および第２の部分的に復号されたインデックスをマージして平文インデックスを形成することと
をさらに含む、請求項２１に記載の方法。
【請求項２３】
前記第１のコンピュータ・システムが、前記第３のコンピュータ・システムから、前記平文インデックスに対応する平文のギャラリーの実体に対する要求を受信することと、前記要求に応答して、前記平文のギャラリーの実体を前記第１のコンピュータ・システムから前記第３のコンピュータ・システムに送信することとをさらに含む、請求項２２に記載の方法。
【請求項２４】
コンピュータ・プログラムであって、請求項１ないし２３のいずれか１項に記載の方法の各ステップをコンピュータに実行させるための、コンピュータ・プログラム。
【請求項２５】
コンピュータ・プログラムを記録したコンピュータ可読ストレージ媒体であって、前記コンピュータ・プログラムは、請求項１ないし２３のいずれか１項に記載の方法の各ステップをコンピュータに実行させるための前記コンピュータ・プログラムである、コンピュータ可読ストレージ媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、一般に、パターンの照合および暗号化に関連しており、より詳細には、パターンの安全な照合および識別に関連している。
【背景技術】
【０００２】
企業が、規模を拡大してトランザクションを効率的に処理するために、データをクラウドに移行するにつれて、データの機密性およびセキュリティに関連する懸念および規制が

増大している。特に、暗号化されていないデータをクラウドに配置することは、他の人が許可されずにデータにアクセスすることを可能にすることがある。一方、適切な鍵なしでは、クラウドで情報をホストしているサービス・プロバイダが、暗号化データに何が含まれているかを決定する能力を有するため、データを暗号化すること自体が課題をもたらす。言い換えると、企業が暗号化データ内の情報を検索したい場合、企業が適切な鍵をサービス・プロバイダに与えない限り（それによって、セキュリティを低下させない限り）、企業はこの検索自体を実行する必要があるであろう。

【発明の概要】

【０００３】

実施形態例では、方法が、暗号化されたクエリの実体の表現と１つまたは複数の暗号化されたギャラリーの実体の表現を比較することを含む。暗号化されたクエリの実体の表現と１つまたは複数の暗号化されたギャラリーの実体の表現の比較は、対応する比較された表現間の指標の二重に暗号化された値をもたらす。暗号化されたクエリの実体の表現が、第１の秘密鍵を使用して準同型に暗号化され、１つまたは複数の暗号化されたギャラリーの実体の表現が、第２の秘密鍵を使用して準同型に暗号化され、これらの表現を復号せずに、暗号化された領域内で比較が実行される。この方法は、指標の１つまたは複数の二重に暗号化された値のうちの選択された１つまたは複数を出力することも含む。

【０００４】

追加の実施形態例は、コンピュータ・システムである。コンピュータ・システムは、１つまたは複数のプロセッサと、コンピュータ・プログラム・コードを含んでいる１つまたは複数のメモリとを含む。１つまたは複数のメモリおよびコンピュータ・プログラム・コードは、１つまたは複数のプロセッサと共に、コンピュータ・システムに、暗号化されたクエリの実体の表現と１つまたは複数の暗号化されたギャラリーの実体の表現を比較することであって、暗号化されたクエリの実体の表現と１つまたは複数の暗号化されたギャラリーの実体の表現の比較が、対応する比較された表現間の指標の二重に暗号化された値をもたらし、暗号化されたクエリの実体の表現が、第１の秘密鍵を使用して準同型に暗号化され、１つまたは複数の暗号化されたギャラリーの実体の表現が、第２の秘密鍵を使用して準同型に暗号化され、これらの表現を復号せずに、暗号化された領域内で比較が実行される、比較することと、指標の１つまたは複数の二重に暗号化された値のうちの選択された１つまたは複数を出力することとを含む動作を実行させるように構成される。

【０００５】

さらなる実施形態は、プログラム命令が具現化されているコンピュータ可読ストレージ媒体を備えているコンピュータ・プログラム製品である。プログラム命令は、コンピュータ・システムによって実行可能であり、コンピュータ・システムに、暗号化されたクエリの実体の表現と１つまたは複数の暗号化されたギャラリーの実体の表現を比較することであって、暗号化されたクエリの実体の表現と１つまたは複数の暗号化されたギャラリーの実体の表現の比較が、対応する比較された表現間の指標の二重に暗号化された値をもたらし、暗号化されたクエリの実体の表現が、第１の秘密鍵を使用して準同型に暗号化され、１つまたは複数の暗号化されたギャラリーの実体の表現が、第２の秘密鍵を使用して準同型に暗号化され、これらの表現を復号せずに、暗号化された領域内で比較が実行される、比較することと、指標の１つまたは複数の二重に暗号化された値のうちの選択された１つまたは複数を出力することとを含む動作を実行させる。

【０００６】

別の実施形態例は方法である。この方法は、第１のコンピュータ・システムによって、暗号化されたクエリの実体の表現を含んでいるクエリを第２のコンピュータ・システムに送信することを含み、暗号化されたクエリの実体の表現が、第１の秘密鍵を使用する第１の準同型暗号方式を使用して準同型に暗号化される。この方法は、第１のコンピュータ・システムで、第２のコンピュータ・システムから、１つまたは複数の暗号化されたギャラリーの実体の表現を暗号化されたクエリの実体の表現と比較するために第２のコンピュータ・システムによって使用される指標の値を示す１つまたは複数の二重に暗号化された値

を受信することを含み、１つまたは複数の二重に暗号化された値が、第１の準同型暗号方式および第２の秘密鍵を使用する第２の準同型暗号方式の両方を使用して暗号化される。この方法は、第１のコンピュータ・システムによって、１つまたは複数の二重に暗号化された値を復号し、第１の準同型暗号方式で復号される対応する１つまたは複数の第１の部分的に復号された値を作成することをさらに含む。この方法は、第１のコンピュータ・システムで、第３のコンピュータ・システムから１つまたは複数の第２の部分的に復号された値を受信することも含み、１つまたは複数の第２の部分的に復号された値は、二重に暗号化された値の個別の値に対応するが、第２の準同型暗号方式で復号される。この方法は、第１のコンピュータ・システムによって、対応する第１および第２の部分的に復号された値の個別の値に対してマージを実行し、平文（plain text）の値を形成することをさらに含み、平文の値は、指標に対応する値を提供し、暗号化されたギャラリーの実体の対応する表現が暗号化されたクエリの実体の表現とどの程度良く一致すると見なされるかを示す。

【０００７】

さらなる実施形態例は、１つまたは複数のプロセッサと、コンピュータ・プログラム・コードを含んでいる１つまたは複数のメモリとを含む例示的な装置である。１つまたは複数のメモリおよびコンピュータ・プログラム・コードは、１つまたは複数のプロセッサと共に、装置に、第１のコンピュータ・システムによって、暗号化されたクエリの実体の表現を含んでいるクエリを第２のコンピュータ・システムに送信することであって、暗号化されたクエリの実体の表現が、第１の秘密鍵を使用する第１の準同型暗号方式を使用して準同型に暗号化される、送信することと、第１のコンピュータ・システムで、第２のコンピュータ・システムから、１つまたは複数の暗号化されたギャラリーの実体の表現を暗号化されたクエリの実体の表現と比較するために第２のコンピュータ・システムによって使用される指標の値を示す１つまたは複数の二重に暗号化された値を受信することであって、１つまたは複数の二重に暗号化された値が、第１の準同型暗号方式および第２の秘密鍵を使用する第２の準同型暗号方式の両方を使用して暗号化される、受信することと、第１のコンピュータ・システムによって、１つまたは複数の二重に暗号化された値を復号し、第１の準同型暗号方式で復号される対応する１つまたは複数の第１の部分的に復号された値を作成することと、第１のコンピュータ・システムで、第３のコンピュータ・システムから１つまたは複数の第２の部分的に復号された値を受信することであって、１つまたは複数の第２の部分的に復号された値が、二重に暗号化された値の個別の値に対応するが、第２の準同型暗号方式で復号される、受信することと、第１のコンピュータ・システムによって、対応する第１および第２の部分的に復号された値の個別の値に対してマージを実行し、平文の値を形成することであって、平文の値が、指標に対応する値を提供し、暗号化されたギャラリーの実体の対応する表現が暗号化されたクエリの実体の表現とどの程度良く一致すると見なされるかを示す、形成することとを含む動作を実行させるように構成される。

【０００８】

コンピュータ・プログラム製品は、追加の実施形態例である。コンピュータ・プログラム製品は、プログラム命令が具現化されているコンピュータ可読ストレージ媒体を備え、プログラム命令は、コンピュータ・システムによって実行可能であり、コンピュータ・システムに、第１のコンピュータ・システムによって、暗号化されたクエリの実体の表現を含んでいるクエリを第２のコンピュータ・システムに送信することであって、暗号化されたクエリの実体の表現が、第１の秘密鍵を使用する第１の準同型暗号方式を使用して準同型に暗号化される、送信することと、第１のコンピュータ・システムで、第２のコンピュータ・システムから、１つまたは複数の暗号化されたギャラリーの実体の表現を暗号化されたクエリの実体の表現と比較するために第２のコンピュータ・システムによって使用される指標の値を示す１つまたは複数の二重に暗号化された値を受信することであって、１つまたは複数の二重に暗号化された値が、第１の準同型暗号方式および第２の秘密鍵を使用する第２の準同型暗号方式の両方を使用して暗号化される、受信することと、第１のコ

ンピュータ・システムによって、１つまたは複数の二重に暗号化された値を復号し、第１の準同型暗号方式で復号される対応する１つまたは複数の第１の部分的に復号された値を作成することと、第１のコンピュータ・システムで、第３のコンピュータ・システムから１つまたは複数の第２の部分的に復号された値を受信することであって、１つまたは複数の第２の部分的に復号された値が、二重に暗号化された値の個別の値に対応するが、第２の準同型暗号方式で復号される、受信することと、第１のコンピュータ・システムによって、対応する第１および第２の部分的に復号された値の個別の値に対してマージを実行し、平文の値を形成することであって、平文の値が、指標に対応する値を提供し、暗号化されたギャラリーの実体の対応する表現が暗号化されたクエリの実体の表現とどの程度良く一致すると見なされるかを示す、形成することとを含む動作を実行させる。

【０００９】

別の実施形態例は、第１のコンピュータ・システムで、第２のコンピュータ・システムから、１つまたは複数の暗号化されたギャラリーの実体の表現を暗号化されたクエリの実体の表現と比較するために第２のコンピュータ・システムによって使用される指標の値を示す１つまたは複数の二重に暗号化された値を受信することを含む方法である。１つまたは複数の二重に暗号化された値は、第１の秘密鍵を使用する第１の準同型暗号方式および第２の秘密鍵を使用する第２の準同型暗号方式の両方を使用して暗号化される。この方法は、第１のコンピュータ・システムによって、１つまたは複数の二重に暗号化された値を復号し、第２の準同型暗号方式で復号される対応する１つまたは複数の第１の部分的に復号された値を作成することを含む。この方法は、第２の準同型暗号方式で復号される１つまたは複数の第１の部分的に復号された値を第３のコンピュータ・システムに出力することも含む。

【００１０】

別の例示的な装置は、１つまたは複数のプロセッサと、コンピュータ・プログラム・コードを含んでいる１つまたは複数のメモリとを含む。１つまたは複数のメモリおよびコンピュータ・プログラム・コードは、１つまたは複数のプロセッサと共に、装置に、第１のコンピュータ・システムで、第２のコンピュータ・システムから、１つまたは複数の暗号化されたギャラリーの実体の表現を暗号化されたクエリの実体の表現と比較するために第２のコンピュータ・システムによって使用される指標の値を示す１つまたは複数の二重に暗号化された値を受信することであって、１つまたは複数の二重に暗号化された値が、第１の秘密鍵を使用する第１の準同型暗号方式および第２の秘密鍵を使用する第２の準同型暗号方式の両方を使用して暗号化される、受信することと、第１のコンピュータ・システムによって、１つまたは複数の二重に暗号化された値を復号し、第２の準同型暗号方式で復号される対応する１つまたは複数の第１の部分的に復号された値を作成することと、第２の準同型暗号方式で復号される１つまたは複数の第１の部分的に復号された値を第３のコンピュータ・システムに出力することとを含む動作を実行させるように構成される。

