

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2007-288747

(P2007-288747A)

(43) 公開日 平成19年11月1日(2007.11.1)

(51) Int. Cl. F I テーマコード (参考)
 H04L 9/08 (2006.01) H04L 9/00 G01C 5J104

審査請求 未請求 請求項の数 17 O L (全 25 頁)

(21) 出願番号	特願2006-116942 (P2006-116942)	(71) 出願人	000006747 株式会社リコー
(22) 出願日	平成18年4月20日 (2006.4.20)	(74) 代理人	100083231 弁理士 紋田 誠
		(74) 代理人	100112287 弁理士 逸見 輝雄
		(72) 発明者	熊谷 和幸 東京都大田区中馬込1丁目3番6号 株式会社リコー内
		(72) 発明者	中村 学 東京都大田区中馬込1丁目3番6号 株式会社リコー内

最終頁に続く

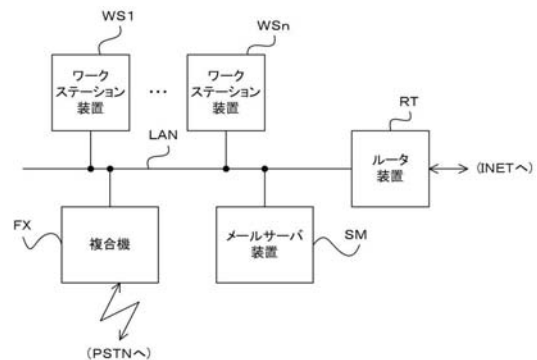
(54) 【発明の名称】 画像処理システムおよび画像処理システムの制御方法および画像形成装置および画像再生装置

(57) 【要約】 (修正有)

【課題】 容易に電子データの改ざんや情報漏えいを防ぐことが可能な画像処理システム、その制御方法、画像形成装置および画像再生装置を提供する。

【解決手段】 原稿画像を読み取り、共通鍵を生成し、暗号化画像データを生成する画像形成装置と、前記暗号化画像データと前記共通鍵を受け取り、復号化して画像データを再生する画像再生装置とからなる画像処理システムで、前記画像形成装置は、画像データの形成ごとに異なる共通鍵を生成し、暗号化画像データにより一意に決定される識別子を生成し、共通鍵に付与して復号鍵情報を形成し、交換可能記憶媒体に記憶し、前記画像再生装置は、交換可能記憶媒体に記憶された復号鍵情報を記憶し、再生指定された暗号化画像データにより一意に決定される識別子を生成し、当該生成した識別子と同一識別子を有する復号鍵情報を探し出し、当該探し出した復号鍵情報を用いて、再生指定された暗号化画像データを復号化する。

【選択図】 図1



【特許請求の範囲】**【請求項 1】**

入力した画像データに所定の暗号化方法を適用して暗号化画像データを生成するとともに、当該暗号化画像データを復号化する際に用いる復号鍵を生成する画像形成装置と、

前記暗号化画像データと前記復号鍵を受け取り、前記暗号化画像データについて前記復号鍵を用いて復号化し、それによって得た前記画像データを再生する画像再生装置とからなる画像処理システムであって、

前記画像形成装置は、前記暗号化画像データを生成するたびに異なる前記復号鍵を生成し、前記画像データを暗号化して得た前記暗号化画像データに基づいて一意に決定される識別子を生成し、前記共通鍵に前記識別子を付与して復号鍵情報を形成し、当該復号鍵情報を交換可能記憶媒体に記憶し、

前記画像再生装置は、前記交換可能記憶媒体に記憶された前記復号鍵情報を読み込んで記憶し、再生指定された前記暗号化画像データに基づいて一意に決定される識別子を生成し、当該生成した識別子に対応する復号鍵情報を用いて、前記再生指定された暗号化画像データを復号化することを特徴とする画像処理システム。

10

【請求項 2】

前記画像形成装置は、電子メールを用いて、前記画像再生装置に前記暗号化画像データを送信することを特徴とする請求項 1 記載の画像処理システム。

【請求項 3】

入力した画像データに所定の暗号化方法を適用して暗号化画像データを生成するとともに、当該暗号化画像データを復号化する際に用いる復号鍵を生成する画像形成装置と、

前記暗号化画像データと前記復号鍵を受け取り、前記暗号化画像データについて前記復号鍵を用いて復号化し、それによって得た前記画像データを再生する画像再生装置とからなる画像処理システムであって、

前記画像形成装置は、前記暗号化画像データを第 1 の交換可能記憶媒体に記憶する一方、前記暗号化画像データを生成するたびに異なる前記復号鍵を生成し、前記画像データを暗号化して得た前記暗号化画像データに基づいて一意に決定される識別子を生成し、前記共通鍵に前記識別子を付与して復号鍵情報を形成し、当該復号鍵情報を第 2 の交換可能記憶媒体に記憶し、

前記画像再生装置は、前記第 1 の交換可能記憶媒体に記憶された前記暗号化画像データ、および、前記第 2 の交換可能記憶媒体に記憶された前記復号鍵情報をそれぞれ読み込んで記憶し、再生指定された前記暗号化画像データに基づいて一意に決定される識別子を生成し、当該生成した識別子に対応する復号鍵情報を用いて、前記再生指定された暗号化画像データを復号化することを特徴とする画像処理システム。

20

30

【請求項 4】

前記暗号化画像データに基づいて一意に決定される識別子を生成する方法は、前記暗号化画像データに所定のメッセージダイジェスト生成関数を適用して前記識別子を算出する方法であることを特徴とする請求項 1 または請求項 2 または請求項 3 記載の画像処理システム。

【請求項 5】

前記画像形成装置は、前記復号鍵情報を前記画像再生装置に送信した後、装置本体側に記憶されている復号鍵情報を消去することを特徴とする請求項 2 記載の画像処理システム。

40

【請求項 6】

前記画像形成装置は、前記復号鍵情報を前記第 2 の交換可能記憶媒体に記憶した後、装置本体側に記憶されている復号鍵情報を消去することを特徴とする請求項 3 または請求項 4 記載の画像処理システム。

【請求項 7】

前記画像形成装置は、前記第 1 の交換可能記憶媒体の 1 つ以上の固有識別情報と、前記第 2 の交換可能記憶媒体の 1 つ以上の固有識別情報を登録し、登録された固有識別情報を

50

備えた前記第1の交換可能記憶媒体および第2の交換可能記憶媒体以外は使用不能にしたことを特徴とする請求項3記載の画像処理システム。

【請求項8】

前記画像形成装置は、装着されている前記第1の交換可能記憶媒体の固有識別情報、または、第2の交換可能記憶媒体の固有識別情報、あるいは、前記第1の交換可能記憶媒体の固有識別情報および前記第2の交換可能記憶媒体の固有識別情報に基づいて、前記共通鍵を生成することを特徴とする請求項3または請求項7記載の画像処理システム。

【請求項9】

入力した画像データに所定の暗号化方法を適用して暗号化画像データを生成するとともに、当該暗号化画像データを復号化する際に用いる復号鍵を生成する画像形成装置と、

10

前記暗号化画像データと前記復号鍵を受け取り、前記暗号化画像データについて前記復号鍵を用いて復号化し、それによって得た前記画像データを再生する画像再生装置とからなる画像処理システムの制御方法であって、

前記画像形成装置は、前記暗号化画像データを生成するたびに異なる前記復号鍵を生成し、前記画像データを暗号化して得た前記暗号化画像データに基づいて一意に決定される識別子を生成し、前記共通鍵に前記識別子を付与して復号鍵情報を形成し、当該復号鍵情報を交換可能記憶媒体に記憶し、

前記画像再生装置は、前記交換可能記憶媒体に記憶された前記復号鍵情報を読み込んで記憶し、再生指定された前記暗号化画像データに基づいて一意に決定される識別子を生成し、当該生成した識別子に対応する復号鍵情報を用いて、前記再生指定された暗号化画像データを復号化することを特徴とする画像処理システムの制御方法。

20

【請求項10】

入力した画像データに所定の暗号化方法を適用して暗号化画像データを生成するとともに、当該暗号化画像データを復号化する際に用いる復号鍵を生成する画像形成装置と、

前記暗号化画像データと前記復号鍵を受け取り、前記暗号化画像データについて前記復号鍵を用いて復号化し、それによって得た前記画像データを再生する画像再生装置とからなる画像処理システムの制御方法であって、

前記画像形成装置は、前記暗号化画像データを第1の交換可能記憶媒体に記憶する一方、前記暗号化画像データを生成するたびに異なる前記復号鍵を生成し、前記画像データを暗号化して得た前記暗号化画像データに基づいて一意に決定される識別子を生成し、前記共通鍵に前記識別子を付与して復号鍵情報を形成し、当該復号鍵情報を第2の交換可能記憶媒体に記憶し、

30

前記画像再生装置は、前記第1の交換可能記憶媒体に記憶された前記暗号化画像データ、および、前記第2の交換可能記憶媒体に記憶された前記復号鍵情報をそれぞれ読み込んで記憶し、再生指定された前記暗号化画像データに基づいて一意に決定される識別子を生成し、当該生成した識別子に対応する復号鍵情報を用いて、前記再生指定された暗号化画像データを復号化することを特徴とする画像処理システムの制御方法。

【請求項11】

入力した画像データに所定の暗号化方法を適用して暗号化画像データを生成するとともに、当該暗号化画像データを復号化する際に用いる復号鍵を生成する画像形成装置と、

40

前記暗号化画像データと前記復号鍵を受け取り、前記暗号化画像データについて前記復号鍵を用いて復号化し、それによって得た前記画像データを再生する画像再生装置とからなる画像処理システムの前記画像形成装置であって、

前記暗号化画像データを生成するたびに異なる前記復号鍵を生成し、前記画像データを暗号化して得た前記暗号化画像データに基づいて一意に決定される識別子を生成し、前記共通鍵に前記識別子を付与して復号鍵情報を形成し、当該復号鍵情報を交換可能記憶媒体に記憶することを特徴とする画像形成装置。

【請求項12】

入力した画像データに所定の暗号化方法を適用して暗号化画像データを生成するとともに、当該暗号化画像データを復号化する際に用いる復号鍵を生成する画像形成装置と、

50

前記暗号化画像データと前記復号鍵を受け取り、前記暗号化画像データについて前記復号鍵を用いて復号化し、それによって得た前記画像データを再生する画像再生装置とからなる画像処理システムの前記画像再生装置であって、

