(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4698261号
(P4698261)
(45)発行日　平成23年6月8日(2011.6.8)　(24)登録日　平成23年3月11日(2011.3.11)

(51)Int.Cl.　F I
H04L 9/08 (2006.01)　H04L 9/00 601A

請求項の数 27　(全 33 頁)

(21)出願番号　特願2005-88054(P2005-88054)
(22)出願日　平成17年3月25日(2005.3.25)
(65)公開番号　特開2006-270718(P2006-270718A)
(43)公開日　平成18年10月5日(2006.10.5)
審査請求日　平成18年10月12日(2006.10.12)

(73)特許権者　000232140
ＮＥＣフィールディング株式会社
東京都港区三田１丁目４番２８号
(74)代理人　100109313
弁理士　机　昌彦
(74)代理人　100121290
弁理士　木村　明隆
(74)代理人　100160554
弁理士　浅井　俊雄
(72)発明者　飯村　健
東京都港区三田一丁目４番２８号
ＮＥＣフィールディング株式会社内

審査官　新田　亮

最終頁に続く

(54)【発明の名称】暗号通信システムと方法、及びプログラム

(57)【特許請求の範囲】
【請求項１】
データを送受信する装置が、通信手段と暗号処理手段を備え、前記通信手段は送信部と受信部を備え、前記暗号処理手段は、画像ファイルと前記画像ファイルの画像データ上の範囲指定情報を受け、前記範囲指定情報が示す指定範囲の画素値を加工しキーを作成するキー作成手段と、対象データに前記キーの値に対応する暗号処理を施す暗号化手段と、暗号化された前記対象データに前記キーの値に対応する逆処理を施す復号手段と、前記画像ファイルを取得し、前記範囲指定情報を生成し、これらを前記キー作成手段に渡し、作成された前記キーと前記対象データのファイルを前記暗号化手段に渡し、暗号化された前記ファイルを受け、これに前記画像ファイルと前記範囲指定情報とを付して前記送信部を通じ送信する手段と、前記受信部が受信した暗号化されたファイルと画像ファイルと範囲指定情報を受け、前記受信した画像ファイルと前記受信した範囲指定情報を前記キー作成手段に渡し、作成されたキーと暗号化されたファイルを前記復号手段に渡し復号させる手段とを備えることを特徴とする暗号通信システム。
【請求項２】
データを送受信する装置が、通信手段と暗号処理手段を備え、前記通信手段は送信部と受信部を備え、前記暗号処理手段は、画像ファイルと前記画像ファイルの画像データ上の範囲指定情報を受け、前記範囲指定情報が示す指定範囲の画素値を加工しキーを作成するキー作成手段と、対象データに前記キーの値に対応する暗号処理を施す暗号化手段と、暗号化された前記対象データに前記キーの値に対応する逆処理を施す復号手段と、画像ファイ

ルを取得し、前記範囲指定情報を生成し、これらを前記キー作成手段に渡し、作成された前記キーと前記対象データのファイルを前記暗号化手段に渡し、暗号化された前記ファイルを受け、範囲指定情報を前記画像ファイルに埋め込み、これを暗号化された前記ファイルに付し前記送信部を通じ送信する手段と、前記受信部が受信した暗号化されたファイルと画像ファイルを受け、前記受信した画像ファイルから範囲指定情報を抽出し、前記受信した画像ファイルと前記抽出した範囲指定情報を前記キー作成手段に渡し、作成されたキーと前記受信した暗号化されたファイルを前記復号手段に渡し復号させる手段とを備えることを特徴とする暗号通信システム。

【請求項３】

データを送受信する装置とこれが接続されるネットワーク上のサーバ装置を含み、前記サーバ装置には画像ファイルを有し、前記データを送受信する装置が、通信手段と暗号処理手段を備え、前記通信手段は送信部と受信部と暗号処理インタフェース部を備え、前記暗号処理インタフェース部が、前記送信部から暗号化を指示されると、画像ファイルの格納場所記憶を参照し、前記サーバより画像ファイルを取得し、これを用いた送信対象ファイルの暗号化を前記暗号処理手段に指示し、暗号化されたファイルと画像ファイルと画像データ上の範囲指定情報とを送信部に返す手段と、前記受信部から暗号化されたファイルと画像ファイルと前記範囲指定情報とを受け、暗号化されたファイルの復号を前記暗号処理手段に指示する手段とを有し、前記暗号処理手段は、画像ファイルと前記範囲指定情報を受け、前記範囲指定情報が示す指定範囲の画素値を加工しキーを作成するキー作成手段と、前記送信対象ファイルのデータに前記キーの値に対応する暗号処理を施す暗号化手段と、暗号化されたデータに前記データのために作成されたキーの値に対応する逆処理を施す復号手段と、暗号化指示を受け前記範囲指定情報を生成し、前記範囲指定情報と前記画像ファイルをキー作成手段に送ってキーを作成させ、前記キーによる前記送信対象ファイルの暗号化を前記暗号化手段に行わせ、暗号化された前記送信対象ファイルに前記範囲指定情報を付し前記暗号処理インタフェース部に返す手段と、復号指示を受け、画像ファイルと前記画像ファイルの範囲指定情報とを、キー作成手段に送ってキーを作成させ、前記作成したキーにより暗号化された受信ファイルの復号を前記復号手段に行わせ復号された前記受信ファイルを前記暗号処理インタフェース部に返す手段を備えることを特徴とする暗号通信システム。

【請求項４】

データを送受信する装置とこれが接続されるネットワーク上のサーバ装置を含み、前記サーバ装置には画像ファイルを有し、前記データを送受信する装置が、通信手段と暗号処理手段を備え、前記通信手段は送信部と受信部と暗号処理インタフェース部を備え、前記暗号処理インタフェース部が、前記送信部から暗号化を指示されると、画像ファイルの格納場所記憶を参照し、前記サーバより画像ファイルを取得し、これを用いた送信対象ファイルの暗号化を前記暗号処理手段に指示し、暗号化されたファイルと、画像データ上の範囲指定情報が埋め込まれた画像ファイルとを前記送信部に返す手段と、前記受信部から暗号化されたファイルと前記範囲指定情報が埋め込まれた画像ファイルとを受け、暗号化されたファイルの復号を前記暗号処理手段に指示する手段とを有し、前記暗号処理手段は、画像ファイルと前記範囲指定情報を受け、前記範囲指定情報が示す指定範囲の画素値を加工しキーを作成するキー作成手段と、前記送信対象ファイルのデータに前記キーの値に対応する暗号処理を施す暗号化手段と、暗号化されたデータに前記データのために作成されたキーの値に対応する逆処理を施す復号手段と、暗号化指示を受け、前記範囲指定情報を生成し、前記範囲指定情報と前記画像ファイルをキー作成手段に送ってキーを作成させ、前記キーによる前記送信対象ファイルの暗号化を前記暗号化手段に行わせ、前記範囲指定情報を前記画像ファイルに埋め込み、前記画像ファイルを暗号化された前記送信対象ファイルに付し前記暗号処理インタフェース部に返す手段と、復号指示を受け、受信した画像ファイルから範囲指定情報を抽出し前記抽出した範囲指定情報と前記受信した画像ファイルを、前記キー作成手段に送ってキーを作成させ、前記作成したキーにより暗号化された受信ファイルの復号を前記復号手段に行わせ、復号された前記受信ファイルを前記暗号処理

インタフェース部に返す手段を備えることを特徴とする暗号通信システム。
【請求項５】
データを送受信する装置とこれが接続されるネットワーク上のファイルサーバ装置及びアプリケーションサーバ装置を含み、前記ファイルサーバ装置は画像ファイルを有し、前記アプリケーションサーバ装置は暗号処理手段を有し、前記データを送受信する装置が、送信部と受信部と暗号処理インタフェース部を備え、前記暗号処理インタフェース部が、前記送信部から暗号化を指示されると、画像ファイル、暗号処理手段の各格納先を示す格納場所記憶を参照し、前記ファイルサーバより画像ファイルを取得し、これを用いた送信対象ファイルの暗号化を前記アプリケーションサーバ装置の暗号処理手段に指示し、暗号化されたファイルと画像ファイルと画像データ上の範囲指定情報とを送信部に返す手段と、前記受信部から暗号化されたファイルと前記画像ファイルと前記範囲指定情報とを受け、暗号化されたファイルの復号を前記暗号処理手段に指示する手段とを有し、前記暗号処理手段は、前記画像ファイルと前記範囲指定情報を受け、前記範囲指定情報が示す指定範囲の画素値を加工しキーを作成するキー作成手段と、前記送信対象ファイルのデータに前記キーの値に対応する暗号処理を施す暗号化手段と、暗号化されたデータに前記データのために作成されたキーの値に対応する逆処理を施す復号手段と、暗号化指示を受け、前記範囲指定情報を生成し、前記範囲指定情報と前記画像ファイルを前記キー作成手段に送ってキーを作成させ、前記作成したキーにより前記送信対象ファイルの暗号化を前記暗号化手段に行わせ、暗号化されたファイルに前記範囲指定情報を付し前記暗号処理インタフェース部に返す手段と、復号指示を受け、受信した画像ファイルと範囲指定情報を前記キー作成手段に送ってキーを作成させ、前記作成したキーにより暗号化された受信ファイルの復号を前記復号手段に行わせ、復号された前記受信ファイルを前記暗号処理インタフェース部に返す手段とを備えることを特徴とする暗号通信システム。
【請求項６】
データを送受信する装置とこれが接続されるネットワーク上のファイルサーバ装置及びアプリケーションサーバ装置を含み、前記ファイルサーバ装置は画像ファイルを有し、前記アプリケーションサーバ装置は暗号処理手段を有し、前記データを送受信する装置が送信部と受信部と暗号処理インタフェース部を備え、前記暗号処理インタフェース部が、前記送信部から暗号化を指示されると、画像ファイル、暗号処理手段の各格納先を示す格納場所記憶を参照し、前記ファイルサーバより画像ファイルを取得し、これを用いた送信対象ファイルの暗号化を前記アプリケーションサーバ装置の暗号処理手段に指示し、暗号化されたファイルと、画像データ上の範囲指定情報が埋め込まれた画像ファイルとを前記送信部に返す手段と、前記受信部から暗号化されたファイルと前記画像ファイルとを受け、暗号化されたファイルの復号を前記暗号処理手段に指示する手段とを有し、前記暗号処理手段は、前記画像ファイルと前記範囲指定情報を受け、前記範囲指定情報が示す指定範囲の画素値を加工しキーを作成するキー作成手段と、前記送信対象ファイルのデータに前記キーの値に対応する暗号処理を施す暗号化手段と、暗号化されたデータに前記データのために作成されたキーの値に対応する逆処理を施す復号手段と、暗号化指示を受け、前記範囲指定情報を生成し、前記範囲指定情報と前記画像ファイルを前記キー作成手段に送ってキーを作成させ、前記作成したキーにより前記送信対象ファイルの暗号化を前記暗号化手段に行わせ、前記範囲指定情報を前記画像ファイルに埋め込み、前記画像ファイルを暗号化された前記送信対象ファイルに付し前記暗号処理インタフェース部に返す手段と、復号指示を受け、受信した画像ファイルより範囲指定情報を抽出し、前記抽出した範囲指定情報と前記受信した画像ファイルを前記キー作成手段に送ってキーを作成させ、前記作成したキーにより暗号化された受信ファイルの復号を前記復号手段に行わせ、復号された前記受信ファイルを前記暗号処理インタフェース部に返す手段を備えることを特徴とする暗号通信システム。
【請求項７】
データを送受信する装置とこれとネットワーク接続されたサーバ装置を含み、前記サーバ装置は認証手段とユーザ情報記憶部とキー作成手段を有し、前記データを送受信する装置