【００１１】

追加の実施形態例は、プログラム命令が具現化されているコンピュータ可読ストレージ媒体を備えているコンピュータ・プログラム製品であり、プログラム命令は、コンピュータ・システムによって実行可能であり、コンピュータ・システムに、第１のコンピュータ・システムで、第２のコンピュータ・システムから、１つまたは複数の暗号化されたギャラリーの実体の表現を暗号化されたクエリの実体の表現と比較するために第２のコンピュータ・システムによって使用される指標の値を示す１つまたは複数の二重に暗号化された値を受信することであって、１つまたは複数の二重に暗号化された値が、第１の秘密鍵を使用する第１の準同型暗号方式および第２の秘密鍵を使用する第２の準同型暗号方式の両方を使用して暗号化される、受信することと、第１のコンピュータ・システムによって、１つまたは複数の二重に暗号化された値を復号し、第２の準同型暗号方式で復号される対応する１つまたは複数の第１の部分的に復号された値を作成することと、第２の準同型暗号方式で復号される１つまたは複数の第１の部分的に復号された値を第３のコンピュータ・システムに出力することとを含む動作を実行させる。

【図面の簡単な説明】
【００１２】
【図１】顔画像のギャラリーに対するプレーンテキストでの照合および識別を示す図である。
【図２】顔画像のギャラリーに対する暗号化された領域内の照合および識別を示す図である。
【図３】実施形態例に従う、パターンの安全な照合および識別に適している例示的なシステムのブロック図である。
【図３Ａ】実施形態例に従う、パターンの安全な照合および識別に適している別の例示的なシステムのブロック図である。
【図４】実施形態例に従う、パターンの安全な照合および識別のための例示的な方法のフローチャートのブロック図である。
【図５】実施形態例に従う、照合アルゴリズムを示す図である。
【図６Ａ】準同型に暗号化された数値に対して、一致した識別情報のインデックスを見つけるために使用されるアルゴリズムの図である。
【図６Ｂ】２つの準同型に暗号化された数値の平方根を見つけるために使用されるアルゴリズムの図である。
【図６Ｃ】ｍｉｎ（ａ，ｂ）およびｍａｘ（ａ，ｂ）の値を見つけるために使用されるアルゴリズムの図である。
【図７】実施形態例が実践され得る１つの可能性のある非限定的な例示的システムのブロック図である。
【図８】実施形態例に従ってクラウド・コンピューティング環境を示す図である。
【図９】実施形態例に従って抽象モデル・レイヤを示す図である。
【発明を実施するための形態】
【００１３】
本明細書または図面あるいはその両方において見られることがある以下の略語が、次のように定義される。
【００１４】
ＦＨＥ（fully homomorphic encryption）　完全準同型暗号化
【００１５】
ＨＥ（homomorphic encryption）　準同型暗号化
【００１６】
Ｉ（index）　インデックス
【００１７】
Ｉ／Ｆ（interface）　インターフェイス
【００１８】
ＭＦＨＥ（multi-key fully homomorphic）　マルチキー完全準同型暗号化
【００１９】
ＳＭＣ（secure multi-party computation）　安全なマルチパーティ計算
【００２０】
ＳＶ（similarity value）　類似性値
【００２１】
「例示的」という単語は、本明細書では「例、事例、または実例としての役割を果たす」ことを意味するために使用される。「例示的」として本明細書に記載されたどの実施形態も、必ずしも他の実施形態よりも好ましいか、または有利であると解釈されるべきではない。この「発明を実施するための形態」において説明される実施形態のすべては、特許請求の範囲によって定義される本発明の範囲を制限するためではなく、当業者が本発明を実行または使用することができるようにするために提供された実施形態例である。
【００２２】
前述したように、例えば、規模を拡大してトランザクションを効率的に処理するために

データをクラウドに移行している企業は、データの機密性およびセキュリティに関連する増大する懸念および規制に対処する必要がある。暗号化ツールセットは、セキュリティおよび機密性の具体的な保証を提供しながら、データをクラウドに移動する１つの手段である。しかし前述したように、暗号化データをクラウドまたは同様のストレージ位置に配置することは、検索をより困難にする。以下で示される技術は、実施形態例において、エンドツーエンドの暗号化された解決策を、クラウド上またはその他の適切な位置で特定の「照合」アプリケーションに提供する。

【００２３】

例えば、企業がやりたいことは、プレーンテキスト（暗号化されていない情報）での照合および識別を実行することであることがある。以下を含む「識別」と呼ばれるアプリケーションの役立つクラスについて考える。

【００２４】

（１）ギャラリーと総称される１つまたは複数の実体の事前に入力された表現。

【００２５】

（２）新しい実体表現（クエリまたはプローブと呼ばれる）を前提として、システムは、ギャラリーの実体のうちのどれが最もクエリの実体に「類似している」かを評価する必要がある。

【００２６】

（３）この評価は、クエリの実体が、「一致」が検出されたことを決定するのに十分なほどギャラリーの実体に類似しているかどうかを含む。

【００２７】

（４）表現は、構造化されている（例えば、「名前」、ｓｓ＃）か、または構造化されていない（例えば、画像）とすることができる。

【００２８】

アプリケーションの例としては、顔認識、ナンバー・プレート認識などが挙げられる。図１は、顔認識に関して、顔画像のギャラリーに対するプレーンテキストでの照合および識別を示している。この例では、データベース１１０はクラウド上にあってよく、ギャラリー１１５は多くの顔の画像を含んでおり、そのうちの画像１～１８が示されている。企業は、クエリ１３０（プローブとも呼ばれる）を、照合要求１２０（「一致」として示されている）と共に、対応する画像１２５で終了する。例えば、従業員情報にアクセスすることが有効化されたフェイシャル・セキュリティ（facial security）が存在することがあり、企業は、この従業員が従業員情報にアクセスできることを検証する必要がある。

【００２９】

実行される評価は、次の方程式を使用する。

【００３０】

$$s(q, g_i) > T \qquad (1)$$

【００３１】

ここで、

【００３２】

ｑ：クエリの実体の表現、

【００３３】

g_i：ｉ番目のギャラリーの実体の表現、

【００３４】

ｓ：類似性関数、および

【００３５】

Ｔ：しきい値、である。

【００３６】

この例では、上の方程式（１）に従って、類似性関数ｓ（・）に基づいて５番目の画像（画像５）が入力画像１２５に一致するため、参照番号１４０および$s(q, g_5) > T$（参照番号１４５を参照）によって示されているように、結果は「はい」（すなわち、一

致が存在する）である。参照番号１５０によって示されているように、場合によっては他の構造化された情報（例えば、従業員が従業員情報に対するアクセス権限を持っているかどうかを示すためのアクセス・レベル）と共に、画像５が出力される。

【００３７】

これは、企業に恩恵をもたらすが、多くの個人データ（この例では、特に従業員の画像）が、企業の制御範囲を越えるということも意味する。実際に、顔画像の例に関して、顔認識に関する機密性の懸念が最近存在している。１つの懸念は、特定の政府機関がデータベースを顔認識検索に使用していることが発覚したことを示す報告を含む。具体的には、政府組織は、運転者の免許証の写真を使用していた。しかし企業が、顔画像を、誰かによってアクセスされ得るクラウドまたはその他の位置に平文として置いた場合、企業は、同様の機密性問題の危険を冒すことになる。

【００３８】

さらに、機密性に対処し、規制の不順守に対して罰金を科すか、またはその他の処置を取るための多くの規制が開始された。例えば、ＥＵ（European Union）一般データ保護規則（ＧＤＰＲ：General Data Protection Regulation）が、２０１８年５月２５日の時点で発効しており、不順守に対して年収の４％までの重い罰金を組織に科す。多くの企業は、規制された業界内で営業し、機密データを扱っており、著しいコストを事業に加えている。

【００３９】

このような懸念を踏まえて、データを暗号化し、暗号化されたデータに対して検索を実行することが可能である。図２は、暗号化された領域内の照合および識別を示している。図１に対して、図２における照合は、ギャラリーの実体およびクエリの実体が暗号化され、結果が、復号される必要がある暗号化された形式で使用可能であるということを除いて、暗号化されていない照合に類似している。

【００４０】

これが図２に示されており、プレーンテキストである（すなわち、暗号化されていない）ギャラリー１１５が暗号化され（２６０）、データベース１１０－１内で暗号化されたギャラリー２１５になる。暗号化動作２６０のための暗号化関数がＥ（g_i，K_g）として示されており、Ｅ（・）は暗号化関数であり、g_iはｉ番目のギャラリーの実体の表現であり、K_gは、ギャラリーに使用され、画像を暗号化するために暗号化関数によって使用される鍵である。暗号化されたギャラリー２１５は、暗号化された画像１－１～１８－１を含んでおり、これらの画像の各々は、対応する平文画像１～１８の暗号化されたバージョンである。

【００４１】

企業は、このシステムを使用して入力画像１２５を暗号化し（２５５）、暗号化された入力画像１２５－１を作成する。照合要求１２０－１は、Ｅ（ｑ，K_q）として表された暗号化されたクエリ（プローブとも呼ばれる）１３０－１を含んでおり、Ｅ（・）は暗号化関数であり、ｑは（例えば、暗号化された入力画像１２５－１を含んでいる）クエリの実体の表現であり、K_qは、クエリに使用され、クエリｑを暗号化されたクエリ１３０－１に暗号化するために暗号化関数によって使用される鍵である。

【００４２】

結果は、企業に返される暗号化された画像２７０である。次の方程式を使用して結果が作成される。

【００４３】

$$E(s(q, g_i), K_g, K_q) > E(T, K_g, K_q) \quad (2)$$

【００４４】

ここで、

【００４５】

ｑ：クエリの実体の表現、

【００４６】

g_i：ｉ番目のギャラリーの実体の表現、
【００４７】
ｓ：類似性関数、
【００４８】
Ｔ：しきい値、
【００４９】
Ｅ（・）：暗号化関数
【００５０】
K_g：ギャラリーを暗号化するために使用される鍵、および
【００５１】
K_q：クエリを暗号化するために使用される鍵、である。
【００５２】
この例では、上の方程式（２）に従って、類似性関数ｓ（・）に基づいて、暗号化された５番目の画像（画像５）５－１が暗号化された入力画像１２５－１に一致するため、結果はＥ（ｓ（ｑ，g_5），K_g，K_q）である。企業は、鍵K_qを使用して結果２７０を復号し（２６５）、参照番号１５０によって示されているように画像５を取得することになる。
【００５３】
ここで、次の２つの競合する利益が存在する。一方で、企業は、図２の暗号化を使用することなどによって、データおよび特にプライベート・データに対するアクセス権限を制御する必要があり、他方で、一部の政府機関またはその他の機関は、そのようなデータを要求する正当な理由を持つことができる。したがって、１つの問題は、企業（データを所有している機関）が、認可を実施するため、（規制との）適合性を判断するため、またはその他の正当な理由のためなどの、正当な理由のための照会を行うことを機関（照会している機関）に対してまだ許可しながら、データを制御する必要があるということである。
【００５４】
本明細書における実施形態例は、暗号化データを格納している、データを所有している機関から、サービス・プロバイダを介して、例えばデータを要求する正当な理由を持っている、照会している機関が暗号化データを要求できるフレームワークを提供することによって、これらの問題に対処する。図３は、実施形態例に従う、パターンの安全な照合および識別に適している例示的なシステムを示している。このフレームワークは、照会している機関３１０が、クエリ・データ３０５に関して、サービス・プロバイダ３２０に対して照合を要求することを許可する。照会している機関３１０は、サービス・プロバイダ３２０がクエリ・データ３０５に類似するデータまたは同じデータを持っている可能性が高いかどうかを示す結果（類似性値３９０）を取得する。データを所有している機関３３０の承認を得た上で、追加の検証３７０が実行されてよい。このことが、以下でさらに詳細に説明される。
【００５５】
一例として、前述したように、照会している機関は、このフレームワーク３００において、認可を実施するため、（例えば、規制との）適合性を判断するため、またはその他の正当な理由のためなどの、正当な理由のための照会を行うことを許可される。１つの例として、照会している機関３１０は、連邦捜査局（ＦＢＩ：Federal Bureau of Investigation）であることがあり、一方、データを所有している機関は、連邦政府の別の部分であることができる。ＦＢＩは、ＦＢＩが撮影したある人物の写真が、指名手配されている人物であるかどうかを知る必要があることがある。ＦＢＩは、この制限された照会を使用して、写真の人物が本当に指名手配されている人物であるかどうか判断することができる。ブロック３７０の検証が合格する（例えば、顔画像が類似している）か、または不合格になる（例えば、異なる人の顔画像であるなど、顔画像が類似していない）可能性があるということに注意する。
【００５６】