前記画像形成装置が、前記暗号化画像データに基づいて生成した識別子を前記共通鍵に付与して形成した復号鍵情報を記憶した交換可能記憶媒体から、前記復号鍵情報を読み込んで記憶し、

再生指定された前記暗号化画像データに基づいて一意に決定される識別子を生成し、当該生成した識別子に対応した復号鍵情報を用いて、前記再生指定された暗号化画像データを復号化することを特徴とする画像再生装置。

【請求項 13】

10

前記所定の暗号化方法は、共通鍵方式の暗号化方法であり、前記復号鍵は、暗号化の際に用いられる暗号鍵と同一の共通鍵であることを特徴とする請求項 1 または請求項 2 または請求項 3 または請求項 4 または請求項 5 または請求項 6 または請求項 7 または請求項 8 記載の画像処理システム。

【請求項 14】

前記所定の暗号化方法は、共通鍵方式の暗号化方法であり、前記復号鍵は、暗号化の際に用いられる暗号鍵と同一の共通鍵であることを特徴とする請求項 9 または請求項 10 記載の画像処理システムの制御方法。

【請求項 15】

前記所定の暗号化方法は、共通鍵方式の暗号化方法であり、前記復号鍵は、暗号化の際に用いられる暗号鍵と同一の共通鍵であることを特徴とする請求項 11 記載の画像形成装置。

20

【請求項 16】

前記所定の暗号化方法は、共通鍵方式の暗号化方法であり、前記復号鍵は、暗号化の際に用いられる暗号鍵と同一の共通鍵であることを特徴とする請求項 12 記載の画像再生装置。

【請求項 17】

原稿画像を読み取り、共通鍵方式の暗号化方法に適用する共通鍵を生成し、前記読み取って得た画像データについて、前記共通鍵を用いて前記暗号化方法を適用して暗号化し、それによって得た暗号化画像データを生成する画像形成装置と、

30

前記暗号化画像データと前記共通鍵を受け取り、前記暗号化画像データについて前記共通鍵を用いて前記暗号化方法に対応した復号化方法を適用して復号化し、それによって得た前記画像データを再生する画像再生装置とからなる画像処理システムであって、

前記画像形成装置は、前記暗号化画像データを第 1 の交換可能記憶媒体に記憶する一方、前記画像データを形成するたびに異なる前記共通鍵を生成し、前記画像データを暗号化して得た前記暗号化画像データに基づいて一意に決定される識別子を生成し、前記共通鍵に前記識別子を付与して復号鍵情報を形成し、当該復号鍵情報を第 2 の交換可能記憶媒体に記憶し、

前記画像再生装置は、前記第 1 の交換可能記憶媒体に記憶された前記暗号化画像データ、および、前記第 2 の交換可能記憶媒体に記憶された前記復号鍵情報をそれぞれ読み込んで多数記憶し、再生指定された前記暗号化画像データに基づいて一意に決定される識別子を生成し、当該生成した識別子と同一識別子を有する復号鍵情報を、記憶された復号鍵情報から探し出し、当該探し出した復号鍵情報を用いて、前記再生指定された暗号化画像データを復号化することを特徴とする画像処理システム。

40

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、原稿画像を読み取り、共通鍵方式の暗号化方法に適用する共通鍵を生成し、前記読み取って得た画像データについて、前記共通鍵を用いて前記暗号化方法を適用して暗号化し、それによって得た暗号化画像データを生成する画像形成装置と、

50

【 0 0 0 2 】

前記暗号化画像データと前記共通鍵を受け取り、前記暗号化画像データについて前記共通鍵を用いて前記暗号化方法に対応した復号化方法を適用して復号化し、それによって得た前記画像データを再生する画像再生装置とからなる画像処理システム、および、その制御方法、および、画像処理システムの画像形成装置、および、画像処理システムの画像再生装置に関する。

【 背景技術 】

【 0 0 0 3 】

近年、オフィスのペーパーレス化によって、スキャナ機能を有する画像形成装置で読み取った文書を電子化し、そのデータをクライアントPCやファイルサーバへ送信する機能が使われるようになった。

10

【 0 0 0 4 】

しかし、スキャナで読み込んで電子化したデータに対して、内容の不正な改ざんがなされる危険性がある。

【 0 0 0 5 】

また、電子化したデータをネットワークで転送した場合には、データの盗聴などによって情報が漏洩する危険性もある。

【 0 0 0 6 】

その危険性に対して、電子化したデータを暗号化することで情報の漏洩を防ぐ技術が発明されている。

20

【 0 0 0 7 】

特許文献1では、画像形成装置においてスキャンした電子データに対して画像形成装置に接続した外部記憶媒体に保存されている秘密鍵を利用して電子署名を施し、ネットワークを介して接続されるデータ処理装置へ送信することを特徴とする画像形成装置が開示されている。

【 特許文献1 】特許第3616601号公報

【 発明の開示 】

【 発明が解決しようとする課題 】

【 0 0 0 8 】

しかしながら、特許文献1では、利用者があらかじめ秘密鍵と公開鍵のペアを生成し、そのうちの秘密鍵を外部記憶媒体に保存したうえで画像形成装置に接続するという煩雑な手続きが必要であった。

30

【 0 0 0 9 】

また、利用者の秘密鍵が保存された外部記憶装置を紛失した場合、それを手に入れた悪意の第三者に不正に利用される危険性があった。

【 0 0 1 0 】

本発明は、かかる実情に鑑みてなされたものであり、容易に電子データの改ざんならびに情報漏えいを防ぐことが可能な画像処理システムおよび画像処理システムの制御方法および画像形成装置および画像再生装置を提供すること目的とする。

【 課題を解決するための手段 】

40

【 0 0 1 1 】

本発明は、入力した画像データに所定の暗号化方法を適用して暗号化画像データを生成するとともに、当該暗号化画像データを復号化する際に用いる復号鍵を生成する画像形成装置と、前記暗号化画像データと前記復号鍵を受け取り、前記暗号化画像データについて前記復号鍵を用いて復号化し、それによって得た前記画像データを再生する画像再生装置とからなる画像処理システムであって、前記画像形成装置は、前記暗号化画像データを生成するたびに異なる前記復号鍵を生成し、前記画像データを暗号化して得た前記暗号化画像データに基づいて一意に決定される識別子を生成し、前記共通鍵に前記識別子を付与して復号鍵情報を形成し、当該復号鍵情報を交換可能記憶媒体に記憶し、前記画像再生装置は、前記交換可能記憶媒体に記憶された前記復号鍵情報を読み込んで記憶し、再生指定さ

50

れた前記暗号化画像データに基づいて一意に決定される識別子を生成し、当該生成した識別子に対応する復号鍵情報を用いて、前記再生指定された暗号化画像データを復号化するようにしたものである。

【0012】

また、前記画像形成装置は、電子メールを用いて、前記画像再生装置に前記暗号化画像データを送信するようにしたものである。

【0013】

また、入力した画像データに所定の暗号化方法を適用して暗号化画像データを生成するとともに、当該暗号化画像データを復号化する際に用いる復号鍵を生成する画像形成装置と、前記暗号化画像データと前記復号鍵を受け取り、前記暗号化画像データについて前記復号鍵を用いて復号化し、それによって得た前記画像データを再生する画像再生装置とからなる画像処理システムであって、前記画像形成装置は、前記暗号化画像データを第1の交換可能記憶媒体に記憶する一方、前記暗号化画像データを生成するたびに異なる前記復号鍵を生成し、前記画像データを暗号化して得た前記暗号化画像データに基づいて一意に決定される識別子を生成し、前記共通鍵に前記識別子を付与して復号鍵情報を形成し、当該復号鍵情報を第2の交換可能記憶媒体に記憶し、前記画像再生装置は、前記第1の交換可能記憶媒体に記憶された前記暗号化画像データ、および、前記第2の交換可能記憶媒体に記憶された前記復号鍵情報をそれぞれ読み込んで記憶し、再生指定された前記暗号化画像データに基づいて一意に決定される識別子を生成し、当該生成した識別子に対応する復号鍵情報を用いて、前記再生指定された暗号化画像データを復号化するようにしたものである。

【0014】

また、前記暗号化画像データに基づいて一意に決定される識別子を生成する方法は、前記暗号化画像データに所定のメッセージダイジェスト生成関数を適用して前記識別子を算出する方法である。

【0015】

また、前記画像形成装置は、前記復号鍵情報を前記画像再生装置に送信した後、装置本体側に記憶されている復号鍵情報を消去するようにしたものである。

【0016】

また、前記画像形成装置は、前記復号鍵情報を前記第2の交換可能記憶媒体に記憶した後、装置本体側に記憶されている復号鍵情報を消去するようにしたものである。

【0017】

また、前記画像形成装置は、前記第1の交換可能記憶媒体の1つ以上の固有識別情報と、前記第2の交換可能記憶媒体の1つ以上の固有識別情報を登録し、登録された固有識別情報を備えた前記第1の交換可能記憶媒体および第2の交換可能記憶媒体以外は使用不能にしたものである。

【0018】

また、前記画像形成装置は、装着されている前記第1の交換可能記憶媒体の固有識別情報、または、第2の交換可能記憶媒体の固有識別情報、あるいは、前記第1の交換可能記憶媒体の固有識別情報および前記第2の交換可能記憶媒体の固有識別情報に基づいて、前記復号鍵を生成するようにしたものである。

【0019】

また、入力した画像データに所定の暗号化方法を適用して暗号化画像データを生成するとともに、当該暗号化画像データを復号化する際に用いる復号鍵を生成する画像形成装置と、前記暗号化画像データと前記復号鍵を受け取り、前記暗号化画像データについて前記復号鍵を用いて復号化し、それによって得た前記画像データを再生する画像再生装置とからなる画像処理システムの制御方法であって、前記画像形成装置は、前記暗号化画像データを生成するたびに異なる前記復号鍵を生成し、前記画像データを暗号化して得た前記暗号化画像データに基づいて一意に決定される識別子を生成し、前記共通鍵に前記識別子を付与して復号鍵情報を形成し、当該復号鍵情報を交換可能記憶媒体に記憶し、前記画像再

生装置は、前記交換可能記憶媒体に記憶された前記復号鍵情報を読み込んで記憶し、再生指定された前記暗号化画像データに基づいて一意に決定される識別子を生成し、当該生成した識別子に対応する復号鍵情報を用いて、前記再生指定された暗号化画像データを復号化するようにしたものである。