が、前記サーバ装置の前記認証手段より認証用情報を要求されると、ユーザＩＤと画像ファイルと画像データ上の範囲指定情報を送信する手段を有し、前記キー作成手段が、画像ファイルと前記範囲指定情報を受け、指定範囲の画素値を加工しキーを作成し、前記認証手段は、受信した画像ファイルと前記範囲指定情報を前記キー作成手段に渡し、作成されたキーが、前記ユーザＩＤに対応したパスワードとして、前記ユーザ情報記憶部に登録されていることを確認し認証することを特徴とする暗号通信システム。

【請求項８】

データを送受信する装置とこれとネットワーク接続されたサーバ装置を含み、前記サーバ装置には認証手段とユーザ情報記憶部とキー作成手段を有し、前記データを送受信する装置が、前記サーバ装置の認証手段より認証用情報を要求されると、ユーザＩＤと、画像データ上の範囲指定情報が埋め込まれた画像ファイルとを送信する手段を有し、前記キー作成手段は、前記画像ファイルから前記範囲指定情報を抽出し、指定範囲の画素値を加工しキーを作成し、前記認証手段が、受信した画像ファイルを前記キー作成手段に渡し、作成されたキーが、前記ユーザＩＤに対応したパスワードとして、前記ユーザ情報記憶部に登録されていることを確認し認証することを特徴とする暗号通信システム。

【請求項９】

データを送受信する装置のキー作成部が画像ファイルと前記画像ファイルの画像データ上の範囲指定情報を受け、前記範囲指定情報が示す指定範囲の画素値を加工しキーを作成するキー作成ステップと、データを送受信する装置のデータ暗号化部が対象データに前記キーの値に対応する暗号処理を施す暗号化ステップと、データを送受信する装置のデータ復号部が暗号化された前記対象データに前記キーの値に対応する逆処理を施す復号ステップと、データを送受信する装置の主処理部が前記画像ファイルを取得し、前記範囲指定情報を生成し、これらを前記キー作成ステップに渡し、作成された前記キーと前記対象データのファイルを前記暗号化部に渡し、暗号化された前記ファイルを受けて前記データを送受信する装置の送信部に渡し、前記送信部が前記暗号化されたファイルに前記画像ファイルと前記範囲指定情報とを付して送信するステップと、前記データを送受信する装置の受信部が受信した暗号化されたファイルと画像ファイルと範囲指定情報を受け、前記主処理部に送り、前記主処理部が前記受信した画像ファイルと範囲指定情報を前記キー作成部に渡し、作成されたキーと前記受信した暗号化されたファイルとを前記データ復号部に渡し、前記データ復号部が前記受信した暗号化されたファイルを復号するステップとを、前記データを送受信する装置としてのコンピュータに実行させるためのプログラム。

【請求項１０】

データを送受信する装置のキー作成部が画像ファイルと画像データ上の範囲指定情報を受け、指定範囲の画素値を加工しキーを作成するキー作成ステップと、データを送受信する装置のデータ暗号化部がデータに前記キーの値に対応する暗号処理を施す暗号化ステップと、データを送受信する装置のデータ復号部が暗号化されたデータに前記キーの値に対応する逆処理を施す復号ステップと、データを送受信する装置の主処理部が前記画像ファイルを取得し、前記範囲指定情報を生成し、これらを前記キー作成ステップに渡し、作成された前記キーと前記対象データのファイルを前記暗号化部に渡し、暗号化された前記ファイルを受け、前記範囲指定情報を画像ファイルに埋め込み、前記データを送受信する装置の送信部に渡し、前記送信部が前記画像ファイルを暗号化されたファイルに付し送信するステップと、前記データを送受信する装置の受信部が受信した暗号化されたファイルと画像ファイルを受け、前記データを送受信する装置の主処理部に送り、前記主処理部が前記受信した画像ファイルから範囲指定情報を抽出し、前記受信した画像ファイルと前記抽出した範囲指定情報を前記キー作成部に渡し、作成されたキーと前記受信した暗号化されたファイルを前記復号部に渡し、前記データ復号部が前記受信した暗号化されたファイルを復号するステップとを、前記データを送受信する装置としてのコンピュータに実行させるためのプログラム。

【請求項１１】

データを送受信する装置における送信部がデータを送信する送信ステップと、前記装置に

おける受信部がデータを受信する受信ステップと、前記装置における暗号処理インタフェース部が、前記送信部から暗号化を指示されると、画像ファイルの格納場所記憶を参照し、ネットワーク接続されたサーバより画像ファイルを取得し、これを用いた送信対象ファイルの暗号化を前記装置における暗号処理部に指示し、暗号化されたファイルと画像ファイルと前記画像ファイルの画像データ上の範囲指定情報とを前記送信部に返すステップと、前記受信部から暗号化されたファイルと画像ファイルと前記範囲指定情報とを受け、暗号化されたファイルの復号を前記暗号処理部に指示するステップとを含む暗号処理インタフェースステップと、前記暗号処理部が、前記画像ファイルと前記画像ファイルの画像データ上の範囲指定情報を受け、指定範囲の画素値を加工し、前記暗号処理部内のキー作成部にてキーを作成するキー作成ステップと、データに前記キーの値に対応する暗号処理を前記暗号処理部内の暗号化部にて施す暗号化ステップと、暗号化されたデータに前記キーの値に対応する逆処理を前記暗号処理部内の復号化部にて施す復号ステップと、前記暗号処理部内の主処理部が暗号化指示を受け、前記範囲指定情報を生成し、これと前記画像ファイルを伴い、前記キー作成部にキーを作成させ、これによる送信対象ファイルの暗号化を前記暗号化部に行わせ、暗号化されたファイルに前記範囲指定情報を付し前記暗号処理インタフェース部に返すステップと、復号指示を受け、前記受信部が受信した画像ファイルと範囲指定情報を前記キー作成部に送り、前記キー作成部にキーを作成させ、これによる暗号化された受信ファイルの復号を前記復号部に行わせ、復号された前記受信ファイルを前記暗号処理インタフェース部に返すステップを含む暗号処理ステップとを、前記データを送受信する装置としてのコンピュータに実行させるためのプログラム。

【請求項１２】

データを送受信する装置における送信部がデータを送信する送信ステップと、前記装置における受信部がデータを受信する受信ステップと、前記装置における暗号処理インタフェース部が、前記送信部から暗号化を指示されると、画像ファイルの格納場所記憶を参照し、

ネットワーク接続されたサーバより画像ファイルを取得し、これを用いた送信対象ファイルの暗号化を前記装置における暗号処理部に指示し、暗号化されたファイルと画像データ上の範囲指定情報が埋め込まれた画像ファイルとを前記送信部に返すステップと、前記受信部から暗号化されたファイルと前記範囲指定情報が埋め込まれた画像ファイルとを受け、

暗号化されたファイルの復号を前記暗号処理部に指示するステップとを含む暗号処理インタフェースステップと、前記暗号処理部が前記画像ファイルと前記範囲指定情報を受け、指定範囲の画素値を加工し、前記暗号処理部内のキー作成部にてキーを作成するキー作成ステップと、データに前記キーの値に対応する暗号処理を前記暗号処理部内の暗号化部にて施す暗号化ステップと、暗号化されたデータに前記キーの値に対応する逆処理を
前記暗号処理部内の復号化部にて施す復号ステップと、前記暗号処理部内の主処理部が暗号化指示を受け、前記範囲指定情報を生成し、これと前記画像ファイルを伴い、前記キー作成部にキーを作成させ、これによる送信対象ファイルの暗号化を前記暗号化部に行わせ、暗号化されたファイルに前記範囲指定情報を埋め込んだ画像ファイルを付し前記暗号処理インタフェース部に返すステップと、復号指示を受け、前記受信部が受信した画像ファイルから範囲指定情報を抽出し、前記抽出した範囲指定情報と前記受信した画像ファイルを前記キー作成部に送り、前記キー作成部にキーを作成させ、これによる暗号化された受信ファイルの復号を前記復号部に行わせ、復号された前記受信ファイルを前記暗号処理インタフェース部に返すステップを含む暗号処理ステップとを、前記データを送受信する装置としてのコンピュータに実行させるためのプログラム。

【請求項１３】

データを送受信する装置における送信部がデータを送信する送信ステップと、前記装置における受信部がデータを受信する受信ステップと、前記装置における暗号処理インタフェース部が前記送信部から暗号化を指示されると、前記暗号処理インターフェース部が画像ファイル、暗号処理ステップの各格納先を示す格納場所記憶を参照し、ネットワーク接続

されたファイルサーバより画像ファイルを取得し、これを用いた送信対象ファイルの暗号化をネットワーク接続されたアプリケーションサーバ装置の暗号処理部に指示し、暗号化されたファイルと画像ファイルと画像データ上の範囲指定情報とを前記送信部に返すステップと、前記受信部から暗号化されたファイルと画像ファイルと前記範囲指定情報とを受け、暗号化されたファイルの復号を前記暗号処理部に指示するステップと、
復号されたファイルを受け取るステップを含む暗号処理インタフェースステップと、前記暗号処理部のキー作成部が、画像ファイルと前記範囲指定情報を受け、指定範囲の画素値を加工しキーを作成するステップと、前記暗号処理部の暗号化部が、データに前記キーの値に対応する暗号処理を施すステップと、前記暗号処理部の復号部が、暗号化されたデータに前記キーの値に対応する逆処理を施すステップと、前記暗号処理部の主処理部が、暗号化指示を受け、前記範囲指定情報を生成し、これと画像ファイルを伴い、前記キー作成部にキーを作成させ、これによる送信対象ファイルの暗号化を前記暗号化部に行わせ、暗号化されたファイルに前記範囲指定情報を付し前記暗号処理インタフェース部に返すステップと、復号指示を受け、画像ファイルと前記範囲指定情報を伴い、前記キー作成部にキーを作成させ、これによる暗号化された受信ファイルの復号を前記復号部に行わせ、
復号された受信ファイルを前記暗号処理インタフェース部に返すステップとを、前記データを送受信する装置としてのコンピュータに実行させるためのプログラム。