サービス・プロバイダ３２０が、特定の組織からのクエリを許可するか、またはある期間のみにわたって非常に多くのクエリを許可するか、あるいはその他の制限を照会している機関に課してよいということに注意する。データを所有している機関３３０は、環境に応じて承認を提供してもよく、または裁判所が、これらのクエリに対する承認を提供することができる。制限および承認は、本開示の範囲外である。代わりに、本開示は、暗号化されたデータに対して発生するそのような（通常は制限された）クエリのためのフレームワーク３００を提供する。

【００５７】

追加の詳細では、照会している機関３１０、クラウド上に存在してよいサービス・プロバイダ３２０、およびデータを所有している機関３３０という、３つの実体がフレームワークに含まれている。照会している機関３１０は、暗号化プロセス３０８、復号プロセス３３０、およびマージ・プロセス３５０を含んでおり、検証プロセス３７０を含んでよい。サービス・プロバイダ３２０は、照合プロセス３１５を含んでいる。データを所有している機関３３０は、暗号化プロセス３２１、復号プロセス３４０、およびマージ・プロセス３６０を含んでいる。データを所有している機関３３０は、サービス・プロバイダ３２０と共に、配置されたデータを所有している。照会している機関３１０は、クエリ・データ３０５が（例えば、暗号化された）データベース３８９内に含まれているかどうかを判定したいと考えるであろう。

【００５８】

図３の実体によって行われる動作は、図４も含んでいる例によって最も良く説明され、図４は、実施形態例に従う、パターンの安全な照合および識別のための例示的な方法のフローチャートのブロック図である。以下の説明では図３および４を参照し、３ＸＸ（「Ｘ」は任意の整数である）の参照番号は図３（または図３Ａ）上にあり、４ＸＸの参照番号は図４上にある。

【００５９】

図３および４などの本技術は、マルチキー完全準同型暗号化（ＭＦＨＥ）の技術を活用し、暗号化された領域内のパターン照合を可能にすると言うことに注意する。これらのマルチキー技術については、特に、Adriana Lopez-Alt, Eran Tromer, and Vinod Vaikuntanathan, “On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption”, Proceedings of the Forty-Fourth Annual ACM Symposium on Theory of Computing, ACM, 2012を参照されたい。

【００６０】

ブロック４１０で、データを所有している機関３３０は、暗号化プロセス３２１によって、秘密鍵Ｋｇ３２６を使用する完全準同型技術を使用してデータ（例えば、ギャラリー）の実体（例えば、ギャラリー・データ３２２）の表現を暗号化する。完全準同型モードで実行されることができるものは何でも、やや準同型のモードで実行されることもできるが、この逆は真ではないことがあるということに注意するべきである。データを所有している機関３３０は、結果として得られた暗号化ギャラリー・データ３１６をサービス・プロバイダ３２０に送信する。データを所有している機関３３０は、公開鍵３０２もサービス・プロバイダ３２０に送信する。完全準同型技術は、秘密鍵Ｋｇ３２６および公開鍵３０２の両方を作成する。本明細書では、顔の画像のギャラリーが主な例として使用されるが、これらの技術がこの例に限定されないということに注意する。さらに、「ギャラリー」という用語は、データベース内の物体またはその他の実体の集合を包含してよい。

【００６１】

表現が、（画像のギャラリーの場合は）ギャラリー内の画像の暗号化データであってよいということにさらに注意する。しかし、表現は、顔情報の特徴ベクトルの暗号化データである可能性がより高く、その場合、より良い比較を可能にすることができる。表現は、そのような特徴ベクトルとして（暗号化ギャラリー・データ３１６として）受信されてよいが、暗号化ギャラリー・データ３１６を画像として受信し、これらを準同型演算を使用して特徴ベクトルに変換することが可能であってよい。すなわち、ギャラリー・データ３

１６が暗号化される。暗号化された画像を前提として、準同型に入力された画像またはテキストから特徴ベクトルが作成されることができるように、準同型の領域内で暗号化された特徴ベクトルを計算することが可能である。次に、特徴ベクトルは、対応する画像と共に、例えば、対応する画像のメタデータとして、暗号化されたギャラリー３１７に格納されることができる。同様に、暗号化クエリ・データ３１２も、暗号化された画像または画像の暗号化された特徴ベクトルであることができる。

【００６２】

サービス・プロバイダ３２０は、暗号化ギャラリー・データ３１６をデータベース３８９内の暗号化されたギャラリー３１７に入れる。図２を参照すると、暗号化されたギャラリー３１７は、暗号化されたギャラリー２１５であると考えることができ、データベース３８９は、データベース１１０－１であると考えることができる。暗号化データは基本的に、パターンを形成する一連のバイナリ・データであるため、暗号化されたギャラリー３１７内の暗号化ギャラリー・データ３１６は、パターンであると考えることができ、その場合、下で説明されているように、他のパターンと比較されることができる。

【００６３】

図４のブロック４２０で、照会している機関３１０は、暗号化プロセス３０８によって、鍵K_q３２５を使用する完全準同型技術を使用してクエリの実体（例えば、クエリ・データ３０５）の表現を暗号化する。図５に示されているように、複数のクエリの実体がクエリ内に存在してよい。照会している機関３１０は、結果として得られた暗号化クエリ・データ３１２をクエリ（プローブとも呼ばれる）３１３の一部としてサービス・プロバイダ３２０に送信する。照会している機関３１０は、公開鍵３０１もサービス・プロバイダ３２０に送信する。完全準同型技術は、秘密鍵K_q３２５および公開鍵３０１の両方を作成する。

【００６４】

暗号化クエリ・データ３１２の受信に応答して、サービス・プロバイダ３２０は、照合プロセス３１５を実行する。図４で、照合プロセス３１５は、ブロック４３０および４４０の動作を含んでいる。ブロック４３０で、サービス・プロバイダは、指標（例えば、距離、コサイン距離、類似性指標）および対応するアルゴリズムを使用して比較を実行し、暗号化されたクエリ／プローブ３１３とギャラリー内の実体の暗号化された表現の各々との間の指標の値を見つけ、結果として得られる値は、K_gおよびK_qの両方によって暗号化される。使用され得る例示的なアルゴリズムが図６Ａ、６Ｂ、および６Ｃに示されている。サービス・プロバイダ３２０は、秘密鍵K_gおよびK_qにアクセスせずに、距離計算を実行することに加えて、計算された距離をしきい値と比較することができるということに注意する。さらに詳細には、ＳＰ（サービス・プロバイダ：service provider）３２０は、鍵K_gに従って暗号化されたギャラリー・データ３１６を含み、K_qに従って暗号化されたクエリ・データ３１２を含む。異なる鍵を使用して距離計算などの計算への２つの入力が暗号化される場合、出力距離は、両方の鍵によって暗号化される。この特性を実現するための１つの選択肢は、Hao Chen et al., “Efficient Multi-Key Homomorphic Encryption with Packed Ciphertexts with Application to Oblivious Neural Network Inference”, The 26th ACM Conference on Computer and Communications Security (CCS 2019), DOI: 10.1145/3319535.3363207で提案されたマルチキー準同型暗号方式の方法を使用することである。さらに具体的には、上記の参考文献のセクション４で説明されているように、異なる鍵を使用して暗号化された暗号文間の任意の動作が、ＳＰ（サービス・プロバイダ）で拡張された暗号文を生成する。関係者（照会している機関およびデータを所有している機関）ごとに再線形化鍵（relinearization key）を生成するために、各関係者の公開鍵３０１および３０２が、対応する評価鍵（各関係者単独での秘密鍵の特殊な暗号化）と組み合わせられることができる。各再線形化鍵を使用する再線形化と呼ばれる複雑なプロセスを適用することによって、ＳＰによって送信された拡張された暗号文が、両関係者によってより従来的な暗号文に変換されることができる。これらの従来の暗号文は、最終的な復号された計算結果を得るために、両関係者によって

部分的に復号され、最終的にマージされることができる。

【００６５】

コサイン距離は、使用され得る１つの例示的な距離指標である。使用されている指標が、データが暗号化されていることを事実上「無視する」ということに注意する。言い換えると、指標は、暗号化されたデータに使用されるように変更される必要はない。他の「距離」指標が使用されてよいということにも注意する。ハミング距離指標などの、そのような多くの指標が存在する。しかし、代わりに、または場合によっては追加的に、さまざまな「類似性」指標および対応するアルゴリズムが使用されてよい。これらは類似しているが、異なる尺度を使用する。例えば、距離指標の場合、複数の項目間の最小距離が項目間の「最良の」一致を示し、一方、類似性指標の場合、最高の類似性指標が最良の一致を示す。多くのその他の距離尺度（例えば、ハミング、ユークリッド、マンハッタン、マハラノビスなど）または類似性尺度（例えば、相関関係）が使用されてよい。

【００６６】

ブロック４４０で、サービス・プロバイダ３２０が、どの選択された値を変更するか、ならびに照会している機関３１０およびデータを所有している機関３３０に送信するかを決定する。ブロック４３０および４４０は、下で説明される図５の実施形態例において図で説明される。

【００６７】

図４の追加の説明を進める前に、サービス・プロバイダ３２０によって実行される可能性のある例示的なプロセスについて説明することは有益である。最初に、図３で、単一の暗号化された結果３９７（l_{qg}，SV_{qg}）のみが示されたことについて検討し、下付き文字ｑｇは、秘密鍵K_q３２５およびK_g３２６（例えばまたは、それらの対応する公開鍵３０１、３０２）に対応する準同型暗号方式に従う二重の暗号化を示している。しかし、サービス・プロバイダ３２０は、代わりに、下で説明される理由のため、複数の結果３９７を生成することができる。このことが、図３Ａによっても示されており、図３Ａは、実施形態例に従う、パターンの安全な照合および識別に適している別の例示的なシステムの図３に類似するブロック図である。１つの図３のそのような複数の結果３９７－１は、Ｎ個のインデックスおよび対応するＮ個の類似性値のベクトル［（I_1，SV_1），（I_2，SV_2），．．．，（I_N，SV_N）］である。別の例は、Ｎ個のインデックスのベクトルおよび対応するＮ個の類似性値のベクトル［I_1，I_2，．．．，I_N］および［SV_1，SV_2，．．．，SV_N］を含んでいる複数の結果３９７－２である。インデックスは、対応する類似性値が、データベース３８９内などの他の類似性値から一意にアクセスされることができるようにする情報である。類似性値は、画像に対応することもできる（または特徴ベクトルに対応することもできるが、暗号化ギャラリー・データ３１６が格納される）。さらに、ブロック３３０での復号は、Ｎ個のインデックス$I_{g1...N}$およびＮ個の類似性値$SV_{g1...N}$を復号することを含んでよい。表記$I_{g1...N}$は、スペースを節約するために使用されており、（I_{g1}，I_{g2}，．．．，I_{gN}）と同等である。同様に表記$SV_{g1...N}$は、スペースを節約するために使用されており、（SV_{g1}，SV_{g2}，．．．，SV_{gN}）と同等である。類似する表記が、図３Ａの他の場所でも使用されている。例えば、復号３４０は、Ｎ個のインデックス$I_{g1...N}$およびＮ個の類似性値$SV_{q1...N}$を復号することを含んでよい。