【0020】

また、入力した画像データに所定の暗号化方法を適用して暗号化画像データを生成するとともに、当該暗号化画像データを復号化する際に用いる復号鍵を生成する画像形成装置と、前記暗号化画像データと前記復号鍵を受け取り、前記暗号化画像データについて前記復号鍵を用いて復号化し、それによって得た前記画像データを再生する画像再生装置とからなる画像処理システムの制御方法であって、前記画像形成装置は、前記暗号化画像データを第1の交換可能記憶媒体に記憶する一方、前記暗号化画像データを生成するたびに異なる前記復号鍵を生成し、前記画像データを暗号化して得た前記暗号化画像データに基づいて一意に決定される識別子を生成し、前記共通鍵に前記識別子を付与して復号鍵情報を形成し、当該復号鍵情報を第2の交換可能記憶媒体に記憶し、前記画像再生装置は、前記第1の交換可能記憶媒体に記憶された前記暗号化画像データ、および、前記第2の交換可能記憶媒体に記憶された前記復号鍵情報をそれぞれ読み込んで記憶し、再生指定された前記暗号化画像データに基づいて一意に決定される識別子を生成し、当該生成した識別子に対応する復号鍵情報を用いて、前記再生指定された暗号化画像データを復号化するようにしたものである。

10

【0021】

また、入力した画像データに所定の暗号化方法を適用して暗号化画像データを生成するとともに、当該暗号化画像データを復号化する際に用いる復号鍵を生成する画像形成装置と、前記暗号化画像データと前記復号鍵を受け取り、前記暗号化画像データについて前記復号鍵を用いて復号化し、それによって得た前記画像データを再生する画像再生装置とからなる画像処理システムの前記画像形成装置であって、前記暗号化画像データを生成するたびに異なる前記復号鍵を生成し、前記画像データを暗号化して得た前記暗号化画像データに基づいて一意に決定される識別子を生成し、前記共通鍵に前記識別子を付与して復号鍵情報を形成し、当該復号鍵情報を交換可能記憶媒体に記憶するようにしたものである。

20

【0022】

また、入力した画像データに所定の暗号化方法を適用して暗号化画像データを生成するとともに、当該暗号化画像データを復号化する際に用いる復号鍵を生成する画像形成装置と、前記暗号化画像データと前記復号鍵を受け取り、前記暗号化画像データについて前記復号鍵を用いて復号化し、それによって得た前記画像データを再生する画像再生装置とからなる画像処理システムの前記画像再生装置であって、前記画像形成装置が、前記暗号化画像データに基づいて生成した識別子を前記共通鍵に付与して形成した復号鍵情報を記憶した交換可能記憶媒体から、前記復号鍵情報を読み込んで記憶し、再生指定された前記暗号化画像データに基づいて一意に決定される識別子を生成し、当該生成した識別子に対応した復号鍵情報を用いて、前記再生指定された暗号化画像データを復号化するようにしたものである。

30

【0023】

また、前記所定の暗号化方法は、共通鍵方式の暗号化方法であり、前記復号鍵は、暗号化の際に用いられる暗号鍵と同一の共通鍵である。

40

【0024】

また、原稿画像を読み取り、共通鍵方式の暗号化方法に適用する共通鍵を生成し、前記読み取って得た画像データについて、前記共通鍵を用いて前記暗号化方法を適用して暗号化し、それによって得た暗号化画像データを生成する画像形成装置と、前記暗号化画像データと前記共通鍵を受け取り、前記暗号化画像データについて前記共通鍵を用いて前記暗号化方法に対応した復号化方法を適用して復号化し、それによって得た前記画像データを再生する画像再生装置とからなる画像処理システムであって、前記画像形成装置は、前記暗号化画像データを第1の交換可能記憶媒体に記憶する一方、前記画像データを形成する

50

たびに異なる前記共通鍵を生成し、前記画像データを暗号化して得た前記暗号化画像データに基づいて一意に決定される識別子を生成し、前記共通鍵に前記識別子を付与して復号鍵情報を形成し、当該復号鍵情報を第2の交換可能記憶媒体に記憶し、前記画像再生装置は、前記第1の交換可能記憶媒体に記憶された前記暗号化画像データ、および、前記第2の交換可能記憶媒体に記憶された前記復号鍵情報をそれぞれ読み込んで多数記憶し、再生指定された前記暗号化画像データに基づいて一意に決定される識別子を生成し、当該生成した識別子と同一識別子を有する復号鍵情報を、記憶された復号鍵情報から探し出し、当該探し出した復号鍵情報を用いて、前記再生指定された暗号化画像データを復号化するようにしたものである。

【発明の効果】

10

【0025】

したがって、本発明によれば、暗号化と復号化に利用する共通鍵を画像形成装置が生成し、復号に使う復号鍵情報を画像形成装置が画像再生装置に出力する手段を持つことで、ユーザが事前に鍵の生成などの準備を行うことが不要となり、任意の画像データの暗号化とその復号が可能となるという効果を得る。また、暗号化されたデータと復号鍵の関連付けを行うことにより、復号鍵の管理が容易となるという効果も得る。

【発明を実施するための最良の形態】

【0026】

以下、添付図面を参照しながら、本発明の実施の形態を詳細に説明する。

【0027】

20

図1は、本発明の一実施例にかかるネットワークシステムを示している。

【0028】

同図において、ローカルエリアネットワークLANには、複数のワークステーション装置WS1~WSn、メールサーバ装置SM、および、複合機FXが接続されているとともに、ルータ装置RTを介してインターネットへ接続されている。したがって、ワークステーション装置WS1~WSn、メールサーバ装置SM、および、複合機FXは、インターネットを介し、他の適宜な端末装置との間でデータをやりとりすることができる。

【0029】

ここで、メールサーバ装置SMは、ローカルエリアネットワークLANに接続されているワークステーション装置WS1~WSnを利用するユーザ、および、ネットワーク複合機FXに対して、周知の電子メールの収集および配布のサービスを提供するものである。

30

【0030】

また、ワークステーション装置WS1~WSnには、複合機FXから出力される暗号化画像データおよび復号鍵情報を入力して処理するためのソフトウェア、ファクシミリ画情報を作成および表示出力するファクシミリアプリケーションソフトウェア、および、ローカルエリアネットワークLANを介して複合機FXとの間で種々のデータのやりとりを行うための通信ソフトウェアなどの種々のプログラムが導入されており、特定のユーザにより使用されるものである。ここで、特定のユーザは、一人または複数人のユーザであってよい。

【0031】

40

また、複合機FXは、原稿画像を読み取って得た画像データを暗号化してワークステーション装置WS1~WSnに配布する暗号化画像データ配布機能、画情報や各種レポートなどを電子メールとしてやりとりするための電子メール処理機能、および、アナログ公衆回線網PSTNに接続し、この公衆網を伝送路として用いてグループ3ファクシミリ伝送手順による画情報伝送を行う伝送機能を備えている。

【0032】

図2は、複合機FXの構成例を示している。

【0033】

同図において、システム制御部1は、この複合機FXの各部の制御処理、暗号化処理、および、ファクシミリ伝送制御手順処理などの各種制御処理を行うものであり、システム

50

メモリ 2 は、システム制御部 1 が実行する制御処理プログラム、および、処理プログラムを実行するときに必要な各種データなどを記憶するとともに、システム制御部 1 のワークエリアを構成するものであり、ROM (リード・オンリ・メモリ) および RAM (ランダム・アクセス・メモリ) からなる。また、パラメータメモリ 3 は、この複合機 F X に固有な各種の情報を記憶するためのものであり、NV-RAM (不揮発性 RAM) などから構成される。時計回路 4 は、現在時刻情報を出力するものである。

【0034】

スキャナ 5 は、所定の解像度で原稿画像を読み取るためのものであり、自動原稿搬送装置 (ADF) を備えている。また、プロッタ 6 は、所定の解像度で画像を記録出力するためのものであり、操作表示部 7 は、この複合機 F X を操作するためのもので、各種の操作キー、および、各種の表示器からなる。

10

【0035】

符号化復号化部 8 は、画信号を符号化圧縮するとともに、符号化圧縮されている画情報を元の画信号に復号化するためのものであり、磁気ディスク装置 9 は、符号化圧縮された状態の画情報を多数記憶したり、復号鍵情報などの各種データを記憶するためのものである。

【0036】

グループ 3 ファクシミリモデム 10 は、グループ 3 ファクシミリのモデム機能を実現するためのものであり、伝送手順信号をやりとりするための低速モデム機能 (V.21 モデム)、および、おもに画情報をやりとりするための高速モデム機能 (V.17 モデム、V.34 モデム、V.29 モデム、V.27ter モデムなど) を備えている。

20

【0037】

網制御装置 11 は、この複合機 F X をアナログ公衆回線網 P S T N に接続するためのものであり、自動発着信機能を備えている。

【0038】

ローカルエリアネットワークインターフェース回路 12 は、この複合機 F X をローカルエリアネットワーク LAN に接続するためのものであり、ローカルエリアネットワーク伝送制御部 13 は、ローカルエリアネットワーク LAN を介して、他のデータ端末装置との間で種々のデータをやりとりするための各種所定のプロトコルスイートの通信制御処理を実行するためのものである。

30

【0039】

USB ホストユニット 14 は、USB によるデータストレージ等の機能を実現するためのものであり、2 つの USB ソケット 15, 16 が備えられている。この USB スロット 15, 16 には、それぞれ着脱自在の USB メモリデバイス 17, 18 を装着して、外部記憶装置として用いることができる。

【0040】

これらの、システム制御部 1、システムメモリ 2、パラメータメモリ 3、時計回路 4、スキャナ 5、プロッタ 6、操作表示部 7、符号化復号化部 8、磁気ディスク装置 9、グループ 3 ファクシミリモデム 10、網制御装置 11、ローカルエリアネットワーク伝送制御部 13、および、USB ホストユニット 14 は、内部バス 19 に接続されており、これらの各要素間でのデータのやりとりは、主としてこの内部バス 19 を介して行われている。

40

【0041】

また、網制御装置 11 とグループ 3 ファクシミリモデム 10 との間のデータのやりとりは、直接行なわれている。

【0042】

ここで、本実施例において、基本的には、ローカルエリアネットワーク LAN に接続されている端末相互間でのデータのやりとりは、いわゆる TCP/IP と呼ばれるトランスポートレイヤまでの伝送プロトコルと、それ以上の上位レイヤの通信プロトコルとの組み合わせ (いわゆるプロトコルスイート) が適用して行われる。例えば、電子メールのデータのやりとりでは上位レイヤの通信プロトコルとして SMTP (Simple Mail