【請求項１４】

データを送受信する装置の送信部がデータを送信する送信ステップと、前記データを送受信する装置の受信部がデータを受信する受信ステップと、暗号処理インタフェース部が
画像ファイル、暗号処理ステップの格納先を示す格納場所記憶を参照し、ネットワーク接続されたファイルサーバより画像ファイルを取得し、これを用いた送信対象ファイルの暗号化をネットワーク接続されたアプリケーションサーバ装置の暗号処理部に指示し、暗号化されたファイルと画像データ上の範囲指定情報が埋め込まれた画像ファイルとを前記送信部に送信するステップと、前記受信部から暗号化されたファイルと前記範囲指定情報が埋め込まれた画像ファイルとを受け、前記暗号化されたファイルの復号を前記暗号処理部に指示するステップと、復号されたファイルを受け取るステップを含む暗号処理インタフェースステップと、前記暗号化処理部のキー作成部が、画像ファイルと前記範囲指定情報を受け、指定範囲の画素値を加工しキーを作成するステップと、前記暗号化処理部の暗号化部がデータに前記キーの値に対応する暗号処理を施すステップと、前記暗号化処理部の復号部が暗号化されたデータに前記キーの値に対応する逆処理を施すステップと、前記暗号化処理部の主処理部が暗号化指示を受け、前記範囲指定情報を生成し、これと画像ファイルを伴い、前記キー作成部にキーを作成させ、これによる送信対象ファイルの暗号化を前記暗号化部に行わせ、範囲指定情報を画像ファイルに埋め込み、これを暗号化されたファイルに付し前記暗号処理インタフェース部に返すステップと、復号指示を受け、画像ファイルより前記範囲指定情報を抽出し、これと画像ファイルを伴い、前記キー作成部にキーを作成させ、これによる暗号化された受信ファイルの復号を前記復号部に行わせ、復号された受信ファイルを前記暗号処理インタフェース部に返すステップとを、前記データを送受信する装置としてのコンピュータに実行させるためのプログラム。

【請求項１５】

データを送受信する装置に、これとネットワーク接続されているサーバ装置の認証部が認証用情報を要求するステップと、前記データを送受信する装置がユーザIDと画像ファイルと画像データ上の範囲指定情報とを前記サーバ装置に送るステップと、前記サーバが有するキー作成部が、前記データを送受信する装置が前記サーバに送信した前記画像ファイルと前記範囲指定情報とを受け、指定範囲の画素値を加工しキーを作成するキー作成ステップと、前記サーバが有する認証部が、作成された前記キーが、前記ユーザＩＤに対応したパスワードとして、前記サーバのユーザ情報記憶部に登録されていることを確認し、認証するステップとを、前記データを送受信する装置としてのコンピュータに実行させるためのプログラム。

【請求項１６】

データを送受信する装置に、これとネットワーク接続されているサーバ装置の認証部が認証用情報を要求するステップと、前記データを送受信する装置がユーザIDと画像データ上の範囲指定情報が埋め込まれた画像ファイルを前記サーバ装置に送るステップと、前記サーバが有するキー作成部が、前記データを送受信する装置が前記サーバに送信した前記画像ファイルを受け、前記範囲指定情報を抽出し前記範囲指定情報が示す指定範囲の画素値を加工しキーを作成するキー作成ステップと、前記サーバが有する認証部が、作成された前記キーが、前記ユーザＩＤに対応したパスワードとして、前記サーバのユーザ情報記憶部に登録されていることを確認し、認証するステップとを、前記データを送受信する装置としてのコンピュータに実行させるためのプログラム。

【請求項１７】

データを送受信する装置の、キー作成部が画像ファイルと前記画像ファイルの画像データ上の範囲指定情報を受け、前記指定範囲情報が示す指定範囲の画素値を加工しキーを作成するキー作成ステップと、前記データを送受信する装置のデータ暗号化部が対象データに前記キーの値に対応する暗号処理を施す暗号化ステップと、前記データを送受信する装置のデータ復号部が暗号化された前記対象データに前記キーの値に対応する逆処理を施す復号ステップと、前記データを送受信する装置の主処理部が前記画像ファイルを取得し、前記範囲指定情報を生成し、これらを前記キー作成部に渡し、作成された前記キーと前記対象データのファイルを前記暗号化部に渡し、暗号化された前記ファイルを受け、これに前記画像ファイルと前記範囲指定情報を付して前記データを送受信する装置の送信部を通じ送信するステップと、前記データを送受信する装置の受信部が受信した暗号化されたファイルと画像ファイルと範囲指定情報を受け、前記受信した画像ファイルと前記受信した範囲指定情報を前記キー作成部に渡し、作成されたキーと前記受信した暗号化されたファイルを前記復号部に渡し、復号させるステップと、を含むことを特徴とする暗号通信方法。

【請求項１８】

データを送受信する装置の、キー作成部が画像ファイルと前記画像ファイルの画像データ上の範囲指定情報を受け、前記指定範囲情報が示す指定範囲の画素値を加工しキーを作成するキー作成ステップと、対象データに前記キーの値に対応する暗号処理を施す暗号化ステップと、暗号化されたデータに前記キーの値に対応する逆処理を施す復号ステップと、前記データを送受信する装置の主処理部が前記画像ファイルを取得し、前記範囲指定情報を生成し、これらを前記キー作成部に渡し、作成された前記キーと前記対象データのファイルを前記暗号化部に渡し、暗号化された前記ファイルを受け、前記範囲指定情報を前記画像ファイルに埋め込み、これを暗号化された前記ファイルに付し送信するステップと、受信した暗号化されたファイルと画像ファイルを受け、前記受信した画像ファイルから範囲指定情報を抽出し、前記受信した画像ファイルと前記抽出した範囲指定情報を前記キー作成ステップに渡し、作成されたキーと前記受信した暗号化されたファイルを前記復号部に渡し復号させるステップとを含むことを特徴とする暗号通信方法。

【請求項１９】

データを送受信する装置における送信部がデータを送信する送信ステップと、前記データを送受信する装置における受信部がデータを受信する受信ステップと、前記データを送受信する装置における暗号処理インタフェース部が、前記送信部から暗号化を指示されると、

画像ファイルの格納場所記憶を参照し、ネットワーク接続されたサーバより画像ファイルを取得し、これを用いた送信対象のファイルの暗号化を前記データを送受信する装置における暗号処理部に指示し、暗号化された前記ファイルと前記画像ファイルと前記画像ファイルの画像データ上の範囲指定情報とを前記送信部に返すステップと、前記受信部から暗号化された前記ファイルと前記画像ファイルと前記範囲指定情報とを受け、暗号化された前記ファイルの復号を前記暗号処理部に指示するステップと、前記暗号処理部が、前記画像ファイルと、前記範囲指定情報を受け、指定範囲の画素値を加工し、前記暗号処理部内のキー作成部にてキーを作成するキー作成ステップと、前記送信対象のファイルに前記キーの値に対応する暗号処理を前記暗号処理部内の暗号化部にて施す暗号化ステップと、暗

号化された前記ファイルに前記キーの値に対応する逆処理を前記暗号処理部内の復号化部にて施す復号ステップと、暗号化指示を受け、前記範囲指定情報を生成し、前記範囲指定情報と前記画像ファイルを、前記キー作成部に送ってキーを作成させ、これによる送信対象ファイルの暗号化を前記暗号化部に行わせ、暗号化された前記ファイルに前記範囲指定情報を付し前記暗号処理インタフェースステップに返すステップと、復号指示を受け、前記画像ファイルと前記範囲指定情報を前記キー作成部に送ってキーを作成させ、これによる暗号化された受信ファイルの復号を前記復号部に行わせ、復号された前記受信ファイルを前記暗号処理インタフェース部に返すステップとを含むことを特徴とする暗号通信方法。

【請求項２０】

データを送受信する装置における送信部がデータを送信する送信ステップと、前記データを送受信する装置における受信部がデータを受信する受信ステップと、前記データを送受信する装置における暗号処理インタフェース部が、前記送信部から暗号化を指示されると、

画像ファイルの格納場所記憶を参照し、ネットワーク接続されたサーバより画像ファイルを取得し、これを用いた送信対象のファイルの暗号化を前記データを送受信する装置における暗号処理部に指示し、暗号化された前記ファイルと前記画像ファイルの画像データ上の範囲指定情報が埋め込まれた画像ファイルとを前記送信部に返すステップと、前記受信部から暗号化された前記ファイルと前記範囲指定情報が埋め込まれた画像ファイルとを受け、暗号化された前記ファイルの復号を前記暗号処理部に指示するステップとを含む暗号処理インターフェースステップと、前記暗号処理部が前記画像ファイルと、前記範囲指定情報を受け、指定範囲の画素値を加工し、前記暗号処理部内のキー作成部にてキーを作成するキー作成ステップと、前記送信対象のファイルに前記キーの値に対応する暗号処理を前記暗号処理部内の暗号化部にて施す暗号化ステップと、暗号化された前記送信対象のファイルのデータに前記キーの値に対応する逆処理を前記暗号処理部内の復号部にて施す復号ステップと、前記暗号処理部内の主処理部が暗号化指示を受け、前記範囲指定情報を生成し、これと前記画像ファイルを前記キー作成部に送って、キーを作成させ、前記キーによる前記送信対象のファイルの暗号化を前記暗号化部に行わせ、暗号化された前記送信対象のファイルに、前記範囲指定情報を埋め込んだ前記画像ファイルを付し、暗号処理インタフェースステップに返すステップと、復号指示を受け、前記受信部が受信した画像ファイルから範囲指定情報を抽出し、受信した画像ファイルと前記抽出した範囲指定情報とを前記キー作成部に送って、キーを作成させ、これによる暗号化された受信ファイルの復号を前記復号ステップに行わせ、復号された前記受信ファイルを前記暗号処理インタフェースステップに返すステップとを含むことを特徴とする暗号通信方法。