【００６８】

次に、このプロセスに関して、サービス・プロバイダ３２０が暗号化された領域内で完全に動作するということを理解するのは重要である。したがって、サービス・プロバイダ３２０は（下で説明されているように）複数の計算を実行し、アルゴリズムを実行し、しきい値を使用することができるが、サービス・プロバイダは、これらの計算の結果を知ることがない。

【００６９】

いくつかの単純な実施例について考える。サービス・プロバイダ３２０が、照合の後に類似性値のベクトル［SV_1，SV_2，SV_3，SV_4，SV_5，SV_6］を計算すると仮

定する。ステップ４４０の決定ルール（ブロック３１１を参照）が、（二重に暗号化された）しきい値Ｔより大きい上位２つの類似性値を送信すると仮定する。サービス・プロバイダは、ｍａｘ（ＳＶ$_i$－Ｔ，０）（ｍａｘ（Ａ，Ｂ）は、ＡとＢのうちの最大値を選択する）を計算し、結果を並べ替え、最初の２つ以外のエントリを隠すことができる。決定ルール３１１は、本明細書ではＬと呼ばれる制限を使用してよい。下記の実施例１および２では、Ｌ＝２である。決定ルール３１１およびその制限Ｌは、データを所有している機関３３０、照会している機関３１０、またはサービス・プロバイダ３２０、あるいはその組み合わせによって設定されてよい。制限Ｌは、平文であるか、または実装に応じて、二重に暗号化された値であってよい。

【実施例】

【００７０】

（実施例１）

ＳＶ$_2$、ＳＶ$_4$、およびＳＶ$_5$がＴより大きいと仮定し、ＳＶ$_2$＞ＳＶ$_5$＞ＳＶ$_4$である。この場合、暗号化された類似性ベクトルは［ＳＶ$_2$，ＳＶ$_5$，０，０，０，０］であることができ、暗号化されたインデックス・ベクトルは［２，５，０，０，０，０］になることになる。これらの２つの結果は、結果３９７として照会している機関およびデータを所有している機関にそれぞれ送信される。ゼロ（「０」）が実際にゼロの二重に暗号化された表現であることに注意する。使用されている指標に基づいて、使用されている値が変化することになることにも注意する（例えば、距離値は、ゼロの代わりに「１」になってよい）。

【００７１】

（実施例２）

どの類似性値もＴより大きくないと仮定する。この場合、暗号化された類似性ベクトルは［０，０，０，０，０，０］になることになり、暗号化されたインデックス・ベクトルは［０，０，０，０，０，０］になることになる。これらの２つの結果（最初の２つのゼロ）は、結果３９７として照会している機関およびデータを所有している機関にそれぞれ送信される。

【００７２】

両方の実施例において、サービス・プロバイダは結果ベクトルの内容に関して全く分からないと言うことに注意する。照会している機関およびデータを所有している機関のみが、結果３９７を共同で復号することができる。

【００７３】

第１の実施例では、照会している機関３１０が上位２つの類似性値を知り、データを所有している機関３３０が上位２つの最も類似する一致のインデックスを知る。第２の実施例では、両方の機関が、十分に類似する一致がなかったことを知る。

【００７４】

これらに従って、ブロック４４０の例であるブロック４５０で、サービス・プロバイダ３２０は、二重に暗号化されたしきい値Ｔを使用して、どの暗号化されたクエリの実体がそのまま送信されるか、およびどの暗号化されたクエリの実体が変更されるか（例えば、ゼロに設定されるか）を決定し、暗号化された結果３９７を照会している機関３１０およびデータを所有している機関３３０に出力する。「二重に暗号化されたしきい値」が概念であることに注意する。一部の実装では、しきい値は、両方の公開鍵を使用して明示的に暗号化され、本明細書において説明されたように使用されることができる。他の実装では、プレーンテキストのしきい値を使用することができるが、比較の結果がまだ二重に暗号化される。これは、ＦＨＥ方式の特性に起因する。

【００７５】

この例では、暗号化された結果３９７は、対応する一致したギャラリーのエントリのインデックス３１８および対応する類似性値３１９をも（例えば、データベース３８９に）含む。類似性値は、一致したギャラリーのエントリが暗号化クエリ・データ３１２に「どの程度類似するか」の指示である。例えば、使用される１つの一般的な尺度は、０（類似

しない）から１（非常に類似する）までであり、類似性値はこの範囲内になることになる。その他の範囲が使用されてもよい。Hao Chen他の参考文献（“Efficient Multi-Key Homomorphic Encryption with Packed Ciphertexts with Application to Oblivious Neural Network Inference”）も、「類似性」決定のための適切なアルゴリズムとして使用され得る例示的な予測モデルについて説明していることに注意する。

【００７６】

しかし、これらは「未加工の」類似性値ではなく、代わりに、二重に暗号化された類似性値３１９であるということに注意することは重要である。照会している機関３１０は、データを所有している機関３３０およびまた照会している機関３１０からの支援なしでは、これらの類似性値を復号することができない。さらに、サービス・プロバイダ３２０は二重に暗号化された比較結果３９７のみを見るため、サービス・プロバイダ３２０は、いずれかのギャラリーの実体がクエリに十分に類似しているかどうか分からないということを繰り返し述べることは重要である。照会している機関３１０のみが（データを所有している機関３３０および照会している機関から支援されて）、プレーンテキストの形態で比較の結果を見ることができる。そのため、選択されたギャラリーの実体を破棄するか、または維持するかの決定は、サービス・プロバイダ３２０によっては行われない。しかし、サービス・プロバイダ３２０は、アルゴリズムおよび場合によっては二重に暗号化されたしきい値Ｔ（または、決定ルール３１１と共に使用され得る、送信する結果の数として示す制限、Ｌ）を使用して、送信される結果の数を制限する。

【００７７】

したがって、すべての結果３９７が送信され得るが、暗号化された結果３９７の特定のサブセットが送信されることができる。例えば、１００万個の画像（または画像の特徴ベクトル）が暗号化されたギャラリー３１７に存在すると仮定する。これは、１００万個のエントリを含んでいる暗号化された結果３９７をもたらす可能性があり、各エントリはインデックスおよび対応する類似性値を含む。１００万個のエントリ全体を送信する代わりに、どのサブセットが送信されるかを選択するために、二重に暗号化されたしきい値Ｔが使用されてよく、場合によっては、（制限Ｌが送信される数を示す上述の実施例１および２におけるように）制限、Ｌと共に使用されてよい。これがブロック４５５によって示されており、類似性値が、使用されている指標に基づいて並べ替えられてよい。例えば、指標が類似性指標である場合、数値が大きいほどより良い。一方、指標が距離指標である場合、数値が小さいほどより良い。二重に暗号化されたしきい値Ｔは、どの値が送信されることになるかを決定するためのカットオフ・ポイントとして使用されることができる。例えば、類似性指標の場合、二重に暗号化されたしきい値Ｔを超える類似性値が送信されてよく、二重に暗号化されたしきい値Ｔ以下の値はサービス・プロバイダ３２０から照会している機関３１０に送信されず、例えばデータを所有している機関３３０にも送信されないことになる。別の実施例は、制限Ｌを使用し、どの結果が変更されるのか、または変更されないのかを決定するために二重に暗号化されたしきい値Ｔが使用されるが、どの結果を送信し、どの結果を送信しないかを決定するために、制限Ｌおよび決定ルール３１１が使用されるようにする。例えば、おそらく（制限Ｌに従って）上位１０個の結果のみが送信され、どの結果が（例えば、ゼロに）変更され、どの結果が変更されないかを決定するために、二重に暗号化されたしきい値がすべての結果に適用されることがある。

【００７８】

ブロック４３０および４４０に関して、出力リストのサイズ、しきい値、使用される距離（またはその他の指標）関数を含めて、入力および結果をパラメータ化することを想像することができる。これによって、サービス・プロバイダ３２０の動作をさらに制御することができることになる。しかし、やはり、サービス・プロバイダ３２０が暗号化された形態（しきい値、結果リスト、クエリなど）でしか情報を持っていないことに注意する。この情報は、照会している機関３１０またはデータを所有している機関３３０のいずれかのみによって（これらのうちの１つのみによって暗号化された情報の場合）、あるいは照会している機関３１０およびデータを所有している機関３３０の両方によって（二重に暗

号化されたか、または二重の暗号化から部分的に復号された情報の場合）復号されることができる。注意するべき重要な部分は、どの部分的結果も、サービス・プロバイダ３２０によって推定されることができないということである。代わりに、サービス・プロバイダ３２０は、暗号化された類似性、暗号化されたしきい値などのみを適用するが、指定されたしきい値に基づいて、いくつの結果に資格が与えられるかに関しては、全く分からない。

【００７９】

ブロック４６０で、データを所有している機関３３０および照会している機関３１０によって、二重に暗号化された結果３９７が復号される。データを所有している機関３３０によって、秘密鍵K_g３２６を使用する復号プロセス３４０を使用して、二重に暗号化された結果３９７が復号される。これによって、部分的に復号されたインデックスI_qおよび部分的に復号された類似性値SV_qを含む結果３４１を生成する。これらは、秘密鍵K_g３２６に対して復号されているが、秘密鍵K_q３２５に対しては暗号化されたままであり、これが下付き文字「ｑ」の理由である。

【００８０】

照会している機関３１０によって、秘密鍵K_q３２５を使用する復号プロセス３３０を使用して、二重に暗号化された結果３９７が復号される。これによって、部分的に復号されたインデックスI_gおよび部分的に復号された類似性値SV_gを含む結果３３１を生成する。これらは、秘密鍵K_q３２５に対して復号されているが、秘密鍵K_g３２６に対しては暗号化されたままであり、これが下付き文字「ｇ」の理由である。

【００８１】

ブロック４７０で、部分的に復号された類似性値SV_q３８５が、データを所有している機関３３０から照会している機関３１０に送信され、部分的に復号された一致したインデックスI_g３８０が、照会している機関３１０からデータを所有している機関３３０に送信される。

【００８２】

ブロック４８０で、照会している機関およびデータを所有している機関によって、単独で暗号化された結果３８０、３８５が復号される。具体的には、インデックス３７５が平文である場合、一致したギャラリーの実体のインデックス３７５を作成するために、部分的に復号された一致したインデックスI_g３８０が、データを所有している機関３３０によって復号される。同様に、類似性値が平文である場合、一致したギャラリーの実体の類似性値３９０を作成するために、部分的に復号された類似性値SV_q３８５が、照会している機関３１０によって復号される。