50

Transfer Protocol)という通信プロトコルが適用される。

【0043】

また、各端末がメールサーバ装置SMに対して、ユーザ宛の電子メールの受信確認や取得要求などのために適用するプロトコルとしては、いわゆるPOP(Post Office Protocol)などを適用することができる。

【0044】

また、TCP/IP, SMTP, POPなどの通信プロトコル、および、電子メールのデータ形式やデータ構造などについては、それぞれIETFから発行されているRFC文書により規定されている。例えば、TCPはRFC793、IPはRFC793、SMTPはRFC821、電子メールの形式は、RFC822, RFC1521, RFC1522(MIME(Multi Purpose Mail Extension)形式)などでそれぞれ規定されている。

10

【0045】

図3は、ワークステーション装置WS(WS1~WSn)の構成例を示している。

【0046】

同図において、CPU(中央処理装置)21は、このワークステーション装置WSの動作制御を行うものであり、ROM(リード・オンリ・メモリ)22は、CPU21が起動時に実行するプログラムや必要なデータ等を記憶するためのものであり、RAM(ランダム・アクセス・メモリ)23は、CPU21のワークエリア等を構成するためのものである。

20

【0047】

キャラクタジェネレータ24は、図形文字の表示データを発生するためのものであり、時計回路25は、現在日時情報を出力するためのものであり、ローカルエリアネットワークインターフェース回路26は、このワークステーション装置WSをローカルエリアネットワークLANに接続するためのものであり、ローカルエリアネットワーク伝送制御部27は、ローカルエリアネットワークLANを介して、他のデータ端末装置との間で種々のデータをやりとりするための各種所定のプロトコルスイートの通信制御処理を実行するためのものである。

【0048】

磁気ディスク装置28は、Webブラウザなどの種々のアプリケーションプログラム、ワークデータ、ファイルデータ、復号鍵情報、暗号化画像データ、および、画情報データなどの種々のデータを記憶するためのものであり、CRT画面表示装置29は、このワークステーション装置WSを操作するための画面を表示するためのものであり、表示制御部30は、CRT画面表示装置29の表示内容を制御するためのものである。

30

【0049】

キーボード装置31は、このワークステーション装置WSに種々のキー操作を行うためのものであり、画面指示装置32は、CRT画面表示装置29の任意の点を指示する等の操作作業を行うためのものであり、入力制御部33は、キーボード装置31および画面指示装置32の入力情報を取り込む等するためのものである。

【0050】

USBホストユニット34は、USBによるデータストレージ等の機能を実現するためのものであり、1つのUSBソケット35が備えられている。このUSBスロット35には、着脱自在のUSBメモリデバイス36を装着して、外部記憶装置として用いることができる。

40

【0051】

これらのCPU21、ROM22、RAM23、キャラクタジェネレータ24、時計回路25、ローカルエリアネットワーク伝送制御部27、磁気ディスク装置28、表示制御部30、入力制御部33、および、USBホストユニット34は、バス37に接続されており、これらの各要素間のデータのやりとりは、主としてこのバス37を介して行われる。

50

【0052】

さて、本実施例では、複合機 F X は、スキャナ 5 によって読み取って得た画像データを暗号化し、その暗号化画像データを U S B メモリデバイス 1 7 または U S B メモリデバイス 1 8 に保存し、あるいは、ローカルエリアネットワーク L A N を介してワークステーション装置 W S に転送するとともに、暗号化画像データを復号化の際に必要な復号鍵情報（後述）を形成し、その復号鍵情報を U S B メモリデバイス 1 8 あるいは U S B メモリデバイス 1 7 に保存する。また、復号鍵情報には、対応する暗号化画像データをあらかず識別情報が付加される。

【0053】

一方、ワークステーション装置 W S では、暗号化画像データまたは復号鍵情報を保存した U S B メモリデバイス 1 7 , 1 8 が U S B スロット 3 5 に装着され、U S B メモリデバイス 1 7 , 1 8 がワークステーション装置 W S の外部記憶装置として用いられる。

【0054】

そして、ワークステーション装置 W S では、U S B メモリデバイス 1 7 , 1 8 に保存されている暗号化画像データおよび復号鍵情報を読み込み、磁気ディスク装置 2 8 に保存する。

【0055】

ワークステーション装置 W S のユーザは、例えば、磁気ディスク装置 2 8 に保存されている暗号化画像データの一覧を表示させ、表示出力を希望する暗号化画像データを選択する。

【0056】

それにより、ワークステーション装置 W S は、選択された暗号化画像データに基づいて、復号鍵の識別情報を作成し、その識別情報を持つ復号鍵情報を、磁気ディスク装置 2 8 に保存されて多数の復号鍵情報から探し出す。

【0057】

そして、探し出した復号鍵情報に含まれる復号鍵を用いて、選択された暗号化画像データについて復号化処理を適用し、元の画像データを復号して、表示出力する。

【0058】

このようにして、本実施例では、画像データを読み取るたびに異なる暗号鍵を生成して、その生成した暗号鍵を用いて読取画像データを暗号化し、その暗号化画像データを U S B メモリデバイスに保存するかあるいは指定されたワークステーション装置 W S の保存領域に保存するとともに、復号化処理の際に必要な復号鍵情報を U S B メモリデバイスに保存する。

【0059】

また、暗号化の際に用いる暗号鍵は、いわば使い捨て的な暗号鍵であり、暗号化処理対象となる画像データのそれぞれについて生成するため、U S B メモリデバイスには、多数の復号鍵情報が保存される。そこで、それぞれの暗号化画像データとそれを復号化処理する際に必要となる復号鍵情報とを関連づけできる識別情報を生成して、復号鍵情報にその識別情報を含めるようにする。

【0060】

ここで、複合機 F X が適用する暗号化方法について説明する。

【0061】

本実施例では、図 4 に示すような共通鍵方式の暗号化方法、あるいは、図 5 に示すような公開鍵方式に準拠した暗号鍵と復号鍵を用いた暗号化方法のいずれかを採用する。共通鍵方式の暗号化方法では、暗号化処理と復号化処理とで同一の鍵（共通鍵）を用いる。したがって、この場合の復号鍵は共通鍵である。また、暗号鍵と復号鍵を用いた暗号化方法では、暗号鍵と対になった復号鍵を生成し、暗号鍵を用いて暗号化処理を行い、復号鍵を用いて復号化処理を行う。

【0062】

なお、暗号化処理の具体的な方式は、適宜な暗号化方法を適用することができる。

10

20

30

40

50

【 0 0 6 3 】

また、復号鍵情報の一例を図 6 (a) ~ (c) に示す。

【 0 0 6 4 】

USBメモリデバイスには、同図 (a) に示すように、複数の復号鍵情報が記憶される。

【 0 0 6 5 】

また、おのおのの復号鍵情報は、例えば、同図 (b) に示すように、USBメモリデバイスのファイルシステムにおいてそれぞれのファイルを識別するために必要となる識別情報であるファイル名が付与され、また、そのファイルの本体は、当該復号鍵情報を対応する暗号化画像データと対応付けるために用いられる鍵識別情報、および、復号鍵の本体である復号鍵データからなる。

10

【 0 0 6 6 】

復号鍵情報の他の例を同図 (c) に示す。この場合は、ファイル名として、当該復号鍵情報を対応する暗号化画像データと対応付けるために用いられる鍵識別情報を付与するとともに、ファイルの本体は、復号鍵の本体である復号鍵データのみからなる。なお、この場合、鍵識別情報は、USBメモリデバイスのファイルシステムで適用可能なファイル名のフォーマットに従った桁数および文字種から構成されることとなる。

【 0 0 6 7 】

また、共通鍵の生成方法は、暗号化処理に必要なビット数のバイナリデータを作成する適宜な方法を採用することができる。基本的には、所定ビット数のデータを種データとして、乱数関数を適用して必要なビット数のバイナリデータを生成する。

20

【 0 0 6 8 】

また、種データとしては、例えば、日時データ、画像データから抽出した所定ビット数のデータ (抽出する場所は、日時やファイル名を種データとして発生させた乱数に対応したオフセットアドレスを起点とする等)、あるいは、画像データにメッセージダイジェスト関数を適用して生成した所定ビット数のデータなどを適用することができる。

【 0 0 6 9 】

一方、暗号鍵と復号鍵をともに生成する場合は、上述した共通鍵と同様の方法を適用することができる。

【 0 0 7 0 】

また、鍵識別情報は、暗号化画像データに対して所定のハッシュ関数 (メッセージダイジェスト関数) を適用して形成した所定ビット数のデータを用いることができる。また、ハッシュ関数は、例えば、MD5 や SHA - 1 を適用することができる。

30

【 0 0 7 1 】

また、鍵識別情報の他の例としては、例えば、ファイル名にファイル生成日時を連結したものをを用いることができる。

【 0 0 7 2 】

図 7 は、複合機 F X の処理の一例を示している。この場合、暗号化方法として、共通鍵方式の暗号化方法を適用している。

【 0 0 7 3 】

ユーザが原稿読み取りを指令すると、スキャナ 5 にセットされている読取原稿の画像を読み取り、磁気ディスク装置 9 に一時的に蓄積する (処理 1 0 1)。次いで、上述した方法を適用して共通鍵を生成し、パラメータメモリ 3 または磁気ディスク装置 9 に一時的に保存する (処理 1 0 2)。

40

【 0 0 7 4 】

次に、生成した共通鍵を用い、読取画像データを暗号化処理し、暗号化画像データを磁気ディスク装置 9 に一時的に保存する (処理 1 0 3)。

【 0 0 7 5 】

そして、暗号化画像データにハッシュ関数を適用して、識別情報を生成し (処理 1 0 4)、上述したような復号鍵情報を作成し、パラメータメモリ 3 または磁気ディスク装置 9

50

に一時的に保存する（処理 105）。

【0076】

ここで、図 8 に示すような出力先選択画面を表示して、ユーザに対し、暗号化画像データおよび復号鍵の保存先（暗号化電子データ出力先および復号鍵出力先）を選択させる。また、暗号化画像データの保存先として「ネットワーク」を選択した場合、保存先のネットワークアドレス（例えば、ワークステーション装置 WS1 の磁気ディスク装置 28 に形成されている共有記憶領域のネットワークフォルダ名等）を入力させる。