【請求項２１】

データを送受信する装置における送信部がデータを送信する送信ステップと、前記データを送受信する装置における受信部がデータを受信する受信ステップと、前記データを送受信する装置における暗号処理インタフェース部が前記送信部から暗号化を指示されると、前記暗号処理インターフェース部が、画像ファイル、暗号処理ステップの各格納先を示す格納場所記憶を参照し、ネットワーク接続されたファイルサーバより画像ファイルを取得し、これを用いた送信対象ファイルの暗号化をネットワーク接続されたアプリケーションサーバ装置の暗号処理部に指示し、暗号化されたファイルと画像ファイルと画像データ上の範囲指定情報とを前記送信部に返すステップと、前記受信部から暗号化されたファイルと画像ファイルと前記範囲指定情報とを受け、暗号化されたファイルの復号を暗号処理ステップに指示するステップと、前記暗号処理部のキー作成部が、画像ファイルと前記範囲指定情報を受け、指定範囲の画素値を加工しキーを作成するキー作成ステップと、前記暗号処理部の暗号化部が、前記送信対象のファイルに前記キーの値に対応する暗号処理を施すステップと、前記暗号処理部の復号部が、暗号化されたデータに前記キーの値に対応する逆処理を施すステップと、前記暗号処理部の主処理部が、暗号化指示を受け、前記範囲指定情報を生成し、前記範囲指定情報と画像ファイルを前記キー作成部に送って、キーを

作成させ、これによる前記送信対象のファイルの暗号化を前記暗号化部に行わせ、暗号化された前記ファイルに前記範囲指定情報を付し前記暗号処理インタフェース部に返すステップと、復号指示を受け、画像ファイルと範囲指定情報を前記キー作成部に送ってキーを作成させ、これによる暗号化された受信ファイルの復号を前記復号部に行わせ、復号された受信ファイルを前記暗号処理インタフェース部に返すステップとを含むことを特徴とする暗号通信方法。

【請求項２２】

データを送受信する装置の送信部がデータを送信する送信ステップと、前記データを送受信する装置の受信部がデータを受信する受信ステップと、前記データを送受信する装置における暗号処理インタフェース部が前記送信部から暗号化を指示されると、前記暗号処理インターフェース部が、画像ファイル、暗号処理ステップの格納先を示す格納場所記憶を参照し、ネットワーク接続されたファイルサーバより画像ファイルを取得し、これを用いた送信対象のファイルの暗号化をネットワーク接続されたアプリケーションサーバ装置の暗号処理部に指示し、暗号化されたファイルと画像データ上の範囲指定情報が埋め込まれた画像ファイルとを前記送信部に送信するステップと、前記受信部から暗号化されたファイルと前記範囲指定情報が埋め込まれた画像ファイルとを受け、前記暗号化されたファイルの復号を前記暗号処理部に指示するステップと、前記暗号化処理部のキー作成部が、画像ファイルと前記範囲指定情報を受け、指定範囲の画素値を加工しキーを作成するステップと、前記暗号化処理部の暗号化部が前記送信対象のファイルに前記キーの値に対応する暗号処理を施すステップと、前記暗号化処理部の復号部が暗号化されたデータに前記キーの値に対応する逆処理を施す復号部と、前記暗号化処理部の主処理部が暗号化指示を受け、前記範囲指定情報を生成し、前記範囲指定情報と画像ファイルを前記キー作成部に送って、キーを作成させ、これによる前記送信対象のファイルの暗号化を前記暗号化部に行わせ、前記範囲指定情報を画像ファイルに埋め込み、これを暗号化されたファイルに付し前記暗号処理インタフェース部に返すステップと、復号指示を受け、画像ファイルより前記範囲指定情報を抽出し、これと画像ファイルとを前記キー作成部に送ってキーを作成させ、これによる暗号化された受信ファイルの復号を前記復号部に行わせ、復号された受信ファイルを前記暗号処理インタフェース部に返すステップとを含むことを特徴とする暗号通信方法。

【請求項２３】

データを送受信する装置に、これとネットワーク接続されているサーバ装置の認証部が認証用情報を要求するステップと、前記データを送受信する装置がユーザＩＤと画像ファイルと画像データ上の範囲指定情報とを前記サーバ装置に送るステップと、前記サーバが有するキー作成部が、前記データを送受信する装置が前記サーバに送信した画像ファイルと画像データ上の範囲指定情報を受け、前記範囲指定情報が示す指定範囲の画素値を加工しキーを作成するキー作成ステップと、前記サーバが有する認証部が、作成された前記キーが、前記ユーザＩＤに対応したパスワードとして、前記サーバのユーザ情報記憶部に登録されていることを確認し、認証するステップとを含むことを特徴とする暗号通信方法。

【請求項２４】

データを送受信する装置に、これとネットワーク接続されているサーバ装置の認証部が認証用情報を要求するステップと、前記データを送受信する装置がユーザＩＤと画像データ上の範囲指定情報が埋め込まれた画像ファイルとを前記サーバ装置に送るステップと、前記サーバが有するキー作成部が、前記データを送受信する装置が前記サーバに送信した前記画像データ上の範囲指定情報が埋め込まれた画像ファイルを受け、前記画像ファイルから前記範囲指定情報を抽出し、前記範囲指定情報が示す指定範囲の画素値を加工しキーを作成するキー作成ステップと、前記サーバが有する認証部が、作成された前記キーが、前記ユーザＩＤに対応したパスワードとして、前記サーバのユーザ情報記憶部に登録されていることを確認し、認証するステップとを含むことを特徴とする暗号通信方法。

【請求項２５】

送信データを暗号化して送信側機器からネットワークを介して相手先受信機器に送信する

暗号通信方法において、前記送信側機器の有するキー作成部が任意の画像ファイルにおける画像データの任意の範囲を指定し、この指定された範囲の画像データから暗号化キーを作成するステップと、前記送信側機器の有する暗号化部が前記送信データを前記暗号化キーにより暗号化し、暗号化送信データを作成するステップと、前記送信側機器の有する送信部がこの暗号化送信データと前記画像ファイルと前記範囲を示す範囲指定情報とを送信側機器から相手先受信機器に送信するステップと、を備えることを特徴とする暗号通信方法。

【請求項２６】

暗号化された送信データを送信側機器からネットワークを介して受信する暗号通信方法において、前記送信側機器の有する受信部が暗号化された送信データと共に画像ファイルとこのファイルにおける画像データの範囲を指定する範囲指定情報を前記ネットワークから受信するステップと、前記送信側機器の有するキー作成部が受信した前記画像ファイルと前記範囲指定情報とから復号化キーを作成するステップと、前記送信側機器の有する復号部がこの復号化キーにより前記暗号化された送信データを復号するステップと、を備えたことを特徴とする暗号通信方法。

【請求項２７】

送信データを暗号化して送信側機器からネットワークを介して受信側機器に送信し、受信側機器にて復号する暗号通信方法において、前記送信側機器が有するキー作成部が、任意の画像ファイルにおける画像データの任意の範囲を指定し、前記範囲の画像データから暗号化キーを作成するステップと、前記送信側機器が有する暗号化部が、前記送信データを前記暗号化キーにより暗号化し、暗号化送信データを作成するステップと、前記送信側機器が有する送信部が、この暗号化送信データと前記画像ファイルと前記範囲を示す範囲指定情報とを送信側機器からネットワークに送信するステップと、前記送信側機器が有する受信部が、ネットワークから前記暗号化送信データと前記画像ファイルと前記範囲指定情報を受信するステップと、前記送信側機器が有するキー作成部が、受信した前記画像ファイルと前記範囲指定情報とから復号化キーを作成するステップと、前記送信側機器が有する復号部が、この復号化キーにより前記暗号化された送信データを復号するステップと、を備えたことを特徴とする暗号通信方法。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は暗号通信システムと方法、及びプログラムに関し、特に、画像の一部の色情報を利用した暗号通信システムと方法、及びプログラムに関する。

【背景技術】

【０００２】

現在、ファイルの暗号化方式には、共通鍵暗号方式（対称アルゴリズム）と公開鍵暗号方式（非対称アルゴリズム）の二つの方式が存在する。

【０００３】

共通鍵暗号方式とは、送信者(暗号を行う側)と受信者（暗号を受け取って解読する側）が同じ鍵を使う方式である。

【０００４】

この共通鍵暗号方式では、暗号と解読に同じ鍵を使用するため、高速な処理を行うことができる。

【０００５】

公開鍵暗号方式とは、暗号化する際に使用する鍵（公開鍵）と解読に使用する鍵（秘密鍵）がそれぞれ違う鍵を使用する方式である。

【０００６】

また、予め乱数文を作り、その乱数文を共有鍵暗号や公開鍵暗号を用いて、暗号通信を行う双方に配布しておき、その乱数文を鍵にしてｏｎｅ－ｔｉｍｅ　ｐａｄを用いて通信文を送信・受信する暗号処理が提案されている（特許文献１参照。）。

【０００７】
【特許文献１】特開２００３－２８３４８７号公報（第１ページ）
【発明の開示】
【発明が解決しようとする課題】
【０００８】
上記共通鍵暗号方式では、第三者に鍵が漏れてしまえば、暗号を解読されてしまう危険性があり、また多数の相手に対して暗号化を行う場合、暗号化する鍵を相手の数だけ用意する必要があり、鍵の管理等に手間がかかるという課題がある。
【０００９】
公開鍵暗号方式では、解読するための秘密鍵を自分で保管し、暗号化する公開鍵を公開するので、多数の相手とのやり取りを行う場合でも、自分の秘密鍵だけを保管しておけば良いので鍵の管理も容易である。
【００１０】
しかし、アルゴリズムが非対称であるため複雑な処理が多く、処理時間が長くなるという課題がある。
【００１１】
前記乱数文を鍵にする暗号処理では、乱数文を共有鍵暗号や公開鍵暗号を用いて配布する必要があるという課題がある。
【００１２】
この様に、それぞれの方式には長所と課題がある。
【００１３】
本発明の目的は、安全に相手に鍵を渡すことができ、鍵をいくつも用意しなくてもよく、鍵を盗まれても大丈夫であり、パスワードの様に長い複雑な文字を覚えなくてもよく、少ない処理時間で済み手軽に採用できるという、それぞれの方式の長所を兼ね備えた暗号通信システムを提供することにある。
【課題を解決するための手段】
【００１４】
本発明の第１の暗号通信システムは、
データを送受信する装置が、通信手段と暗号処理手段を備え、前記通信手段は送信部と受信部を備え、前記暗号処理手段は、画像ファイルと前記画像ファイルの画像データ上の範囲指定情報を受け、前記範囲指定情報が示す指定範囲の画素値を加工しキーを作成するキー作成手段と、対象データに前記キーの値に対応する暗号処理を施す暗号化手段と、暗号化された前記対象データに前記キーの値に対応する逆処理を施す復号手段と、前記画像ファイルを取得し、前記範囲指定情報を生成し、これらを前記キー作成手段に渡し、作成された前記キーと前記対象データのファイルを前記暗号化手段に渡し、暗号化された前記ファイルを受け、これに前記画像ファイルと前記範囲指定情報とを付して前記送信部を通じ送信する手段と、前記受信部が受信した暗号化されたファイルと画像ファイルと範囲指定情報を受け、前記受信した画像ファイルと前記受信した範囲指定情報を前記キー作成手段に渡し、作成されたキーと暗号化されたファイルを前記復号手段に渡し復号させる手段とを備える。
【００１５】
本発明の第２の暗号通信システムは、
データを送受信する装置が、通信手段と暗号処理手段を備え、前記通信手段は送信部と受信部を備え、前記暗号処理手段は、画像ファイルと前記画像ファイルの画像データ上の範囲指定情報を受け、前記範囲指定情報が示す指定範囲の画素値を加工しキーを作成するキー作成手段と、対象データに前記キーの値に対応する暗号処理を施す暗号化手段と、暗号化された前記対象データに前記キーの値に対応する逆処理を施す復号手段と、画像ファイルを取得し、前記範囲指定情報を生成し、これらを前記キー作成手段に渡し、作成された前記キーと前記対象データのファイルを前記暗号化手段に渡し、暗号化された前記ファイルを受け、範囲指定情報を前記画像ファイルに埋め込み、これを暗号化された前記ファイ