【００８３】

さらなる例として、クライアント（この場合、照会している機関３１０）によってそれまでに渡された複数の値は、画像に加えて応答リストの（例えば、制限Ｌおよび決定ルール３１１によって定義された）しきい値および候補リスト・サイズにおけるクライアントの選択を反映する。制限Ｌに従う候補リスト・サイズは、例えば、暗号化された結果３９７－１、３９７－２のサイズを定義する。これらは、検索のようなアプリケーションにおいても存在するであろう。しきい値および候補リスト・サイズは、応答の数を制限するためにサービス・プロバイダ３２０によって使用され、それらは照会している機関３１０にとって意味がある。例えば、照会している機関３１０は、上位５つの結果のみを含む、８０％を超える一致を有する応答に興味があることがある。別の照会している機関は、０．５を超えるしきい値および１００の候補リスト・サイズに興味があることがある。これらは、暗号化された照合に対して完全な結果が取得された後に適用される。

【００８４】

本明細書において使用されるマルチキーＦＨＥ方式では、二重に暗号化された暗号文は、２つの鍵３２５、３２６を含んでいる２つの連続する復号動作を使用して復号されることができない。代わりに、マルチキーＦＨＥで二重に暗号化された暗号文を復号する方法は、２つの鍵を個別に使用してそれらの暗号文を部分的に復号し、次に、２つの部分的に復号された結果をマージしてプレーンテキストを取得することである。そのため、マージ

・ステップ３５０、３８５が必要になる。例えば、“Distributed Decryption”, of Hao Chen, et al., “Efficient Multi-Key Homomorphic Encryption with Packed Ciphertexts with Application to Oblivious Neural Network Inference”, Cryptology ePrint Archive: Report 2019/524のセクション４．３を参照されたい。この参考文献のセクション４．３は、部分的復号およびマージの２つのアルゴリズムを使用する分散された復号の一例について説明している。類似するアルゴリズムまたは同じアルゴリズムが、本明細書における復号３３０、３４０およびマージ３５０、３６０のステップに使用されてよい。

【００８５】

この時点で、照会している機関３１０は、データベース３８９内のクエリ・データ３０５との一致が存在するということを決定し、この一致の類似性値３９０も決定することができる。類似性値３９０が一致を示さなくてよいということに注意する。例えば、類似性指標が使用される場合、０が類似しないことを示すことができ、１が類似していることを示すことができる。したがって、０．１５の値は、一致が存在しないことを示すことができ、一方、０．９５の値は、一致を示すことができる。照会している機関３１０は類似性値３９０のみを持っているが、インデックス３７５を持っていないため、インデックスに対応する実際のギャラリー・データ３１６にアクセスできないということに注意する。さらに、照会している機関３１０がインデックス３７５を持ち、暗号化されたギャラリー３１７からのそのインデックスに対応する画像にアクセスできる場合でも、その画像は（暗号化ギャラリー・データ３１６として）暗号化されている。したがって、照会している機関３１０は、顔画像に関する制限された情報のみを得る。

【００８６】

その結果、任意選択的動作として、照会している機関３１０は、データを所有している機関３３０に対して、検証のためにプレーンテキストの形態で一致したギャラリーの実体を要求することができる。ブロック４９０を参照されたい。照会している機関が、一致が存在するということを決定すると、照会している機関３１０は、引き続いてデータを所有している機関３３０（またはその他の組織）に対して、平文データを提供することを要求する可能性が高い。例えば、連邦捜査局（ＦＢＩ）が、別の連邦機関のデータベースとの一致を見つけた場合、ＦＢＩは、裁判所またはその他のプロセスを開始し、その機関から（一致した実体のみの）平文データを取得する。そのため、照会している機関３１０から追跡調査要求が来たときに、データを所有している機関３３０が正しいデータを取り出すことができるように、データを所有している機関３３０が一致のインデックス３７５を知ることは重要である。このプロセスが図３に示されており、一致したギャラリーの実体３９５が、プレーンテキストでデータを所有している機関３３０から照会している機関３１０に送信される。照会している機関３１０は、検証プロセス３７０を実行し、一致したギャラリーの実体３９５がクエリ・データ３０５に対応するということを検証する。このステップは、データを所有している機関３３０がこの動作を実行することを必要とし、このための承認方式は本開示の範囲外である。

【００８７】

ブロック３７０での追加の検証は、平文インデックスＩ３７５（または複数の平文インデックスＩ３７５）およびその平文インデックスに対応する（平文）ギャラリー・データ３９５の要求を作成するために、照会している機関３１０によって、部分的に復号された一致したインデックスI_g（またはインデックス）およびインデックス（I_g、I_q）（または対応するインデックスのセット）のマージの要求を送信することを含んでよい（図３のブロック３７１を参照）。この追加の検証は、照会している機関３１０が、「一致している」類似性値SV_x（または類似性値SV_xのセット）および対応するインデックスI_x（またはインデックスI_xのセット）を選択することを含むことができるということに注意する。一致している１つまたは複数の類似性値は、類似性指標または距離指標などの、使用されている指標の値に基づく。上述の実施例１の場合、照会している機関は、［SV_2，SV_5］の類似性値および［２，５］のインデックスというベクトルを（結果３９

７－２として）得た。照会している機関３１０は、データを所有している機関３３０に送信するために、SV_2の類似性値および２のインデックスのみを選択することができた。許可され、照会している機関３１０にとって望ましい場合、この機関は、［SV_2，SV_5］の類似性値および［２，５］のインデックスの両方をデータを所有している機関３３０に送信してよい。データを所有している機関３３０は、適切な場合、インデックス２またはインデックス２および５のいずれかに対応する平文ギャラリー・データ３２２を使用して応答することになる。

【００８８】

図３Ａも同様の概念を示しており、照会している機関３１０は、単一の指標（Ig_1）に関する要求をデータを所有している機関３３０に送信することができ、データを所有している機関３３０は、対応する平文インデックス３７５および対応するギャラリー・データ３９５を送信することができる。しかし、別の例では、照会している機関３１０は、複数のインデックス（$Ig_{1...M}$）（$Ig_{1...M}$は（Ig_1，．．．，Ig_M）およびＭ＞１を意味する）に関する要求をデータを所有している機関３３０に送信することができ、データを所有している機関３３０は、Ｍ個の対応する平文インデックス３７５およびＭ個の対応するギャラリー・データ３９５を照会している機関３１０に送信することができる。

【００８９】

暗号化ギャラリー・データ３１６が、この例では顔情報を含んでいる画像と見なされるということに注意する。本明細書では画像が仮定されるが、例えばレコードが、比較されることができるように定義された特徴を含んでいる限り、フレームワーク３００を従業員レコードなどの他のデータに適用することが可能である。実際、すぐ下で説明されるように、顔情報は通常、画像内の顔の特徴の数学的表現である特徴ベクトルを使用して比較される。したがって比較は、ベクトル間であってよく（または行列間であってもよく）、またはベクトル（または行列）として表されることができる任意のものが使用されてよい。すなわち、本技術は一般的であり、顔画像に制限されない。顔画像は一例にすぎない。

【００９０】

図５を参照すると、この図は、実施形態例に従って、照合アルゴリズムを図で示している。この図は、例えば図４のブロック４３０および４４０における動作の例である。この図は、計算が効率的に実行されることができるように、数値を圧縮する方法を示している。これらの数値を圧縮するための多くのその他の方法が存在する。同様にクエリも、さまざまな方法で圧縮されることができるが、それでも距離は単一のベクトルとして取得されることができる。したがって図５は、例にすぎず、制限ではない。図５の例では、ギャラリーの部分３１７－１が、４つの画像特徴ベクトル５２０－１～５２０－４を含んでいる。すなわち、各列は特徴ベクトルであり、１つの画像からの顔情報に対応し、ギャラリーのインデックスにも対応する。この例では、プローブ３１３が複数の画像を暗号化クエリ・データ３１２として示しており、画像特徴ベクトル５３０－１～５３０－４は、異なる４つの画像からの顔情報に対応する。

【００９１】

距離ベクトル５１０は、特徴ベクトル５２０、５３０の対ごとに作成される。すなわち、１６個の距離ベクトル５１０が存在することになる。これは、ブロック４３０の動作を示している。この動作が、ベクトル乗算またはサポートされている場合は行列乗算によって実行されることができるということに注意する。

【００９２】

２つの距離ベクトルａ５１０－１およびｂ５１０－２が示されており、２つのベクトルの内、最大値を有しているベクトルの決定が次のように行われる（参照番号５２０も参照のこと）：Ｍａｘ（ａ，ｂ）＝０．５＊（（ａ＋ｂ）＋ｓｑｒｔ（（ａ－ｂ）＾２）、ここで、

【数１】

$$Max(a,b) = \frac{(a+b)}{2} + \frac{\sqrt{(a-b)^2}}{2}$$

である。この場合、結果５３０は、距離ベクトルｂ５１０－２である。これは、最大の類似性値を見つけるための図４のブロック４４０の部分を示している。

【００９３】

例えば参照番号５２０の方程式を使用して、一致した識別情報のインデックスを見つけるために、複数のアルゴリズムが使用される。１つのそのようなアルゴリズムは、参考文献Cheon, Jung Hee, et al., “ Numerical Methodsfor Comparison on Homomorphically Encrypted Numbers ”,IACR Cryptology ePrint Archive 2019 (2019): 417で提案されているアルゴリズム６：ＭａｘＩｄｘである。図６Ａは、実施形態例に従う、一致した識別情報のインデックスを見つけるために使用されるアルゴリズムの図である。図６Ｂおよび６Ｃは、使用され得るCheonのアルゴリズムの追加の図である。図６Ｂは、２つの準同型に暗号化された数値の平方根を見つけるために使用されるアルゴリズムの図である。図６Ｃは、ｍｉｎ（ａ，ｂ）およびｍａｘ（ａ，ｂ）の値を見つけるために使用されるアルゴリズムの図であり、ｍｉｎ（・）は最小値を見つけ、ｍａｘ（・）は最大値を見つける。入力が二重に暗号化されるということを除き、これらのアルゴリズムに対して変更を行う必要はない。

【００９４】

図７を参照すると、この図は、実施形態例が実践され得る１つの可能性のある非限定的な例示的システム７００のブロック図を示している。図７では、コンピュータ・システム７１０は、有線または無線あるいはその両方のネットワーク７９７と有線または無線あるいはその両方で通信し、ネットワーク７９７を介して他のコンピュータ・システム７９０と通信する。コンピュータ・システム７１０は、１つまたは複数の有線ネットワークまたは無線ネットワーク７９７を経由してアクセス可能であることができる、クラウド７９５内に実装されることができる、などである。コンピュータ・システム７１０は、代替的または追加的にサーバであることができるが、クライアント／サーバの関係は必要とされない。

【００９５】

コンピュータ・システム７１０は、１つまたは複数のバス７２７を介して相互接続された、１つまたは複数のプロセッサ７２０、１つまたは複数のメモリ７２５、１つまたは複数のトランシーバ７３０、１つまたは複数のネットワーク（Ｎ／Ｗ：network）インターフェイス（Ｉ／Ｆ：interfaces）７４５、およびユーザ・インターフェイス回路７６５を含んでいる。１つまたは複数のトランシーバ７３０の各々は、受信器Ｒｘ７３２および送電器Ｔｘ７３３を含んでいる。１つまたは複数のバス７２７は、アドレス・バス、データ・バス、または制御バス、あるいはその組み合わせであってよく、マザーボードまたは集積回路上の一連の配線、光ファイバ、またはその他の光通信機器などの、任意の相互接続メカニズムを含んでよい。１つまたは複数のトランシーバ７３０は、１つまたは複数のアンテナ７２８に接続される（無線システムが使用される場合）。１つまたは複数のメモリ７２５は、コンピュータ・プログラム・コード７２３を含んでいる。

【００９６】

コンピュータ・システム７１０は、部品７０４－１または７４０－２あるいはその両方のうちの１つを含んでいる制御モジュール７４０を含んでいる。制御モジュール７４０は、本明細書に記載された照会している機関３１０またはサービス・プロバイダ３２０のいずれかの動作を実施するなどのために、本明細書に記載された動作を実行する。制御モジュール７４０は、複数の方法で実装されてよい。制御モジュール７４０は、１つまたは複数のプロセッサ７２０の一部として実装されるなど、ハードウェアにおいて制御モジュール７４０－１として実装されてよい。制御モジュール７４０－１は、集積回路として実装されるか、またはプログラマブル・ゲート・アレイなどのその他のハードウェアによって