【0077】

次いで、暗号化画像データの出力先として USB メモリデバイス 17 が選択されたかどうかを調べ（判断 106）、判断 106 の結果が YES になるときは、暗号化画像データを USB メモリデバイス 17 に保存する（処理 107）。

10

【0078】

また、判断 106 の結果が NO になるときは、暗号化画像データの出力先として USB メモリデバイス 18 が選択されたかどうかを調べ（判断 108）、判断 108 の結果が YES になるときは、暗号化画像データを USB メモリデバイス 18 に保存する（処理 109）。

【0079】

また、判断 108 の結果が NO になるときは、暗号化画像データの出力先としてネットワークが選択された場合なので、暗号化画像データを、ローカルエリアネットワーク LAN を介し、指定されたネットワークアドレスへ転送する（処理 110）。

20

【0080】

次に、復号鍵の出力先として USB メモリデバイス 17 が選択されたかどうかを調べ（判断 111）、判断 111 の結果が YES になるときは、復号鍵情報を USB メモリデバイス 17 に保存する（処理 112）。

【0081】

また、判断 111 の結果が NO になるときは、暗号化画像データの出力先として USB メモリデバイス 18 が選択された場合なので、復号鍵情報を USB メモリデバイス 18 に保存する（処理 113）。

【0082】

このようにして、暗号化画像データおよび復号鍵情報の保存が終了すると、そのときに一時保存した暗号化画像データおよび復号鍵情報を消去して（処理 114）、このときの処理を終了する。

30

【0083】

図 9 は、ローカルエリアネットワーク LAN を介し、暗号化画像データの転送要求を複合機 FX から受信した際のワークステーション装置 WS の処理の一例を示している。

【0084】

転送要求を受信すると（処理 201）、暗号化画像データを受信して、磁気ディスク装置 28 に保存する（処理 202）。

【0085】

図 10 は、ワークステーション装置 WS が、USB メモリデバイス 36 から復号鍵情報を保存するように、ユーザから指令されたときの処理の一例を示している。なお、この処理は、USB メモリデバイス 36 が USB スロット 35 に装着された際、自動的に起動するようにすることもできる。

40

【0086】

復号鍵情報保存指令を入力すると（処理 301）、USB メモリデバイス 36 から復号鍵情報を読み込んで、磁気ディスク装置 28 に保存する（処理 302）。

【0087】

図 11 は、ワークステーション装置 WS において、ユーザが USB メモリデバイス 36 から暗号化画像データの読み込みを指令した際に実行する処理の一例を示している。

【0088】

50

暗号化画像データの読み込み指令を入力すると(処理401)、USBメモリデバイス36から暗号化画像データを読み込んで、磁気ディスク装置28に保存する(処理402)。

【0089】

次に、磁気ディスク装置28に記憶されている復号鍵情報の一覧を取得し(処理403)、そのときに読み込んだ暗号化画像データに所定のハッシュ関数を適用して、ハッシュ値(この場合は、識別情報)を作成する(処理404)。

【0090】

そして、1つ復号鍵情報を取得し(処理405)、復号鍵情報の鍵識別情報と、処理404で作成したハッシュ値が一致するかどうかを調べる(判断406)。判断406の結果がNOになる場合は、まだ調べていない復号鍵情報が存在するかどうかを調べ(判断407)、判断407の結果がYESになるときには、処理405へ戻り、残りの復号鍵情報について処理する。

【0091】

また、判断407の結果がNOになる場合は、該当する復号鍵情報が見つからなかったため、この場合は、エラー表示し(処理408)、エラー終了する。

【0092】

また、いずれかの復号鍵情報の鍵識別情報がハッシュ値と一致し、判断406の結果がYESになるときには、その復号鍵情報の復号鍵データを取得し、その復号鍵データを復号鍵として適用し、暗号化画像データを復号化処理して、画像データを生成する(処理409)。

【0093】

そして、生成した画像データ(電子データ)を出力表示するとともに、磁気ディスク装置28に保存して(処理410)、このときの処理を終了する。

【0094】

また、既に磁気ディスク装置28に保存されている暗号化画像データを表示出力させる場合には、保存されている暗号化画像データの一覧情報を表示して、ユーザに所望する暗号化画像データを選択させ、その選択された暗号化画像データについて同様の処理を適用することができる。

【0095】

図12は、複合機FXの処理の他の例を示している。この場合、暗号化方法として、公開鍵方式に準拠した暗号鍵と復号鍵を用いた暗号化方法を適用している。

【0096】

ユーザが原稿読み取りを指令すると、スキャナ5にセットされている読取原稿の画像を読み取り、磁気ディスク装置9に一時的に蓄積する(処理501)。次いで、上述した方法を適用して暗号鍵および復号鍵を生成し、パラメータメモリ3または磁気ディスク装置9に一時的に保存する(処理502)。

【0097】

次に、生成した暗号鍵を用い、読取画像データを暗号化処理し、暗号化画像データを磁気ディスク装置9に一時的に保存する(処理503)。

【0098】

そして、暗号化画像データにハッシュ関数を適用して、識別情報を生成し(処理504)、上述したような復号鍵情報を作成し、パラメータメモリ3または磁気ディスク装置9に一時的に保存する(処理505)。

【0099】

ここで、図7に示すような出力先選択画面を表示して、ユーザに対し、暗号化画像データおよび復号鍵の保存先(暗号化電子データ出力先および復号鍵出力先)を選択させる。また、暗号化画像データの保存先として「ネットワーク」を選択した場合、保存先のネットワークアドレス(例えば、ワークステーション装置WS1の磁気ディスク装置28に形成されている共有記憶領域のネットワークフォルダ名等)を入力させる。

10

20

30

40

50

【0100】

次いで、暗号化画像データの出力先としてUSBメモリデバイス17が選択されたかどうかを調べ(判断506)、判断506の結果がYESになるときは、暗号化画像データをUSBメモリデバイス17に保存する(処理507)。

【0101】

また、判断506の結果がNOになるときは、暗号化画像データの出力先としてUSBメモリデバイス18が選択されたかどうかを調べ(判断508)、判断508の結果がYESになるときは、暗号化画像データをUSBメモリデバイス18に保存する(処理509)。

【0102】

また、判断508の結果がNOになるときは、暗号化画像データの出力先としてネットワークが選択された場合なので、暗号化画像データを、ローカルエリアネットワークLANを介し、指定されたネットワークアドレスへ転送する(処理550)。

【0103】

次に、復号鍵の出力先としてUSBメモリデバイス17が選択されたかどうかを調べ(判断511)、判断511の結果がYESになるときは、復号鍵情報をUSBメモリデバイス17に保存する(処理512)。

【0104】

また、判断511の結果がNOになるときは、暗号化画像データの出力先としてUSBメモリデバイス18が選択された場合なので、復号鍵情報をUSBメモリデバイス18に保存する(処理513)。

【0105】

このようにして、暗号化画像データおよび復号鍵情報の保存が終了すると、そのときに一時保存した暗号化画像データおよび復号鍵情報を消去して(処理514)、このときの処理を終了する。

【0106】

以上のように、本実施例では、暗号化と復号に利用する鍵を複合機が生成し、復号に使う復号鍵を複合機が外部に出力する手段を持つことで、ユーザが事前に鍵の生成などの準備を行うことが不要となり、任意の画像データの暗号化とその復号が可能となる。また、暗号化されたデータと復号鍵の関連付けを行うことにより、復号鍵の管理が容易となる。

【0107】

また、復号鍵を電子文書(読取画像データ)ごとに関連付け、復号鍵の出力方法をUSBメモリデバイス(可搬性記憶媒体)への書き込みとすることで、復号鍵を盗聴されることなく持ち運びを行うことが可能になるだけでなく、復号鍵の格納された可搬性記憶媒体を紛失するとしても被害を最小限におさえることが可能となる。

【0108】

また、暗号化された電子データの出力方法を復号鍵の出力先である可搬性記憶媒体とは異なる可搬性記憶バイトへの書き込みとすることで、安全に電子データを持ち運びすることが可能となる。

【0109】

また、電子データごとに異なる復号鍵を生成することにより、たとえ1つの鍵が悪意ある第三者に渡ったとしても、被害を最小限におさえることが可能となる。

【0110】

また、電子データに一意的な識別情報を復号鍵に付与して電子データと復号鍵の関連付けを行うことにより、暗号化された電子データを復号するための復号鍵を特定することが可能となる。

【0111】

また、暗号方式として公開鍵暗号方式を用いることで、電子データに対してデジタル署名を行うことが可能となる。

【0112】

10

20

30

40

50

また、暗号方式として共通鍵暗号方式を用いることで、文書を編集した後に、再度同じ鍵で復号できる情報として暗号化することが可能となる。

【0113】

また、関連付け手段は、暗号化画像データから不可逆的な処理により計算される一意な値と、復号鍵に付与されている識別情報とを比較し、一致する組合せを関連付けることにより、ユーザが鍵の種類を意識することなく暗号化画像データを復号することが可能となる。

【0114】

また、復号鍵を出力した後に装置内部から削除することで、復号鍵漏洩の危険性を低減させることが可能となる。

【0115】

ところで、上述した実施例では、暗号化画像データの出力先としてネットワークが選択された場合、複合機FXとワークステーション装置WSはローカルエリアネットワークLANを介して直接通信しているが、この場合の通信手段として電子メールを用いることができる。その場合、ユーザは、宛先のメールアドレスを指定する必要がある。

【0116】

また、上述した実施例では、1つの読取ジョブについて、1つの共通鍵または一組の暗号鍵/復号鍵を生成しているが、複数の読取ジョブについて、1つの共通鍵または一組の暗号鍵/復号鍵を生成するようにすることもできる。その場合、全ての画像データをまとめて1つの暗号化画像データとして作成することができる。

【0117】

ところで、USBメモリデバイスには、それぞれの個体を識別するための製造番号が付与されて、USBメモリデバイスの適宜な記憶領域に保存されている。そこで、複合機FXに、USBメモリデバイスの製造番号を登録させておき、この登録されたUSBメモリデバイスのみを使用可能にすることができる。