ルに付し前記送信部を通じ送信する手段と、前記受信部が受信した暗号化されたファイルと画像ファイルを受け、前記受信した画像ファイルから範囲指定情報を抽出し、前記受信した画像ファイルと前記抽出した範囲指定情報を前記キー作成手段に渡し、作成されたキーと前記受信した暗号化されたファイルを前記復号手段に渡し復号させる手段とを備える。

【００１６】

本発明の第３の暗号通信システムは、

データを送受信する装置とこれが接続されるネットワーク上のサーバ装置を含み、前記サーバ装置には画像ファイルを有し、前記データを送受信する装置が、通信手段と暗号処理手段を備え、前記通信手段は送信部と受信部と暗号処理インタフェース部を備え、前記暗号処理インタフェース部が、前記送信部から暗号化を指示されると、画像ファイルの格納場所記憶を参照し、前記サーバより画像ファイルを取得し、これを用いた送信対象ファイルの暗号化を前記暗号処理手段に指示し、暗号化されたファイルと画像ファイルと画像データ上の範囲指定情報とを送信部に返す手段と、前記受信部から暗号化されたファイルと画像ファイルと前記範囲指定情報とを受け、暗号化されたファイルの復号を前記暗号処理手段に指示する手段とを有し、前記暗号処理手段は、画像ファイルと前記範囲指定情報を受け、前記範囲指定情報が示す指定範囲の画素値を加工しキーを作成するキー作成手段と、前記送信対象ファイルのデータに前記キーの値に対応する暗号処理を施す暗号化手段と、暗号化されたデータに前記データのために作成されたキーの値に対応する逆処理を施す復号手段と、暗号化指示を受け前記範囲指定情報を生成し、前記範囲指定情報と前記画像ファイルをキー作成手段に送ってキーを作成させ、前記キーによる前記送信対象ファイルの暗号化を前記暗号化手段に行わせ、暗号化された前記送信対象ファイルに前記範囲指定情報を付し前記暗号処理インタフェース部に返す手段と、復号指示を受け、画像ファイルと前記画像ファイルの範囲指定情報とを、キー作成手段に送ってキーを作成させ、前記作成したキーにより暗号化された受信ファイルの復号を前記復号手段に行わせ復号された前記受信ファイルを前記暗号処理インタフェース部に返す手段を備える。

【００１７】

本発明の第４の暗号通信システムは、

データを送受信する装置とこれが接続されるネットワーク上のサーバ装置を含み、前記サーバ装置には画像ファイルを有し、前記データを送受信する装置が、通信手段と暗号処理手段を備え、前記通信手段は送信部と受信部と暗号処理インタフェース部を備え、前記暗号処理インタフェース部が、前記送信部から暗号化を指示されると、画像ファイルの格納場所記憶を参照し、前記サーバより画像ファイルを取得し、これを用いた送信対象ファイルの暗号化を前記暗号処理手段に指示し、暗号化されたファイルと、画像データ上の範囲指定情報が埋め込まれた画像ファイルとを前記送信部に返す手段と、前記受信部から暗号化されたファイルと前記範囲指定情報が埋め込まれた画像ファイルとを受け、暗号化されたファイルの復号を前記暗号処理手段に指示する手段とを有し、前記暗号処理手段は、画像ファイルと前記範囲指定情報を受け、前記範囲指定情報が示す指定範囲の画素値を加工しキーを作成するキー作成手段と、前記送信対象ファイルのデータに前記キーの値に対応する暗号処理を施す暗号化手段と、暗号化されたデータに前記データのために作成されたキーの値に対応する逆処理を施す復号手段と、暗号化指示を受け、前記範囲指定情報を生成し、前記範囲指定情報と前記画像ファイルをキー作成手段に送ってキーを作成させ、前記キーによる前記送信対象ファイルの暗号化を前記暗号化手段に行わせ、前記範囲指定情報を前記画像ファイルに埋め込み、前記画像ファイルを暗号化された前記送信対象ファイルに付し前記暗号処理インタフェース部に返す手段と、復号指示を受け、受信した画像ファイルから範囲指定情報を抽出し前記抽出した範囲指定情報と前記受信した画像ファイルを、前記キー作成手段に送ってキーを作成させ、前記作成したキーにより暗号化された受信ファイルの復号を前記復号手段に行わせ、復号された前記受信ファイルを前記暗号処理インタフェース部に返す手段を備える。

【００１８】

本発明の第５の暗号通信システムは、
データを送受信する装置とこれが接続されるネットワーク上のファイルサーバ装置及びアプリケーションサーバ装置を含み、前記ファイルサーバ装置は画像ファイルを有し、前記アプリケーションサーバ装置は暗号処理手段を有し、前記データを送受信する装置が、送信部と受信部と暗号処理インタフェース部を備え、前記暗号処理インタフェース部が、前記送信部から暗号化を指示されると、画像ファイル、暗号処理手段の各格納先を示す格納場所記憶を参照し、前記ファイルサーバより画像ファイルを取得し、これを用いた送信対象ファイルの暗号化を前記アプリケーションサーバ装置の暗号処理手段に指示し、暗号化されたファイルと画像ファイルと画像データ上の範囲指定情報とを送信部に返す手段と、前記受信部から暗号化されたファイルと前記画像ファイルと前記範囲指定情報とを受け、暗号化されたファイルの復号を前記暗号処理手段に指示する手段とを有し、前記暗号処理手段は、前記画像ファイルと前記範囲指定情報を受け、前記範囲指定情報が示す指定範囲の画素値を加工しキーを作成するキー作成手段と、前記送信対象ファイルのデータに前記キーの値に対応する暗号処理を施す暗号化手段と、暗号化されたデータに前記データのために作成されたキーの値に対応する逆処理を施す復号手段と、暗号化指示を受け、前記範囲指定情報を生成し、前記範囲指定情報と前記画像ファイルを前記キー作成手段に送ってキーを作成させ、前記作成したキーにより前記送信対象ファイルの暗号化を前記暗号化手段に行わせ、暗号化されたファイルに前記範囲指定情報を付し前記暗号処理インタフェース部に返す手段と、復号指示を受け、受信した画像ファイルと範囲指定情報を前記キー作成手段に送ってキーを作成させ、前記作成したキーにより暗号化された受信ファイルの復号を前記復号手段に行わせ、復号された前記受信ファイルを前記暗号処理インタフェース部に返す手段とを備える。

【００１９】

本発明の第６の暗号通信システムは、
データを送受信する装置とこれが接続されるネットワーク上のファイルサーバ装置及びアプリケーションサーバ装置を含み、前記ファイルサーバ装置は画像ファイルを有し、前記アプリケーションサーバ装置は暗号処理手段を有し、前記データを送受信する装置が送信部と受信部と暗号処理インタフェース部を備え、前記暗号処理インタフェース部が、前記送信部から暗号化を指示されると、画像ファイル、暗号処理手段の各格納先を示す格納場所記憶を参照し、前記ファイルサーバより画像ファイルを取得し、これを用いた送信対象ファイルの暗号化を前記アプリケーションサーバ装置の暗号処理手段に指示し、暗号化されたファイルと、画像データ上の範囲指定情報が埋め込まれた画像ファイルとを前記送信部に返す手段と、前記受信部から暗号化されたファイルと前記画像ファイルとを受け、暗号化されたファイルの復号を前記暗号処理手段に指示する手段とを有し、前記暗号処理手段は、前記画像ファイルと前記範囲指定情報を受け、前記範囲指定情報が示す指定範囲の画素値を加工しキーを作成するキー作成手段と、前記送信対象ファイルのデータに前記キーの値に対応する暗号処理を施す暗号化手段と、暗号化されたデータに前記データのために作成されたキーの値に対応する逆処理を施す復号手段と、暗号化指示を受け、前記範囲指定情報を生成し、前記範囲指定情報と前記画像ファイルを前記キー作成手段に送ってキーを作成させ、前記作成したキーにより前記送信対象ファイルの暗号化を前記暗号化手段に行わせ、前記範囲指定情報を前記画像ファイルに埋め込み、前記画像ファイルを暗号化された前記送信対象ファイルに付し前記暗号処理インタフェース部に返す手段と、復号指示を受け、受信した画像ファイルより範囲指定情報を抽出し、前記抽出した範囲指定情報と前記受信した画像ファイルを前記キー作成手段に送ってキーを作成させ、前記作成したキーにより暗号化された受信ファイルの復号を前記復号手段に行わせ、復号された前記受信ファイルを前記暗号処理インタフェース部に返す手段を備える。

【００２０】

本発明の第７の暗号通信システムは、
データを送受信する装置とこれとネットワーク接続されたサーバ装置を含み、前記サーバ装置は認証手段とユーザ情報記憶部とキー作成手段を有し、前記データを送受信する装置

が、前記サーバ装置の前記認証手段より認証用情報を要求されると、ユーザＩＤと画像ファイルと画像データ上の範囲指定情報を送信する手段を有し、前記キー作成手段が、画像ファイルと前記範囲指定情報を受け、指定範囲の画素値を加工しキーを作成し、前記認証手段は、受信した画像ファイルと前記範囲指定情報を前記キー作成手段に渡し、作成されたキーが、前記ユーザＩＤに対応したパスワードとして、前記ユーザ情報記憶部に登録されていることを確認し認証する。