実装されてもよい。別の例では、制御モジュール７４０は、コンピュータ・プログラム・コード７２３として実装され、１つまたは複数のプロセッサ７２０によって実行される、制御モジュール７４０－２として実装されてよい。例えば、１つまたは複数のメモリ７２５およびコンピュータ・プログラム・コード７２３は、１つまたは複数のプロセッサ７２０と共に、コンピュータ・プログラム・コード７２３の取得および実行に応答して、コンピュータ・システム７１０に、本明細書において説明されているような動作のうちの１つまたは複数を実行させるように、構成されてよい。コンピュータ・システム７１０に示されたデバイスは制限ではなく、追加のデバイス、異なるデバイス、またはより少ないデバイスが使用されてよいということにも、注意するべきである。

【００９７】

ユーザ・インターフェイス回路７６５は、１つまたは複数のユーザ・インターフェイス要素７０５と通信し、ユーザ・インターフェイス要素７０５は、コンピュータ・システム７１０と一体で形成されてよく、またはコンピュータ・システム７１０の外部にあり、ただしコンピュータ・システム７１０に結合されてよい。インターフェイス要素７０５は、１つまたは複数のカメラ、１つまたは複数の音声デバイス（マイクロホン、スピーカなど）、１つまたは複数のセンサ（ＧＰＳセンサ、指紋センサ、方位センサなど）、１つまたは複数のディスプレイ、または１つまたは複数のキーボード、あるいはその組み合わせのうちの１つまたは複数を含んでいる。ディスプレイ７１１が示されており、ディスプレイ７１１は、コンピュータ・システム７１０の外部または内部にあることができる。このリストは網羅的でも限定的でもなく、その他の要素、異なる要素、またはより少ない要素が使用されてよい。ユーザ７０１－１（この例では人間）は、例えば、システム７１０に特定の動作を実行させるために、コンピュータ・システム７１０と情報をやりとりしてよい。これらの動作は、ユーザ７０１－１による動作と組み合わせて、またはユーザ７０１－１による動作なしで、コンピュータ・システム７１０によって引き起こされてもよい。コンピュータ・システム７１０は、有線リンク７７７および無線リンク７７８のうちの１つまたは両方を介する１つまたは複数の有線ネットワークまたは無線ネットワーク７９７を介して、他のコンピュータ・システム７９０と通信する。さらに、コンピュータ・システム７１０がクラウド７９５内で実装される場合、ユーザ７０１－２は、コンピュータ・システム７９０を使用して、有線または無線あるいはその両方のネットワーク７９７を介して、コンピュータ・システム７１０と情報をやりとりしてよい。この例では、コンピュータ・システム７９０は、適切なユーザＩ／Ｆ回路およびユーザＩ／Ｆ要素（図示されていない）を含むであろうが、ユーザＩ／Ｆ要素７０５と同様であるであろう。

【００９８】

１つの例は、コンピュータ・システム７１０がクラウド７９５内にあり、したがって、クラウド・サービス・プロバイダ３２０である場合である。その場合、他のコンピュータ・システム７９０が照会している機関３１０およびデータを所有している機関３３０になることになる。制御モジュール７４０は、サービス・プロバイダ３２０によって実行されるとして前に説明された照合プロセス３１５およびその他の動作を実施することになる。別の例では、コンピュータ・システム７１０が、照会している機関３１０またはサービス・プロバイダ３２０のうちの１つであることになり、他のコンピュータ・システム７９０が、例えばネットワーク７９７を介してコンピュータ・システム７１０に接続されたサーバとして、サービス・プロバイダ３２０になることになる
。

【００９９】

サービス・プロバイダ３２０がクラウド３９５内で実装される場合、図８および９が、クラウドの実装に関する追加情報を提供する。図８は、実施形態例に従うクラウド・コンピューティング環境を示しており、図９は、実施形態例に従う抽象モデル・レイヤを示している。

【０１００】

ここで図８を参照すると、例示的なクラウド・コンピューティング環境５０が示されて

いる。本明細書における実施例のいずれかを実施するクラウド・コンピューティング環境５０の一部または全部は、コンピュータ・システム１１０であると考えられる。言い替えると、コンピュータ・システム１１０は、本明細書における実施例のいずれかを実施するクラウド・コンピューティング環境５０の一部であると考えられ得る。図示されているように、クラウド・コンピューティング環境５０は、クラウドの利用者によって使用されるローカル・コンピューティング・デバイス（例えば、パーソナル・デジタル・アシスタント（ＰＤＡ：personal digital assistant）または携帯電話５４Ａ、デスクトップ・コンピュータ５４Ｂ、ラップトップ・コンピュータ５４Ｃ、または自動車コンピュータ・システム５４Ｎ、あるいはその組み合わせなど）が通信できる１つまたは複数のクラウド・コンピューティング・ノード１０を含んでいる。ノード１０は、互いに通信してよい。ノード１０は、１つまたは複数のネットワーク内で、本明細書において前述されたプライベート・クラウド、コミュニティ・クラウド、パブリック・クラウド、またはハイブリッド・クラウド、あるいはこれらの組み合わせなどに、物理的または仮想的にグループ化されてよい（図示されていない）。これによって、クラウド・コンピューティング環境５０は、クラウドの利用者がローカル・コンピューティング・デバイス上でリソースを維持する必要のないインフラストラクチャ、プラットフォーム、またはＳａａＳ、あるいはその組み合わせを提供できる。図８に示されたコンピューティング・デバイス５４Ａ～Ｎの種類は、例示のみが意図されており、コンピューティング・ノード１０およびクラウド・コンピューティング環境５０は、任意の種類のネットワークまたはネットワーク・アドレス可能な接続（例えば、Ｗｅｂブラウザを使用した接続）あるいはその両方を経由して任意の種類のコンピュータ制御デバイスと通信することができると理解される。

【０１０１】

ここで図９を参照すると、クラウド・コンピューティング環境５０（図８）によって提供される機能的抽象レイヤのセットが示されている。図９に示されたコンポーネント、レイヤ、および機能は、例示のみが意図されており、本発明の実施形態がこれらに限定されないということが、あらかじめ理解されるべきである。図示されているように、次のレイヤおよび対応する機能が提供される。

【０１０２】

ハードウェアおよびソフトウェア・レイヤ６０は、ハードウェア・コンポーネントおよびソフトウェア・コンポーネントを含む。ハードウェア・コンポーネントの例としては、メインフレーム６１、ＲＩＳＣ（Reduced Instruction Set Computer）アーキテクチャベースのサーバ６２、サーバ６３、ブレード・サーバ６４、ストレージ・デバイス６５、ならびにネットワークおよびネットワーク・コンポーネント６６が挙げられる。一部の実施形態では、ソフトウェア・コンポーネントは、ネットワーク・アプリケーション・サーバ・ソフトウェア６７およびデータベース・ソフトウェア６８を含む。

【０１０３】

仮想化レイヤ７０は、仮想サーバ７１、仮想ストレージ７２、仮想プライベート・ネットワークを含む仮想ネットワーク７３、仮想アプリケーションおよびオペレーティング・システム７４、ならびに仮想クライアント７５などの仮想的実体の例を提供できる抽象レイヤを備える。

【０１０４】

一例を挙げると、管理レイヤ８０は、以下で説明される機能を提供してよい。リソース・プロビジョニング８１は、クラウド・コンピューティング環境内でタスクを実行するために利用される計算リソースおよびその他のリソースの動的調達を行う。計測および価格設定８２は、クラウド・コンピューティング環境内でリソースが利用される際のコスト追跡、およびそれらのリソースの利用に対する請求書またはインボイスの送付を行う。一例を挙げると、それらのリソースは、アプリケーション・ソフトウェア・ライセンスを含んでよい。セキュリティは、クラウドの利用者およびタスクのＩＤ検証を行うと共に、データおよびその他のリソースの保護を行う。ユーザ・ポータル８３は、クラウド・コンピューティング環境へのアクセスを利用者およびシステム管理者に提供する。サービス・レベ

ル管理８４は、必要なサービス・レベルを満たすように、クラウドの計算リソースの割り当てと管理を行う。サービス水準合意（ＳＬＡ：Service Level Agreement）計画および実行８５は、今後の要求が予想されるクラウドの計算リソースの事前準備および調達を、ＳＬＡに従って行う。

【０１０５】

ワークロード・レイヤ９０は、クラウド・コンピューティング環境で利用できる機能の例を示している。このレイヤから提供されてよいワークロードおよび機能の例としては、マッピングおよびナビゲーション９１、ソフトウェア開発およびライフサイクル管理９２、仮想クラスルーム教育の配信９３、データ解析処理９４、トランザクション処理９５、および安全な照合および識別サービス９６が挙げられる。安全な照合および識別９６は、図２～４のクラウド・サービス・プロバイダ３２０の動作を実施するなどの、本明細書において提供された実施例を実施するサービスである。

【０１０６】

本発明は、システム、方法、またはコンピュータ・プログラム製品、あるいはその組み合わせであってよい。コンピュータ・プログラム製品は、プロセッサに本発明の態様を実行させるためのコンピュータ可読プログラム命令を含んでいるコンピュータ可読ストレージ媒体を含んでよい。

【０１０７】

コンピュータ可読ストレージ媒体は、命令実行デバイスによって使用するための命令を保持および格納できる有形のデバイスであることができる。コンピュータ可読ストレージ媒体は、例えば、電子ストレージ・デバイス、磁気ストレージ・デバイス、光ストレージ・デバイス、電磁ストレージ・デバイス、半導体ストレージ・デバイス、またはこれらの任意の適切な組み合わせであってよいが、これらに限定されない。コンピュータ可読ストレージ媒体のさらに具体的な例の非網羅的リストは、ポータブル・フロッピー（Ｒ）・ディスク、ハード・ディスク、ランダム・アクセス・メモリ（ＲＡＭ：random access memory）、読み取り専用メモリ（ＲＯＭ：read-only memory）、消去可能プログラマブル読み取り専用メモリ（ＥＰＲＯＭ：erasable programmable read-only memoryまたはフラッシュ・メモリ）、スタティック・ランダム・アクセス・メモリ（ＳＲＡＭ：static random access memory）、ポータブル・コンパクト・ディスク読み取り専用メモリ（ＣＤ－ＲＯＭ：compact disc read-only memory）、デジタル・バーサタイル・ディスク（ＤＶＤ：digital versatile disk）、メモリ・スティック、フロッピー（Ｒ）・ディスク、命令が記録されているパンチカードまたは溝の中の隆起構造などの機械的にエンコードされるデバイス、およびこれらの任意の適切な組み合わせを含む。本明細書において使用されるとき、コンピュータ可読ストレージ媒体は、それ自体が、電波またはその他の自由に伝搬する電磁波、導波管またはその他の送信媒体を伝搬する電磁波（例えば、光ファイバ・ケーブルを通過する光パルス）、あるいはワイヤを介して送信される電気信号などの一過性の信号であると解釈されるべきではない。

【０１０８】

本明細書に記載されたコンピュータ可読プログラム命令は、コンピュータ可読ストレージ媒体から各コンピューティング・デバイス／処理デバイスへ、またはネットワーク（例えば、インターネット、ローカル・エリア・ネットワーク、広域ネットワーク、または無線ネットワーク、あるいはその組み合わせ）を介して外部コンピュータまたは外部ストレージ・デバイスへダウンロードされることができる。このネットワークは、銅伝送ケーブル、光伝送ファイバ、無線送信、ルータ、ファイアウォール、スイッチ、ゲートウェイ・コンピュータ、またはエッジ・サーバ、あるいはその組み合わせを備えてよい。各コンピューティング・デバイス／処理デバイス内のネットワーク・アダプタ・カードまたはネットワーク・インターフェイスは、コンピュータ可読プログラム命令をネットワークから受信し、それらのコンピュータ可読プログラム命令を各コンピューティング・デバイス／処理デバイス内のコンピュータ可読ストレージ媒体に格納するために転送する。