【0118】

その場合、USBメモリデバイスの製造番号に基づいて、共通鍵、あるいは、暗号鍵および復号鍵を生成することができる。例えば、USBメモリデバイスの製造番号と、使用回数を保存しておき、製造番号と使用回数に基づいて、共通鍵、あるいは、暗号鍵および復号鍵を生成すると、毎回異なる共通鍵、あるいは、暗号鍵および復号鍵を生成すること

【0119】

また、上述した実施例では、ローカルエリアネットワークLANに接続されているワークステーション装置WSについて、本発明を適用した場合について説明しているが、ルータ装置RTを介して接続される外のネットワークに接続されているワークステーション装置やパーソナルコンピュータ装置などにも、本発明を適用することができる。

【0120】

また、上述した実施例では、画像データを入力する手段として、スキャナを用いているが、この画像データ入力手段としては、例えば、磁気ディスク装置に記憶された画像データを入力する手段、あるいは、USBメモリデバイスに記憶された画像データを入力する手段、あるいは、ローカルエリアネットワークLANを介して通信により画像データを入力する手段を用いることもできる。

【0121】

また、上述した実施例では、複合機について本発明を適用しているが、それ以外の同様の構成を備えた画像処理装置についても、本発明を同様に適用することができる。

【図面の簡単な説明】

【0122】

【図1】本発明の一実施例にかかるネットワークシステムを示したブロック図。

【図2】複合機FXの構成例を示したブロック図。

【図3】ワークステーション装置WS(W S 1 ~ W S n)の構成例を示したブロック図。

10

20

30

40

50

- 【図4】共通鍵方式の暗号化方法について説明するための概略図。
- 【図5】公開鍵方式に準拠した暗号鍵と復号鍵を用いた暗号化方法について説明するための概略図。
- 【図6】復号鍵情報の一例を示した概略図。
- 【図7】複合機FXの処理の一例を示したフローチャート。
- 【図8】出力先選択画面の一例を示したフローチャート。
- 【図9】ローカルエリアネットワークLANを介し、暗号化画像データの転送要求を複合機FXから受信した際のワークステーション装置WSの処理の一例を示したフローチャート。
- 【図10】ワークステーション装置WSが、USBメモリデバイス36から復号鍵情報を保存するように、ユーザから指令されたときの処理の一例を示したフローチャート。
- 【図11】ワークステーション装置WSにおいて、ユーザがUSBメモリデバイス36から暗号化画像データの読み込みを指令した際に実行する処理の一例を示したフローチャート。
- 【図12】複合機FXの処理の他の例を示したフローチャート。