【００２１】

本発明の第８の暗号通信システムは、

データを送受信する装置とこれとネットワーク接続されたサーバ装置を含み、前記サーバ装置には認証手段とユーザ情報記憶部とキー作成手段を有し、前記データを送受信する装置が、前記サーバ装置の認証手段より認証用情報を要求されると、ユーザＩＤと、画像データ上の範囲指定情報が埋め込まれた画像ファイルとを送信する手段を有し、前記キー作成手段は、前記画像ファイルから前記範囲指定情報を抽出し、指定範囲の画素値を加工しキーを作成し、前記認証手段が、受信した画像ファイルを前記キー作成手段に渡し、作成されたキーが、前記ユーザＩＤに対応したパスワードとして、前記ユーザ情報記憶部に登録されていることを確認し認証する。

【００２２】

本発明の第１のプログラムは、

データを送受信する装置のキー作成部が画像ファイルと前記画像ファイルの画像データ上の範囲指定情報を受け、前記範囲指定情報が示す指定範囲の画素値を加工しキーを作成するキー作成ステップと、データを送受信する装置のデータ暗号化部が対象データに前記キーの値に対応する暗号処理を施す暗号化ステップと、データを送受信する装置のデータ復号部が暗号化された前記対象データに前記キーの値に対応する逆処理を施す復号ステップと、データを送受信する装置の主処理部が前記画像ファイルを取得し、前記範囲指定情報を生成し、これらを前記キー作成ステップに渡し、作成された前記キーと前記対象データのファイルを前記暗号化部に渡し、暗号化された前記ファイルを受けて前記データを送受信する装置の送信部に渡し、前記送信部が前記暗号化されたファイルに前記画像ファイルと前記範囲指定情報とを付して送信するステップと、前記データを送受信する装置の受信部が受信した暗号化されたファイルと画像ファイルと範囲指定情報を受け、前記主処理部に送り、前記主処理部が前記受信した画像ファイルと範囲指定情報を前記キー作成部に渡し、作成されたキーと前記受信した暗号化されたファイルとを前記データ復号部に渡し、前記データ復号部が前記受信した暗号化されたファイルを復号するステップとを、前記データを送受信する装置としてのコンピュータに実行させる。

【００２３】

本発明の第２のプログラムは、

データを送受信する装置のキー作成部が画像ファイルと画像データ上の範囲指定情報を受け、指定範囲の画素値を加工しキーを作成するキー作成ステップと、データを送受信する装置のデータ暗号化部がデータに前記キーの値に対応する暗号処理を施す暗号化ステップと、データを送受信する装置のデータ復号部が暗号化されたデータに前記キーの値に対応する逆処理を施す復号ステップと、データを送受信する装置の主処理部が前記画像ファイルを取得し、前記範囲指定情報を生成し、これらを前記キー作成ステップに渡し、作成された前記キーと前記対象データのファイルを前記暗号化部に渡し、暗号化された前記ファイルを受け、前記範囲指定情報を画像ファイルに埋め込み、前記データを送受信する装置の送信部に渡し、前記送信部が前記画像ファイルを暗号化されたファイルに付し送信するステップと、前記データを送受信する装置の受信部が受信した暗号化されたファイルと画像ファイルを受け、前記データを送受信する装置の主処理部に送り、前記主処理部が前記受信した画像ファイルから範囲指定情報を抽出し、前記受信した画像ファイルと前記抽出した範囲指定情報を前記キー作成部に渡し、作成されたキーと前記受信した暗号化されたファイルを前記復号部に渡し、前記データ復号部が前記受信した暗号化されたファイルを復号するステップとを、前記データを送受信する装置としてのコンピュータに実行させる

。

【００２４】

本発明の第３のプログラムは、

データを送受信する装置における送信部がデータを送信する送信ステップと、前記装置における受信部がデータを受信する受信ステップと、前記装置における暗号処理インタフェース部が、前記送信部から暗号化を指示されると、画像ファイルの格納場所記憶を参照し、ネットワーク接続されたサーバより画像ファイルを取得し、これを用いた送信対象ファイルの暗号化を前記装置における暗号処理部に指示し、暗号化されたファイルと画像ファイルと前記画像ファイルの画像データ上の範囲指定情報とを前記送信部に返すステップと、前記受信部から暗号化されたファイルと画像ファイルと前記範囲指定情報とを受け、暗号化されたファイルの復号を前記暗号処理部に指示するステップとを含む暗号処理インタフェースステップと、前記暗号処理部が、前記画像ファイルと前記画像ファイルの画像データ上の範囲指定情報を受け、指定範囲の画素値を加工し、前記暗号処理部内のキー作成部にてキーを作成するキー作成ステップと、データに前記キーの値に対応する暗号処理を前記暗号処理部内の暗号化部にて施す暗号化ステップと、暗号化されたデータに前記キーの値に対応する逆処理を前記暗号処理部内の復号化部にて施す復号ステップと、前記暗号処理部内の主処理部が暗号化指示を受け、前記範囲指定情報を生成し、これと前記画像ファイルを伴い、前記キー作成部にキーを作成させ、これによる送信対象ファイルの暗号化を前記暗号化部に行わせ、暗号化されたファイルに前記範囲指定情報を付し前記暗号処理インタフェース部に返すステップと、復号指示を受け、前記受信部が受信した画像ファイルと範囲指定情報を前記キー作成部に送り、前記キー作成部にキーを作成させ、これによる暗号化された受信ファイルの復号を前記復号部に行わせ、復号された前記受信ファイルを前記暗号処理インタフェース部に返すステップを含む暗号処理ステップとを、前記データを送受信する装置としてのコンピュータに実行させる。

【００２５】

本発明の第４のプログラムは、

データを送受信する装置における送信部がデータを送信する送信ステップと、前記装置における受信部がデータを受信する受信ステップと、前記装置における暗号処理インタフェース部が、前記送信部から暗号化を指示されると、画像ファイルの格納場所記憶を参照し、

ネットワーク接続されたサーバより画像ファイルを取得し、これを用いた送信対象ファイルの暗号化を前記装置における暗号処理部に指示し、暗号化されたファイルと画像データ上の範囲指定情報が埋め込まれた画像ファイルとを前記送信部に返すステップと、前記受信部から暗号化されたファイルと前記範囲指定情報が埋め込まれた画像ファイルとを受け、

暗号化されたファイルの復号を前記暗号処理部に指示するステップとを含む暗号処理インタフェースステップと、前記暗号処理部が前記画像ファイルと前記範囲指定情報を受け、指定範囲の画素値を加工し、前記暗号処理部内のキー作成部にてキーを作成するキー作成ステップと、データに前記キーの値に対応する暗号処理を前記暗号処理部内の暗号化部にて施す暗号化ステップと、暗号化されたデータに前記キーの値に対応する逆処理を前記暗号処理部内の復号化部にて施す復号ステップと、前記暗号処理部内の主処理部が暗号化指示を受け、前記範囲指定情報を生成し、これと前記画像ファイルを伴い、前記キー作成部にキーを作成させ、これによる送信対象ファイルの暗号化を前記暗号化部に行わせ、暗号化されたファイルに前記範囲指定情報を埋め込んだ画像ファイルを付し前記暗号処理インタフェース部に返すステップと、復号指示を受け、前記受信部が受信した画像ファイルから範囲指定情報を抽出し、前記抽出した範囲指定情報と前記受信した画像ファイルを前記キー作成部に送り、前記キー作成部にキーを作成させ、これによる暗号化された受信ファイルの復号を前記復号部に行わせ、復号された前記受信ファイルを前記暗号処理インタフェース部に返すステップを含む暗号処理ステップとを、前記データを送受信する装置としてのコンピュータに実行させる。

【００２６】
本発明の第５のプログラムは、
データを送受信する装置における送信部がデータを送信する送信ステップと、前記装置における受信部がデータを受信する受信ステップと、前記装置における暗号処理インタフェース部が前記送信部から暗号化を指示されると、前記暗号処理インターフェース部が画像ファイル、暗号処理ステップの各格納先を示す格納場所記憶を参照し、ネットワーク接続されたファイルサーバより画像ファイルを取得し、これを用いた送信対象ファイルの暗号化をネットワーク接続されたアプリケーションサーバ装置の暗号処理部に指示し、暗号化されたファイルと画像ファイルと画像データ上の範囲指定情報とを前記送信部に返すステップと、前記受信部から暗号化されたファイルと画像ファイルと前記範囲指定情報とを受け、暗号化されたファイルの復号を前記暗号処理部に指示するステップと、
復号されたファイルを受け取るステップを含む暗号処理インタフェースステップと、前記暗号処理部のキー作成部が、画像ファイルと前記範囲指定情報を受け、指定範囲の画素値を加工しキーを作成するステップと、前記暗号処理部の暗号化部が、データに前記キーの値に対応する暗号処理を施すステップと、前記暗号処理部の復号部が、暗号化されたデータに前記キーの値に対応する逆処理を施すステップと、前記暗号処理部の主処理部が、暗号化指示を受け、前記範囲指定情報を生成し、これと画像ファイルを伴い、前記キー作成部にキーを作成させ、これによる送信対象ファイルの暗号化を前記暗号化部に行わせ、暗号化されたファイルに前記範囲指定情報を付し前記暗号処理インタフェース部に返すステップと、復号指示を受け、画像ファイルと前記範囲指定情報を伴い、前記キー作成部にキーを作成させ、これによる暗号化された受信ファイルの復号を前記復号部に行わせ、
復号された受信ファイルを前記暗号処理インタフェース部に返すステップとを、前記データを送受信する装置としてのコンピュータに実行させる。
【００２７】
本発明の第６のプログラムは、
データを送受信する装置の送信部がデータを送信する送信ステップと、前記データを送受信する装置の受信部がデータを受信する受信ステップと、暗号処理インタフェース部が
画像ファイル、暗号処理ステップの格納先を示す格納場所記憶を参照し、ネットワーク接続されたファイルサーバより画像ファイルを取得し、これを用いた送信対象ファイルの暗号化をネットワーク接続されたアプリケーションサーバ装置の暗号処理部に指示し、暗号化されたファイルと画像データ上の範囲指定情報が埋め込まれた画像ファイルとを前記送信部に送信するステップと、前記受信部から暗号化されたファイルと前記範囲指定情報が埋め込まれた画像ファイルとを受け、前記暗号化されたファイルの復号を前記暗号処理部に指示するステップと、復号されたファイルを受け取るステップを含む暗号処理インタフェースステップと、前記暗号化処理部のキー作成部が、画像ファイルと前記範囲指定情報を受け、指定範囲の画素値を加工しキーを作成するステップと、前記暗号化処理部の暗号化部がデータに前記キーの値に対応する暗号処理を施すステップと、前記暗号化処理部の復号部が暗号化されたデータに前記キーの値に対応する逆処理を施すステップと、前記暗号化処理部の主処理部が暗号化指示を受け、前記範囲指定情報を生成し、これと画像ファイルを伴い、前記キー作成部にキーを作成させ、これによる送信対象ファイルの暗号化を前記暗号化部に行わせ、範囲指定情報を画像ファイルに埋め込み、これを暗号化されたファイルに付し前記暗号処理インタフェース部に返すステップと、復号指示を受け、画像ファイルより前記範囲指定情報を抽出し、これと画像ファイルを伴い、前記キー作成部にキーを作成させ、これによる暗号化された受信ファイルの復号を前記復号部に行わせ、復号された受信ファイルを前記暗号処理インタフェース部に返すステップとを、前記データを送受信する装置としてのコンピュータに実行させる。
【００２８】
本発明の第７のプログラムは、
データを送受信する装置に、これとネットワーク接続されているサーバ装置の認証部が認証用情報を要求するステップと、前記データを送受信する装置がユーザIDと画像ファイル