【０１０９】

本発明の動作を実行するためのコンピュータ可読プログラム命令は、アセンブラ命令、命令セット・アーキテクチャ（ＩＳＡ：instruction-set-architecture）命令、マシン命令、マシン依存命令、マイクロコード、ファームウェア命令、状態設定データ、あるいは、Ｓｍａｌｌｔａｌｋ（Ｒ）、Ｃ＋＋（Ｒ）などのオブジェクト指向プログラミング言語、および「Ｃ」プログラミング言語（Ｒ）または同様のプログラミング言語などの従来の手続き型プログラミング言語を含む１つまたは複数のプログラミング言語の任意の組み合わせで記述されたソース・コードまたはオブジェクト・コードのどちらかであってよい。コンピュータ可読プログラム命令は、ユーザのコンピュータ上で全体的に実行すること、ユーザのコンピュータ上でスタンドアロン・ソフトウェア・パッケージとして部分的に実行すること、ユーザのコンピュータ上およびリモート・コンピュータ上でそれぞれ部分的に実行すること、あるいはリモート・コンピュータ上またはサーバ上で全体的に実行することができる。後者のシナリオでは、リモート・コンピュータは、ローカル・エリア・ネットワーク（ＬＡＮ：local area network）または広域ネットワーク（ＷＡＮ：wide area network）を含む任意の種類のネットワークを介してユーザのコンピュータに接続されてよく、または接続は、（例えば、インターネット・サービス・プロバイダを使用してインターネットを介して）外部コンピュータに対して行われてよい。一部の実施形態では、本発明の態様を実行するために、例えばプログラマブル・ロジック回路、フィールドプログラマブル・ゲート・アレイ（ＦＰＧＡ：field-programmable gate arrays）、またはプログラマブル・ロジック・アレイ（ＰＬＡ：programmable logic arrays）を含む電子回路は、コンピュータ可読プログラム命令の状態情報を利用することによって、電子回路をカスタマイズするためのコンピュータ可読プログラム命令を実行してよい。

【０１１０】

本発明の態様は、本明細書において、本発明の実施形態に従って、方法、装置（システム）、およびコンピュータ・プログラム製品のフローチャート図またはブロック図あるいはその両方を参照して説明される。フローチャート図またはブロック図あるいはその両方の各ブロック、ならびにフローチャート図またはブロック図あるいはその両方に含まれるブロックの組み合わせが、コンピュータ可読プログラム命令によって実装され得るということが理解されるであろう。

【０１１１】

これらのコンピュータ可読プログラム命令は、コンピュータまたはその他のプログラム可能なデータ処理装置のプロセッサを介して実行される命令が、フローチャートまたはブロック図あるいはその両方のブロックに指定される機能／動作を実施する手段を作り出すべく、汎用コンピュータ、専用コンピュータ、または他のプログラム可能なデータ処理装置のプロセッサに提供されてマシンを作り出すものであってよい。これらのコンピュータ可読プログラム命令は、命令が格納されたコンピュータ可読ストレージ媒体がフローチャートまたはブロック図あるいはその両方のブロックに指定される機能／動作の態様を実施する命令を含んでいる製品を備えるように、コンピュータ可読ストレージ媒体に格納され、コンピュータ、プログラム可能なデータ処理装置、または他のデバイス、あるいはその組み合わせに特定の方式で機能するように指示できるものであってもよい。

【０１１２】

コンピュータ可読プログラム命令は、コンピュータ上、その他のプログラム可能な装置上、またはその他のデバイス上で実行される命令が、フローチャートまたはブロック図あるいはその両方のブロックに指定される機能／動作を実施するように、コンピュータ、その他のプログラム可能なデータ処理装置、またはその他のデバイスに読み込まれてもよく、それによって、一連の動作可能なステップを、コンピュータ上、その他のプログラム可能な装置上、またはコンピュータ実装プロセスを生成するその他のデバイス上で実行させる。

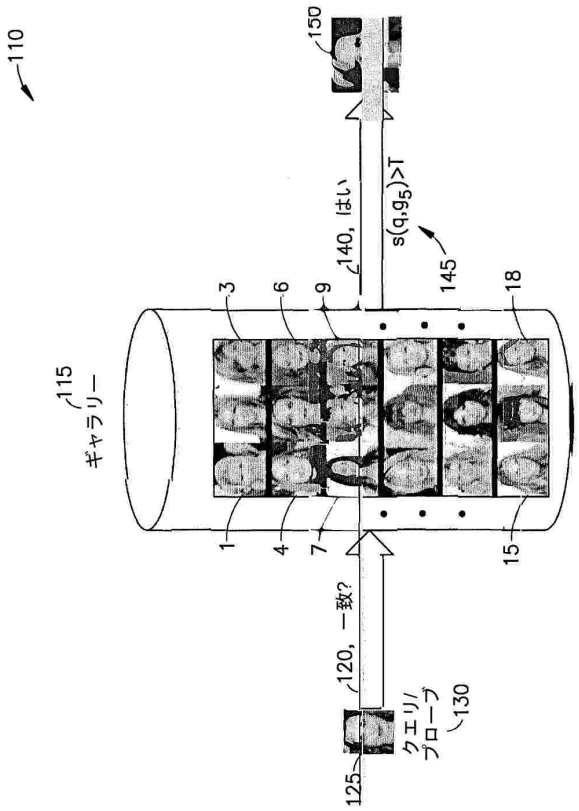
【０１１３】

図内のフローチャートおよびブロック図は、本発明のさまざまな実施形態に従って、システム、方法、およびコンピュータ・プログラム製品の可能な実装のアーキテクチャ、機能、および動作を示す。これに関連して、フローチャートまたはブロック図内の各ブロッ

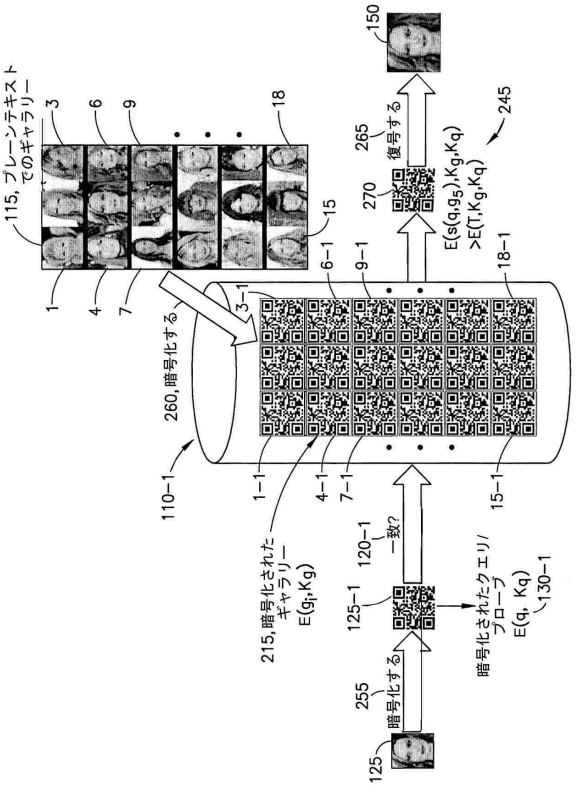
クは、規定された論理機能を実装するための１つまたは複数の実行可能な命令を備える、命令のモジュール、セグメント、または部分を表してよい。一部の代替の実装では、ブロックに示された機能は、図に示された順序とは異なる順序で発生してよい。例えば、連続して示された２つのブロックは、実際には、含まれている機能に応じて、実質的に同時に実行されるか、または場合によっては逆の順序で実行されてよい。ブロック図またはフローチャート図あるいはその両方の各ブロック、ならびにブロック図またはフローチャート図あるいはその両方に含まれるブロックの組み合わせは、規定された機能または動作を実行するか、または専用ハードウェアとコンピュータ命令の組み合わせを実行する専用ハードウェアベースのシステムによって実装され得るということにも注意されよう。