10

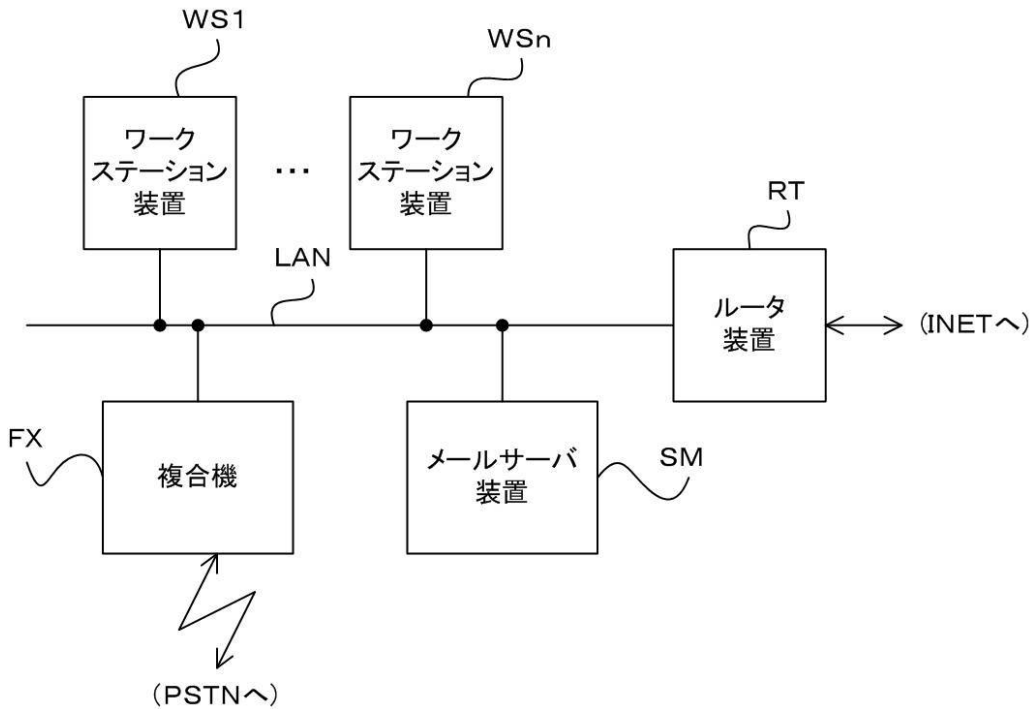
【符号の説明】

【0123】

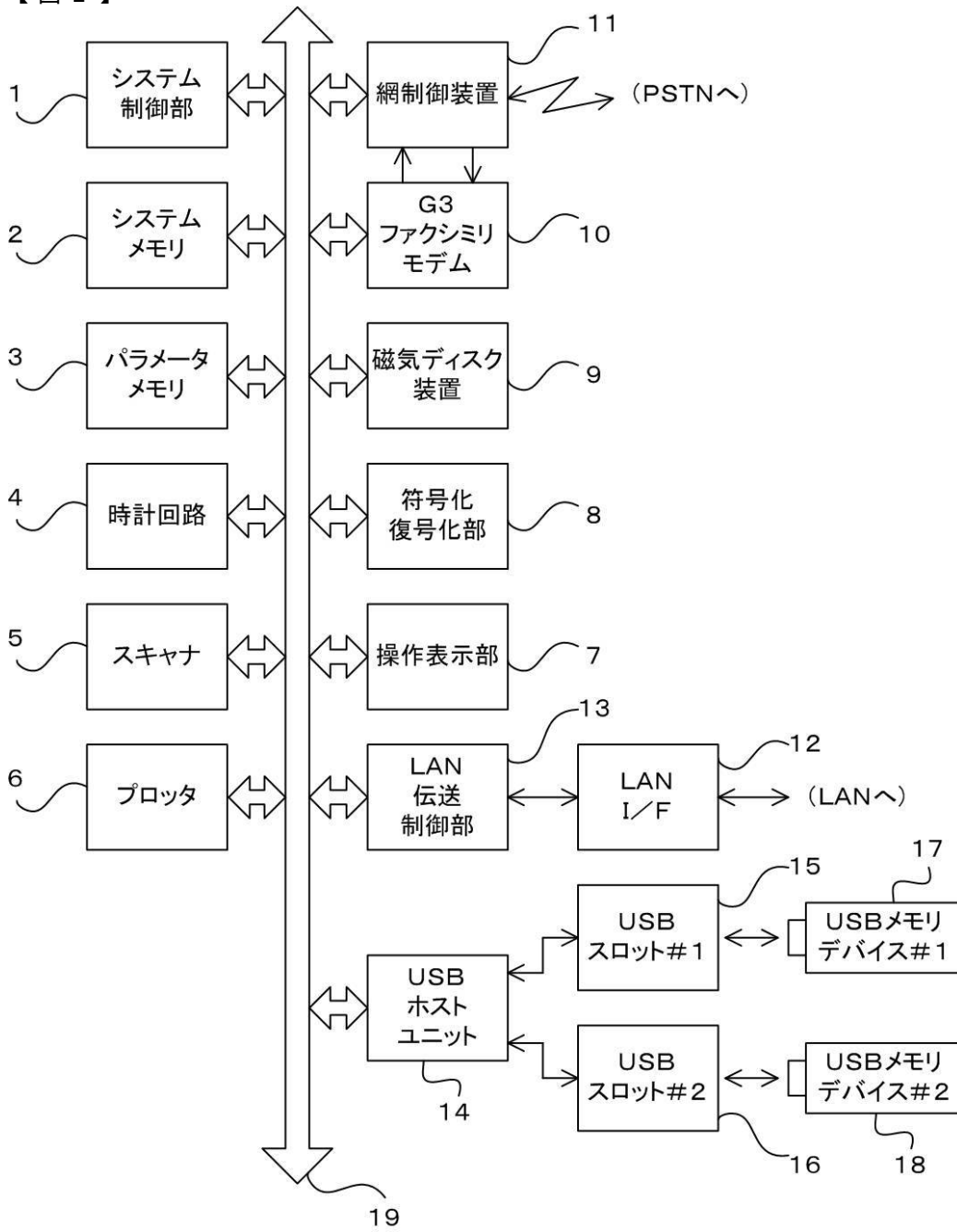
FX 複合機

WS1 ~ WSn, WS ワークステーション装置

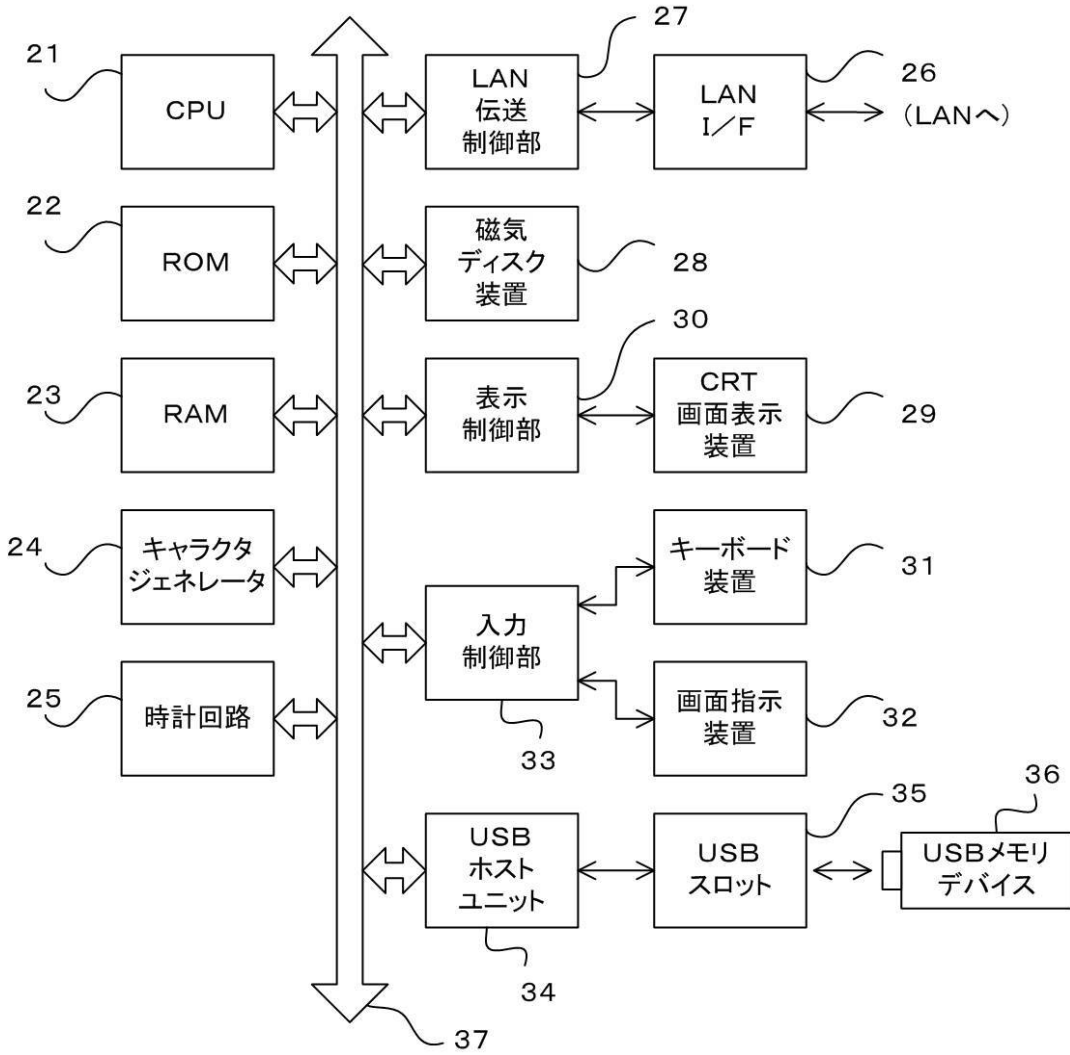
【図1】



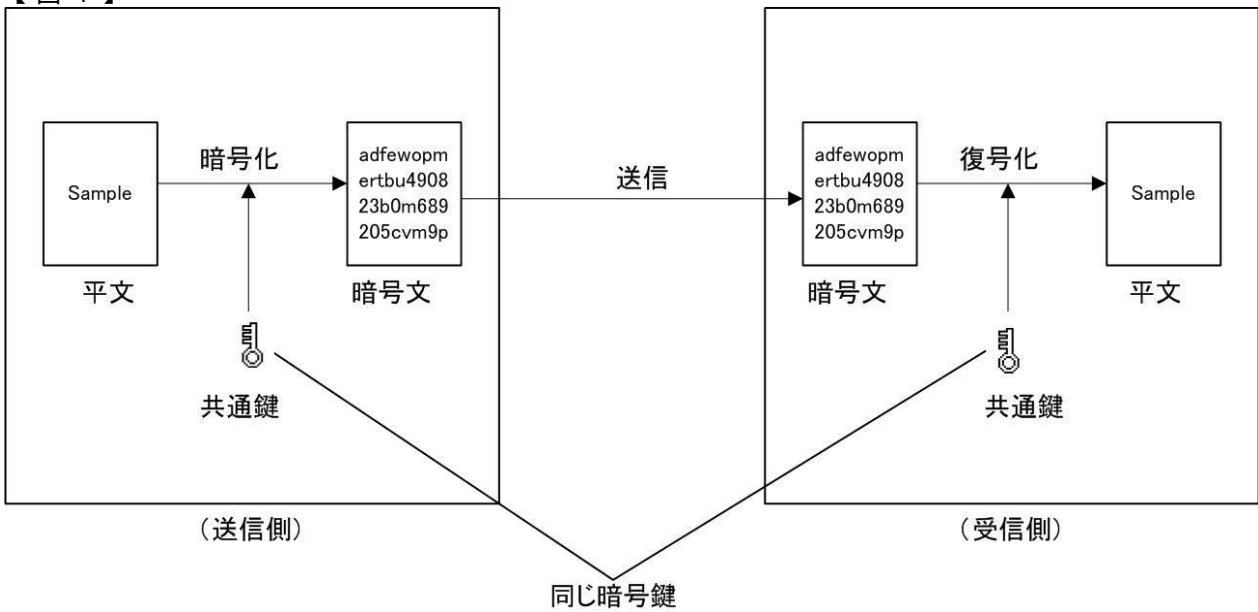
【図2】



【図3】

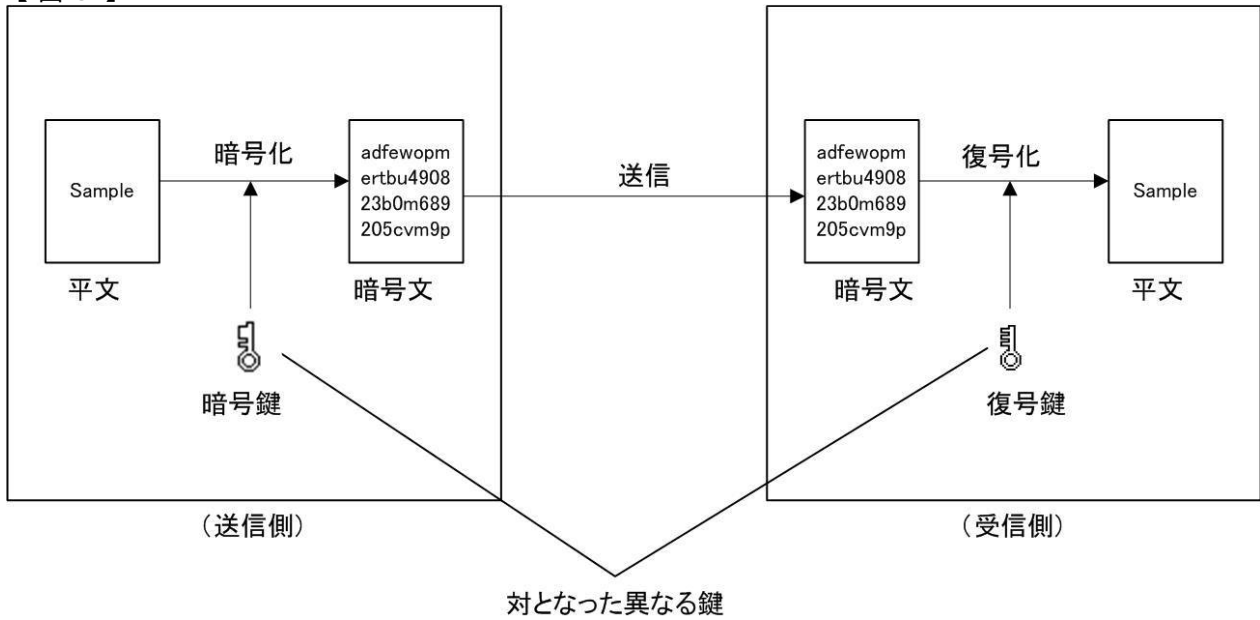


【図4】



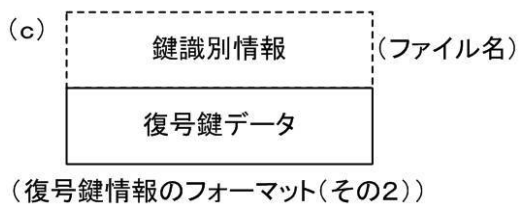
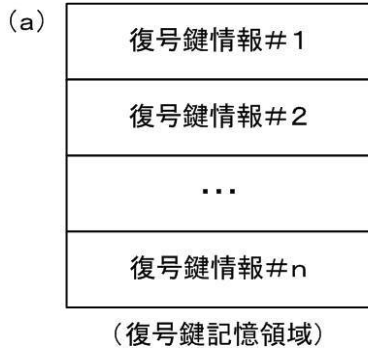
(共通鍵方式の暗号化方法)

【 図 5 】

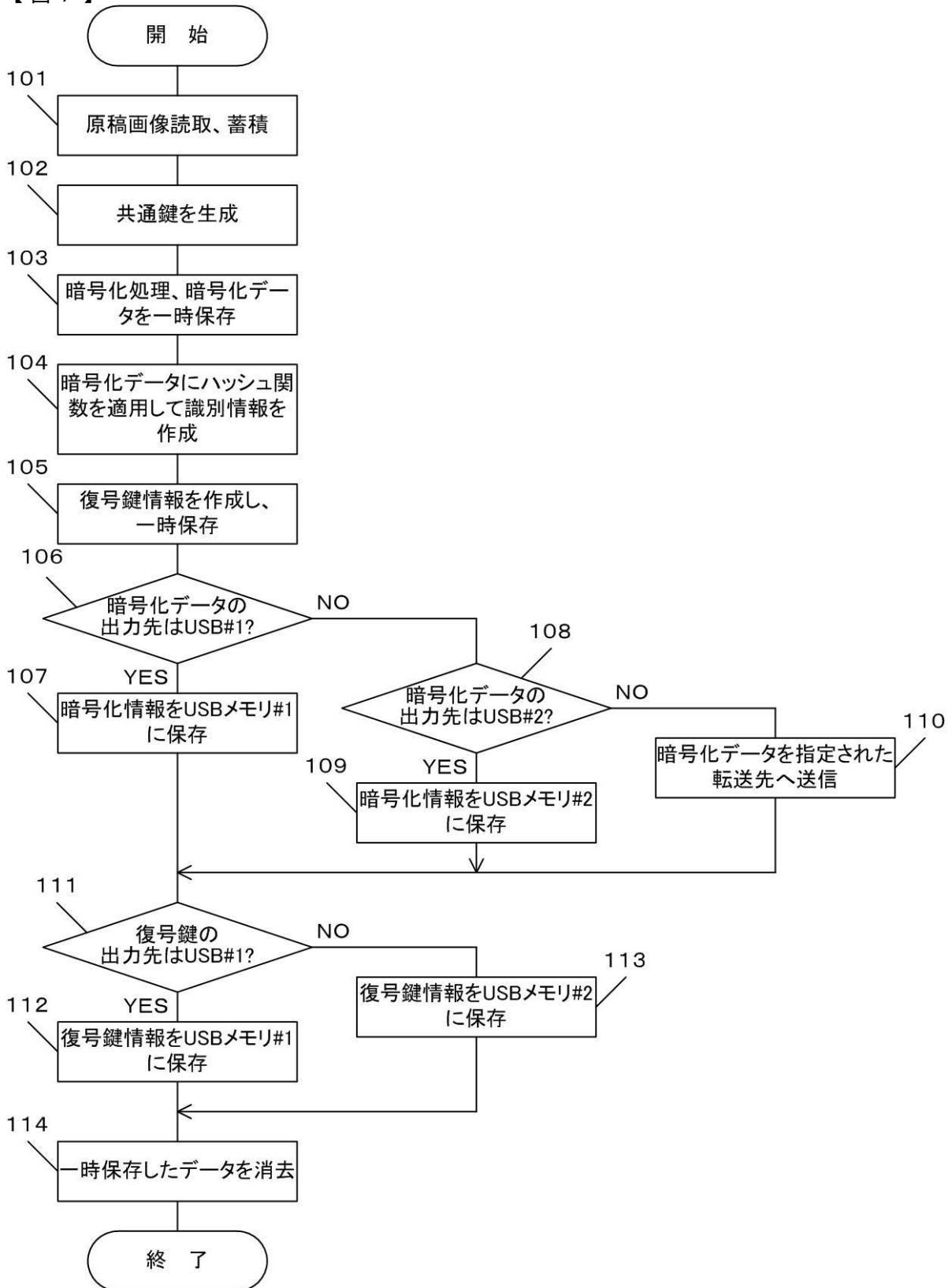


(暗号鍵と復号鍵を用いた暗号化方法(公開鍵方式が基礎))