と画像データ上の範囲指定情報とを前記サーバ装置に送るステップと、前記サーバが有するキー作成部が、前記データを送受信する装置が前記サーバに送信した前記画像ファイルと前記範囲指定情報とを受け、指定範囲の画素値を加工しキーを作成するキー作成ステップと、前記サーバが有する認証部が、作成された前記キーが、前記ユーザＩＤに対応したパスワードとして、前記サーバのユーザ情報記憶部に登録されていることを確認し、認証するステップとを、前記データを送受信する装置としてのコンピュータに実行させる。

【００２９】

本発明の第８のプログラムは、

データを送受信する装置に、これとネットワーク接続されているサーバ装置の認証部が認証用情報を要求するステップと、前記データを送受信する装置がユーザIDと画像データ上の範囲指定情報が埋め込まれた画像ファイルを前記サーバ装置に送るステップと、前記サーバが有するキー作成部が、前記データを送受信する装置が前記サーバに送信した前記画像ファイルを受け、前記範囲指定情報を抽出し前記範囲指定情報が示す指定範囲の画素値を加工しキーを作成するキー作成ステップと、前記サーバが有する認証部が、作成された前記キーが、前記ユーザＩＤに対応したパスワードとして、前記サーバのユーザ情報記憶部に登録されていることを確認し、認証するステップとを、前記データを送受信する装置としてのコンピュータに実行させる。

【００３０】

本発明の第１の暗号通信方法は、

データを送受信する装置の、キー作成部が画像ファイルと前記画像ファイルの画像データ上の範囲指定情報を受け、前記指定範囲情報が示す指定範囲の画素値を加工しキーを作成するキー作成ステップと、前記データを送受信する装置のデータ暗号化部が対象データに前記キーの値に対応する暗号処理を施す暗号化ステップと、前記データを送受信する装置のデータ復号部が暗号化された前記対象データに前記キーの値に対応する逆処理を施す復号ステップと、前記データを送受信する装置の主処理部が前記画像ファイルを取得し、前記範囲指定情報を生成し、これらを前記キー作成部に渡し、作成された前記キーと前記対象データのファイルを前記暗号化部に渡し、暗号化された前記ファイルを受け、これに前記画像ファイルと前記範囲指定情報を付して前記データを送受信する装置の送信部を通じ送信するステップと、前記データを送受信する装置の受信部が受信した暗号化されたファイルと画像ファイルと範囲指定情報を受け、前記受信した画像ファイルと前記受信した範囲指定情報を前記キー作成部に渡し、作成されたキーと前記受信した暗号化されたファイルを前記復号部に渡し、復号させるステップとを含む。

【００３１】

本発明の第２の暗号通信方法は、

データを送受信する装置の、キー作成部が画像ファイルと前記画像ファイルの画像データ上の範囲指定情報を受け、前記指定範囲情報が示す指定範囲の画素値を加工しキーを作成するキー作成ステップと、対象データに前記キーの値に対応する暗号処理を施す暗号化ステップと、暗号化されたデータに前記キーの値に対応する逆処理を施す復号ステップと、前記データを送受信する装置の主処理部が前記画像ファイルを取得し、前記範囲指定情報を生成し、これらを前記キー作成部に渡し、作成された前記キーと前記対象データのファイルを前記暗号化部に渡し、暗号化された前記ファイルを受け、前記範囲指定情報を前記画像ファイルに埋め込み、これを暗号化された前記ファイルに付し送信するステップと、受信した暗号化されたファイルと画像ファイルを受け、前記受信した画像ファイルから範囲指定情報を抽出し、前記受信した画像ファイルと前記抽出した範囲指定情報を前記キー作成ステップに渡し、作成されたキーと前記受信した暗号化されたファイルを前記復号部に渡し復号させるステップとを含む。

【００３２】

本発明の第３の暗号通信方法は、

データを送受信する装置における送信部がデータを送信する送信ステップと、前記データを送受信する装置における受信部がデータを受信する受信ステップと、前記データを送受

信する装置における暗号処理インタフェース部が、前記送信部から暗号化を指示されると、
画像ファイルの格納場所記憶を参照し、ネットワーク接続されたサーバより画像ファイルを取得し、これを用いた送信対象のファイルの暗号化を前記データを送受信する装置における暗号処理部に指示し、暗号化された前記ファイルと前記画像ファイルと前記画像ファイルの画像データ上の範囲指定情報とを前記送信部に返すステップと、前記受信部から暗号化された前記ファイルと前記画像ファイルと前記範囲指定情報とを受け、暗号化された前記ファイルの復号を前記暗号処理部に指示するステップと、前記暗号処理部が、前記画像ファイルと、前記範囲指定情報を受け、指定範囲の画素値を加工し、前記暗号処理部内のキー作成部にてキーを作成するキー作成ステップと、前記送信対象のファイルに前記キーの値に対応する暗号処理を前記暗号処理部内の暗号化部にて施す暗号化ステップと、暗号化された前記ファイルに前記キーの値に対応する逆処理を前記暗号処理部内の復号部にて施す復号ステップと、暗号化指示を受け、前記範囲指定情報を生成し、前記範囲指定情報と前記画像ファイルを、前記キー作成部に送ってキーを作成させ、これによる送信対象ファイルの暗号化を前記暗号化部に行わせ、暗号化された前記ファイルに前記範囲指定情報を付し前記暗号処理インタフェースステップに返すステップと、復号指示を受け、前記画像ファイルと前記範囲指定情報を前記キー作成部に送ってキーを作成させ、これによる暗号化された受信ファイルの復号を前記復号部に行わせ、復号された前記受信ファイルを前記暗号処理インタフェース部に返すステップとを含む。

【００３３】

本発明の第４の暗号通信方法は、
データを送受信する装置における送信部がデータを送信する送信ステップと、前記データを送受信する装置における受信部がデータを受信する受信ステップと、前記データを送受信する装置における暗号処理インタフェース部が、前記送信部から暗号化を指示されると、
画像ファイルの格納場所記憶を参照し、ネットワーク接続されたサーバより画像ファイルを取得し、これを用いた送信対象のファイルの暗号化を前記データを送受信する装置における暗号処理部に指示し、暗号化された前記ファイルと前記画像ファイルの画像データ上の範囲指定情報が埋め込まれた画像ファイルとを前記送信部に返すステップと、前記受信部から暗号化された前記ファイルと前記範囲指定情報が埋め込まれた画像ファイルとを受け、暗号化された前記ファイルの復号を前記暗号処理部に指示するステップとを含む暗号処理インターフェースステップと、前記暗号処理部が前記画像ファイルと、前記範囲指定情報を受け、指定範囲の画素値を加工し、前記暗号処理部内のキー作成部にてキーを作成するキー作成ステップと、前記送信対象のファイルに前記キーの値に対応する暗号処理を前記暗号処理部内の暗号化部にて施す暗号化ステップと、暗号化された前記送信対象のファイルのデータに前記キーの値に対応する逆処理を前記暗号処理部内の復号部にて施す復号ステップと、前記暗号処理部内の主処理部が暗号化指示を受け、前記範囲指定情報を生成し、これと前記画像ファイルを前記キー作成部に送って、キーを作成させ、前記キーによる前記送信対象のファイルの暗号化を前記暗号化部に行わせ、暗号化された前記送信対象のファイルに、前記範囲指定情報を埋め込んだ前記画像ファイルを付し、暗号処理インタフェースステップに返すステップと、復号指示を受け、前記受信部が受信した画像ファイルから範囲指定情報を抽出し、受信した画像ファイルと前記抽出した範囲指定情報とを前記キー作成部に送って、キーを作成させ、これによる暗号化された受信ファイルの復号を前記復号ステップに行わせ、復号された前記受信ファイルを前記暗号処理インタフェースステップに返すステップとを含む。

【００３４】

本発明の第５の暗号通信方法は、
データを送受信する装置における送信部がデータを送信する送信ステップと、前記データを送受信する装置における受信部がデータを受信する受信ステップと、前記データを送受信する装置における暗号処理インタフェース部が前記送信部から暗号化を指示されると、

前記暗号処理インターフェース部が、画像ファイル、暗号処理ステップの各格納先を示す格納場所記憶を参照し、ネットワーク接続されたファイルサーバより画像ファイルを取得し、これを用いた送信対象ファイルの暗号化をネットワーク接続されたアプリケーションサーバ装置の暗号処理部に指示し、暗号化されたファイルと画像ファイルと画像データ上の範囲指定情報とを前記送信部に返すステップと、前記受信部から暗号化されたファイルと画像ファイルと前記範囲指定情報とを受け、暗号化されたファイルの復号を暗号処理ステップに指示するステップと、前記暗号処理部のキー作成部が、画像ファイルと前記範囲指定情報を受け、指定範囲の画素値を加工しキーを作成するキー作成ステップと、前記暗号処理部の暗号化部が、前記送信対象のファイルに前記キーの値に対応する暗号処理を施すステップと、前記暗号処理部の復号部が、暗号化されたデータに前記キーの値に対応する逆処理を施すステップと、前記暗号処理部の主処理部が、暗号化指示を受け、前記範囲指定情報を生成し、前記範囲指定情報と画像ファイルを前記キー作成部に送って、キーを作成させ、これによる前記送信対象のファイルの暗号化を前記暗号化部に行わせ、暗号化された前記ファイルに前記範囲指定情報を付し前記暗号処理インタフェース部に返すステップと、復号指示を受け、画像ファイルと範囲指定情報を前記キー作成部に送ってキーを作成させ、これによる暗号化された受信ファイルの復号を前記復号部に行わせ、復号された受信ファイルを前記暗号処理インタフェース部に返すステップとを含む。