【図面】

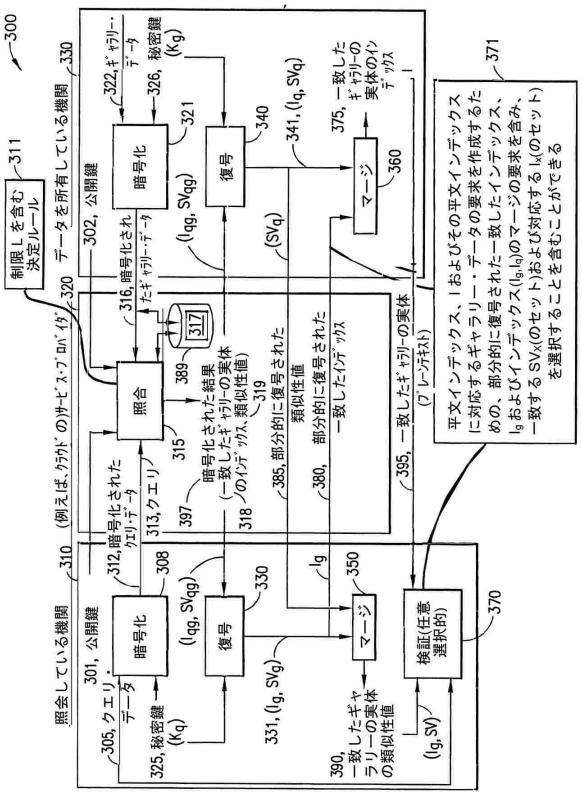
【図１】



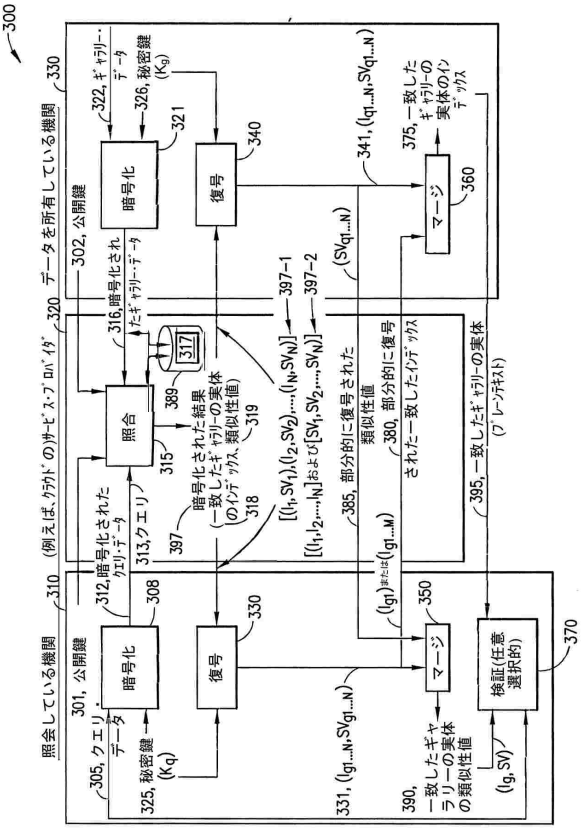
【図２】



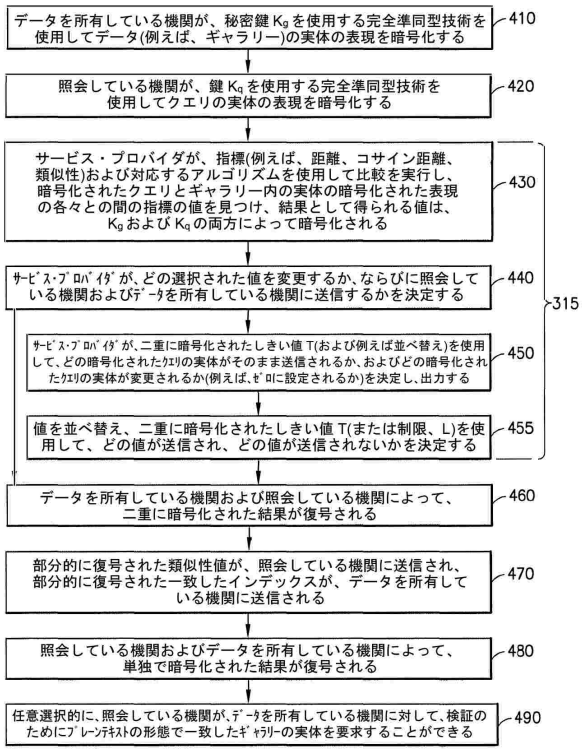
【図３】



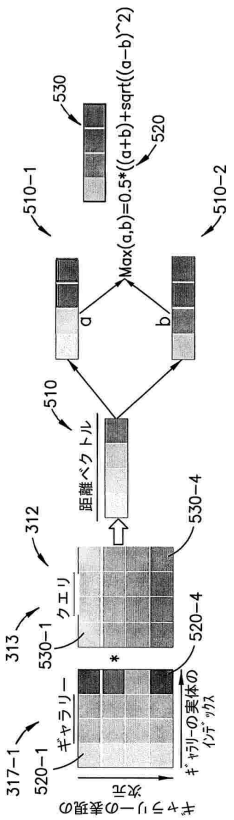
【図３Ａ】



【図４】


データを所有している機関が、秘密鍵 K_g を使用する完全準同型技術を使用してデータ(例えば、ギャラリー)の実体の表現を暗号化する
410
照会している機関が、鍵 K_q を使用する完全準同型技術を使用してクエリの実体の表現を暗号化する
420
サービス・プロバイダが、指標(例えば、距離、コサイン距離、類似性)および対応するアルゴリズムを使用して比較を実行し、暗号化されたクエリとギャラリー内の実体の暗号化された表現の各々との間の指標の値を見つけ、結果として得られる値は、K_g および K_q の両方によって暗号化される
430
ｻｰﾋﾞｽ･ﾌﾟﾛﾊﾞｲﾀﾞが、どの選択された値を変更するか、ならびに照会している機関およびﾃﾞｰﾀを所有している機関に送信するかを決定する
440
ｻｰﾋﾞｽ･ﾌﾟﾛﾊﾞｲﾀﾞが、二重に暗号化されたしきい値 T(および例えば並べ替え)を使用して、どの暗号化されたｸｴﾘの実体がそのまま送信されるか、およびどの暗号化されたｸｴﾘの実体が変更されるか(例えば、ｾﾞﾛに設定されるか)を決定し、出力する
450
値を並べ替え、二重に暗号化されたしきい値 T(または制限、L)を使用して、どの値が送信され、どの値が送信されないかを決定する
455
315
データを所有している機関および照会している機関によって、二重に暗号化された結果が復号される
460
部分的に復号された類似性値が、照会している機関に送信され、部分的に復号された一致したインデックスが、データを所有している機関に送信される
470
照会している機関およびデータを所有している機関によって、単独で暗号化された結果が復号される
480
任意選択的に、照会している機関が、ﾃﾞｰﾀを所有している機関に対して、検証のためにﾌﾟﾚｰﾝﾃｷｽﾄの形態で一致したｷﾞｬﾗﾘｰの実体を要求することができる
490

【図５】


Max(a,b)=0.5*((a+b)+sqrt((a-b)^2))
530
520
510-1
510-2
a
b
510
距離ベクトル
312
クエリ
313
530-1
530-4
520-4
*
317-1
520-1
ギャラリー
ギャラリーの実体のインデックス
ギャラリーの表現の次元

【図６Ａ】

アルゴリズム 6 MaxIdx(a;a₂,...,aₙ;d,d',m,t)

入力: $a_i \in \left[\frac{1}{2}, \frac{3}{2}\right)$ での n 個の異なる数値(a;a₂,...,aₙ)、d、d'、m、$t \in \mathbb{N}$
出力:(b;,b₂,...,bₙ)、ここで、biは、aiがaiのうちで最大である場合、1に近く、
それ以外の場合、0に近い(定理５を参照)

```
1: inv ← Inv (Σ_{j=1}^{n} a_j/n;d')
2: for j←1 to n−1 do
3:     b_j ←a_j/n·inv                    //初期の１ノルムの正規化
4: end for
5: b_n←1−Σ_{k=1}^{n−1} b_j
6: for i←1 to t do
7:     inv ← Inv (Σ_{j=1}^{n} b_j^m;d)
8:     for j←0 to n−1 do
9:         b_j ← b_j^m·inv
10:    end for
11:    b_n←1− Σ_{k=1}^{n−1} b_j
12: end for
13: return (b₁,b₂,...,bₙ)
```

【図６Ｂ】

アルゴリズム 2 Sqrt(x;d)

入力:0≦x≦1、$d \in \mathbb{N}$
出力: $\sqrt{x}$ の近似値(補助定理 2 を参照)

```
1: a_0 ← x
2: b_0 ← x − 1
3: for n ← 0 to d − 1 do
4:     a_{n+1} ← a_n (1 − b_n/2)
5:     b_{n+1} ← b_n^2 ((b_n − 3)/4)
6: end for
7: return a_d
```

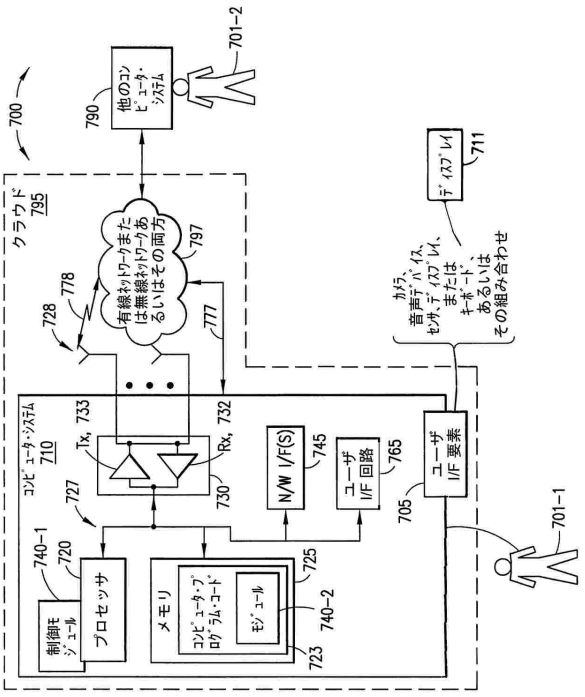
【図６Ｃ】

アルゴリズム 3 Min(a,b;d)、Max(a,b;d)

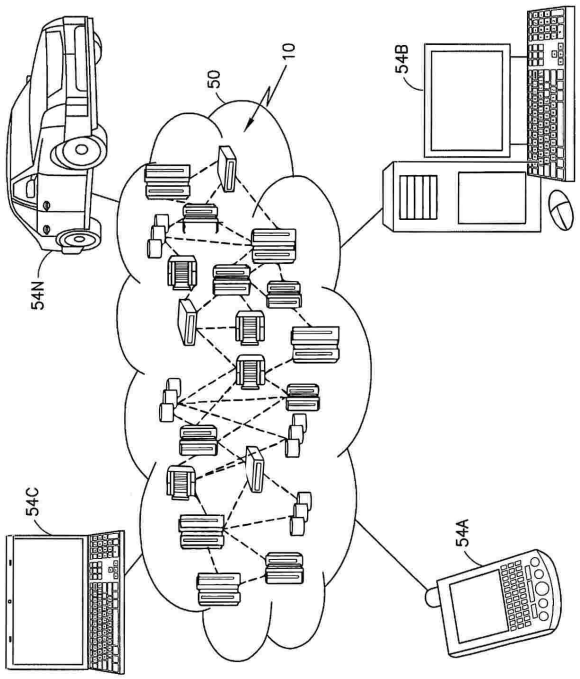
入力:a,b∈[0,1)、$d \in \mathbb{N}$
出力:min(a,b)および max(a,b)の近似値(定理 1、2 を参照)

```
1: x = (a+b)/2 および y = (a−b)/2
2: z ← Sqrt(y²;d)
3: return x−zただし Min(a,b;d)
          x+zただし Max(a,b;d)
```

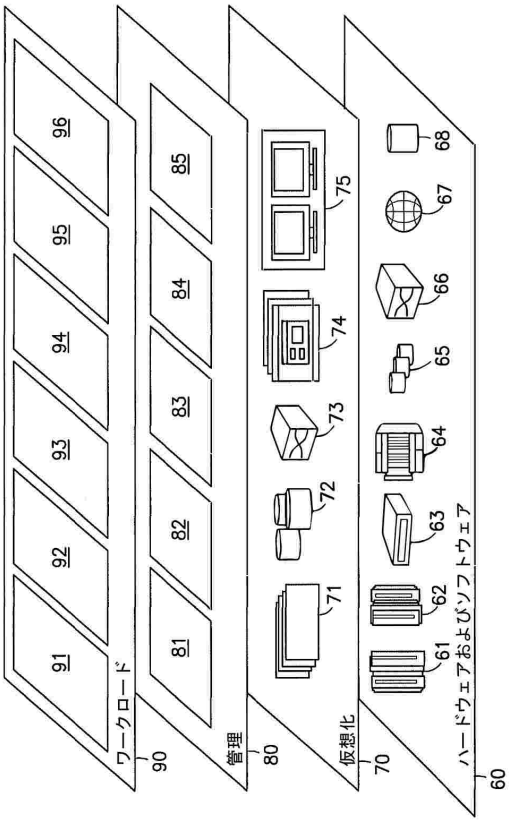
【図７】



【図８】


10
50
54A
54B
54C
54N

【図９】


91
92
93
94
95
96
ワークロード
90
81
82
83
84
85
管理
80
71
72
73
74
75
仮想化
70
61
62
63
64
65
66
67
68
ハードウェアおよびソフトウェア
60

フロントページの続き

(74)代理人　100120710
弁理士　片岡 忠彦
(72)発明者　パンカンティ、シャラートチャンドラ
アメリカ合衆国１０５９８ ニューヨーク州ヨークタウン・ハイツ キッチャワン・ロード１１０１
(72)発明者　ナンダクマール、カーシク
アメリカ合衆国１０５９８ ニューヨーク州ヨークタウン・ハイツ キッチャワン・ロード１１０１
(72)発明者　ラタ、ナリニ
アメリカ合衆国１０５９８ ニューヨーク州ヨークタウン・ハイツ キッチャワン・ロード１１０１
(72)発明者　ハレヴィ、シャイ
アメリカ合衆国１０５９８ ニューヨーク州ヨークタウン・ハイツ キッチャワン・ロード１１０１
審査官　塩澤 如正
(56)参考文献　特開２０１７－０７６８３９（ＪＰ，Ａ）
特開２０１９－１６８５９０（ＪＰ，Ａ）
中国特許出願公開第１０３７４４９７６（ＣＮ，Ａ）
Efficient Multi-Key Homomorphic Encryption with Packed Ciphertexts with Application to Oblivious Neural Network Inference，Cryptology ePrint Archive[online]，2019年09月19日，pp. 1-30，Retrieved from the Internet: 〈URL: https://eprint.iacr.org/archive/2019/524/20190919:223334〉，[2024年7月10日検索]
(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｇ０９Ｃ　１／００
Ｈ０４Ｌ　９／００－ ９／４０