【 図 6 】



【 図 7 】

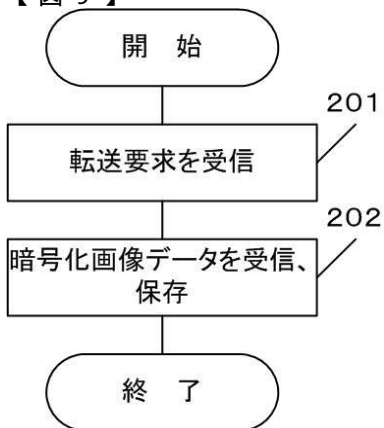


【図8】

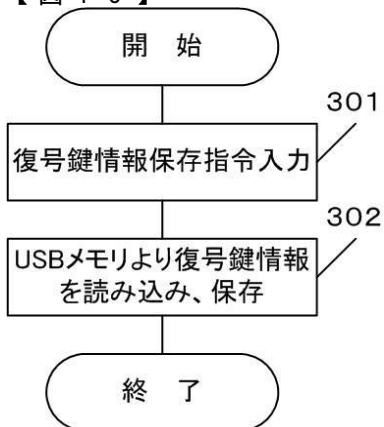


(出力先選択画面)

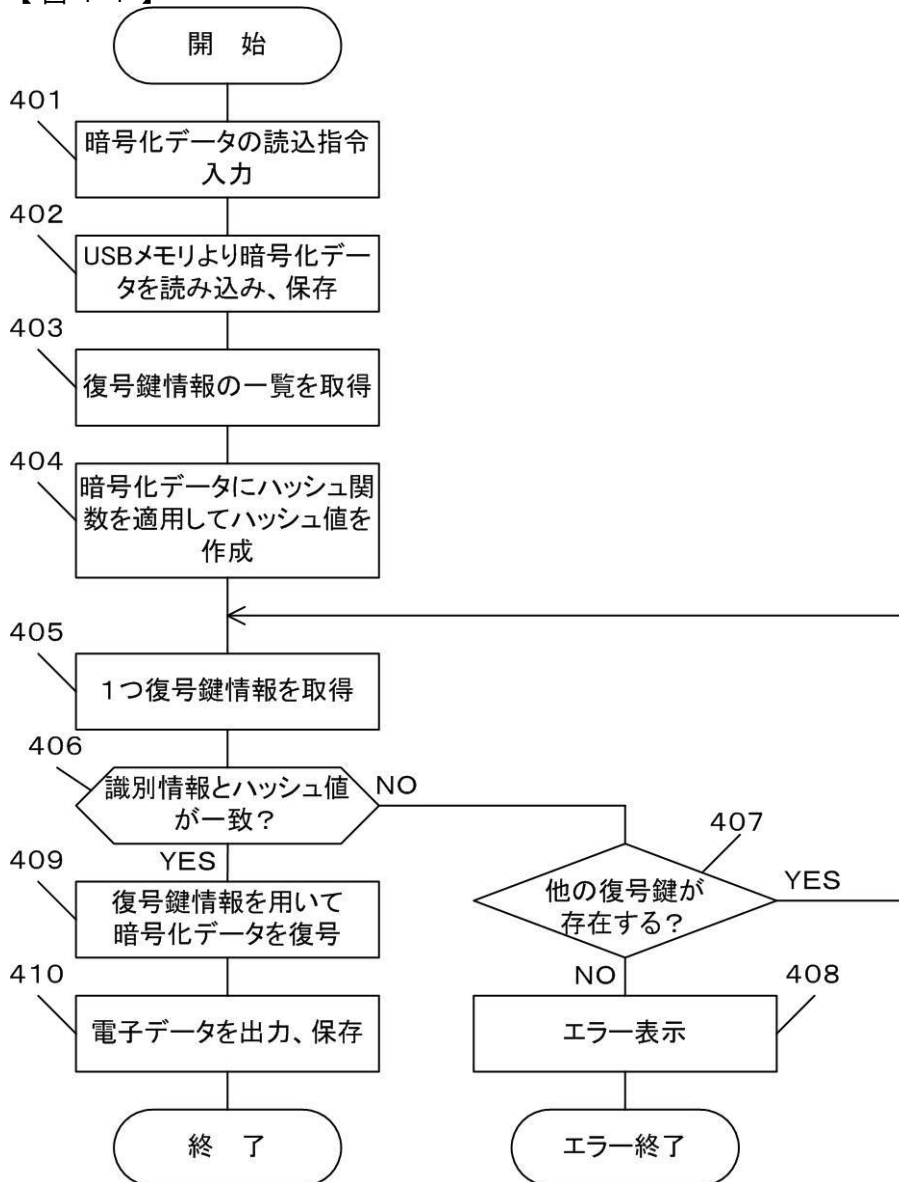
【図9】



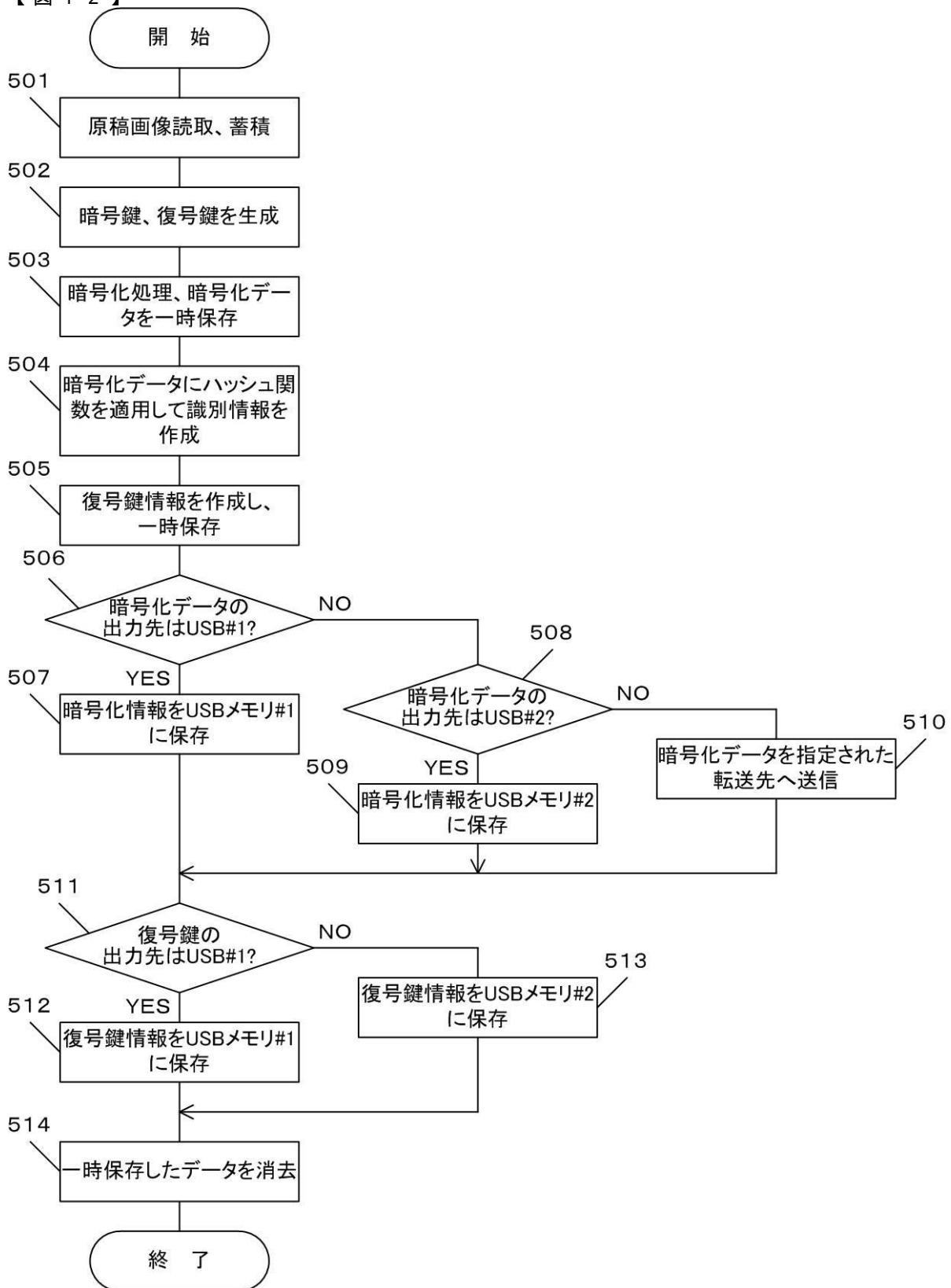
【図10】



【図11】



【 図 1 2 】



フロントページの続き

(72)発明者 黒子 岳人

東京都大田区中馬込 1 丁目 3 番 6 号 株式会社リコー内

Fターム(参考) 5J104 AA16 EA04 EA15 EA16 JA03 JA21 NA02 NA27 NA37 PA14