【００３５】

本発明の第６の暗号通信方法は、

データを送受信する装置の送信部がデータを送信する送信ステップと、前記データを送受信する装置の受信部がデータを受信する受信ステップと、前記データを送受信する装置における暗号処理インタフェース部が前記送信部から暗号化を指示されると、前記暗号処理インターフェース部が、画像ファイル、暗号処理ステップの格納先を示す格納場所記憶を参照し、ネットワーク接続されたファイルサーバより画像ファイルを取得し、これを用いた送信対象のファイルの暗号化をネットワーク接続されたアプリケーションサーバ装置の暗号処理部に指示し、暗号化されたファイルと画像データ上の範囲指定情報が埋め込まれた画像ファイルとを前記送信部に送信するステップと、前記受信部から暗号化されたファイルと前記範囲指定情報が埋め込まれた画像ファイルとを受け、前記暗号化されたファイルの復号を前記暗号処理部に指示するステップと、前記暗号化処理部のキー作成部が、画像ファイルと前記範囲指定情報を受け、指定範囲の画素値を加工しキーを作成するステップと、前記暗号化処理部の暗号化部が前記送信対象のファイルに前記キーの値に対応する暗号処理を施すステップと、前記暗号化処理部の復号部が暗号化されたデータに前記キーの値に対応する逆処理を施す復号部と、前記暗号化処理部の主処理部が暗号化指示を受け、前記範囲指定情報を生成し、前記範囲指定情報と画像ファイルを前記キー作成部に送って、キーを作成させ、これによる前記送信対象のファイルの暗号化を前記暗号化部に行わせ、前記範囲指定情報を画像ファイルに埋め込み、これを暗号化されたファイルに付し前記暗号処理インタフェース部に返すステップと、復号指示を受け、画像ファイルより前記範囲指定情報を抽出し、これと画像ファイルとを前記キー作成部に送ってキーを作成させ、これによる暗号化された受信ファイルの復号を前記復号部に行わせ、復号された受信ファイルを前記暗号処理インタフェース部に返すステップとを含む。

【００３６】

本発明の第７の暗号通信方法は、

データを送受信する装置に、これとネットワーク接続されているサーバ装置の認証部が認証用情報を要求するステップと、前記データを送受信する装置がユーザＩＤと画像ファイルと画像データ上の範囲指定情報とを前記サーバ装置に送るステップと、前記サーバが有するキー作成部が、前記データを送受信する装置が前記サーバに送信した画像ファイルと画像データ上の範囲指定情報を受け、前記範囲指定情報が示す指定範囲の画素値を加工しキーを作成するキー作成ステップと、前記サーバが有する認証部が、作成された前記キーが、前記ユーザＩＤに対応したパスワードとして、前記サーバのユーザ情報記憶部に登録されていることを確認し、認証するステップとを含む。

【００３７】
本発明の第８の暗号通信方法は、
データを送受信する装置に、これとネットワーク接続されているサーバ装置の認証部が認証用情報を要求するステップと、前記データを送受信する装置がユーザＩＤと画像データ上の範囲指定情報が埋め込まれた画像ファイルとを前記サーバ装置に送るステップと、前記サーバが有するキー作成部が、前記データを送受信する装置が前記サーバに送信した前記画像データ上の範囲指定情報が埋め込まれた画像ファイルを受け、前記画像ファイルから前記範囲指定情報を抽出し、前記範囲指定情報が示す指定範囲の画素値を加工しキーを作成するキー作成ステップと、前記サーバが有する認証部が、作成された前記キーが、前記ユーザＩＤに対応したパスワードとして、前記サーバのユーザ情報記憶部に登録されていることを確認し、認証するステップとを含む。
【００３８】
本発明の第９の暗号通信方法は、
送信データを暗号化して送信側機器からネットワークを介して相手先受信機器に送信する暗号通信方法において、前記送信側機器の有するキー作成部が任意の画像ファイルにおける画像データの任意の範囲を指定し、この指定された範囲の画像データから暗号化キーを作成するステップと、前記送信側機器の有する暗号化部が前記送信データを前記暗号化キーにより暗号化し、暗号化送信データを作成するステップと、前記送信側機器の有する送信部がこの暗号化送信データと前記画像ファイルと前記範囲を示す範囲指定情報とを送信側機器から相手先受信機器に送信するステップを備える。
【００３９】
本発明の第１０の暗号通信方法は、
暗号化された送信データを送信側機器からネットワークを介して受信する暗号通信方法において、前記送信側機器の有する受信部が暗号化された送信データと共に画像ファイルとこのファイルにおける画像データの範囲を指定する範囲指定情報を前記ネットワークから受信するステップと、前記送信側機器の有するキー作成部が受信した前記画像ファイルと前記範囲指定情報とから復号化キーを作成するステップと、前記送信側機器の有する復号部がこの復号化キーにより前記暗号化された送信データを復号するステップを備える。
【００４０】
本発明の第１１の暗号通信方法は、
送信データを暗号化して送信側機器からネットワークを介して受信側機器に送信し、受信側機器にて復号する暗号通信方法において、前記送信側機器が有するキー作成部が、任意の画像ファイルにおける画像データの任意の範囲を指定し、前記範囲の画像データから暗号化キーを作成するステップと、前記送信側機器が有する暗号化部が、前記送信データを前記暗号化キーにより暗号化し、暗号化送信データを作成するステップと、前記送信側機器が有する送信部が、この暗号化送信データと前記画像ファイルと前記範囲を示す範囲指定情報とを送信側機器からネットワークに送信するステップと、前記送信側機器が有する受信部が、ネットワークから前記暗号化送信データと前記画像ファイルと前記範囲指定情報を受信するステップと、前記送信側機器が有するキー作成部が、受信した前記画像ファイルと前記範囲指定情報とから復号化キーを作成するステップと、前記送信側機器が有する復号部が、この復号化キーにより前記暗号化された送信データを復号するステップと、を備える。

【発明の効果】
【００４１】
本発明によれば、ユーザは重要な機密ファイルを他のユーザに送るときに、画像ファイルをパスワード（秘密鍵）の代わりに使って、手軽に暗号化を行うことができ、受信側でも手軽に解読できる。

【００４２】
また、画像ファイルなので他の人に見られてもパスワード（秘密鍵）だと気がつかない。気がついても画像のどの部分を使用するかが分からないと解読に使えないので、安全である。
【００４３】
更に、画像ファイルのどの部分(座標)を使用して解読を行うかが知られても暗号処理プログラムを使用しないと解読できないので安全である。
【００４４】
また、画像の一部を利用するので処理する量が少なくて済む。
【００４５】
また、いくつかのパターンの既存の暗号化・復号アルゴリズムを用意しておいて、変えることができる。
【発明を実施するための最良の形態】
【００４６】
次に、本発明を実施するための最良の形態について図面を参照して詳細に説明する。
【００４７】
図１は本発明の暗号通信システムの第１実施形態の第１実施例の全体図である。
【００４８】
図１に示す通り、暗号通信システムはインターネット１、ユーザシステム２、３、４、ユーザネットワーク８、９により構成されている。
【００４９】
ユーザシステム２、３、４のユーザをそれぞれユーザ１０、ユーザ１１，ユーザ１２とする。
【００５０】
ユーザシステム２と３はユーザネットワーク８に接続されていて、ユーザシステム４はユーザネットワーク９に接続されていて、お互いにインターネット１を通じアクセス可能である。
【００５１】
ユーザシステム２、３、４はネットワーク接続されたサーバ機器やクライアント機器であり、この中にＰＣ（パーソナルコンピュータ）端末も含むものとする。
【００５２】
上記機器や端末はプログラム制御で動作する。
【００５３】
ユーザシステム２、３、４はお互いに通信でき、メールやファイルのやり取りができるものとする。
【００５４】
図２はユーザシステム２の構成を示したブロック図である。
【００５５】
ユーザシステム２は、通信プログラム２１、暗号処理プログラム２２、暗号化する際に使用する画像ファイルのフォルダ２４も持っている。
【００５６】
ユーザシステム３，４も同様の構成である。
【００５７】
通信プログラム２１はメーラやファイル転送プログラム等であり、送信部２１１、受信部２１２を含む。
【００５８】
暗号処理プログラム２２は暗号化を行う場合は図３（１）に示す様に、画像ファイル２４－１を用い、暗号化対象ファイル２３のデータを暗号化し、暗号化されたファイル２６、及び用いた画像ファイル２４－１と範囲指定情報２５を出力する。
【００５９】

また、解読を行う場合は図３（２）に示す様に、画像ファイル２４－１と範囲指定情報２５を用い、暗号化されたファイル２６のデータを復号し元の対象ファイル２３を出力する。

【００６０】

尚、範囲指定情報２５を画像ファイル２４－１に埋め込んで受け渡しする例もある。

【００６１】

図２に戻り、暗号処理プログラム２２は、主処理部２２１、キー作成部２２２、データ暗号化部２２３、データ復号部２２４を含む。

【００６２】

主処理部２２１は、暗号化時は暗号化対象ファイル２３、画像ファイル２４－１を取得し、範囲指定情報を生成する。

【００６３】

キー作成部２２２に画像ファイル２４－１と範囲指定情報を渡しキーを作成させ、そのキーと暗号化対象ファイル２３をデータ暗号化部２２３に渡す。

【００６４】

データ暗号化部２２３より暗号化されたファイル２６を受け、これと画像ファイル２４－１と範囲指定情報２５を格納し、その旨表示する。

【００６５】

主処理部２２１は、解読時は暗号化されたファイル２６、画像ファイル２４－１、範囲指定情報２５を受ける。

【００６６】

主処理部２２１は、キー作成部２２２に画像ファイル２４－１と範囲指定情報２５を渡しキーを作成させ、そのキーと暗号化されたファイル２６をデータ復号部２２４に渡す。

【００６７】

主処理部２２１は、データ復号部２２４より復号されたファイルを受け格納し、その旨を表示する。

【００６８】

データ暗号化部２２３はキーの値に対応した処理を暗号化対象ファイル２３のデータ等に施し暗号化する。

【００６９】

データ復号部２２４は、キーの値に対応した逆処理（同じキー値で行う暗号化処理の逆処理）を暗号化されたファイル２６のデータ等に施し復号する。

【００７０】

次に本実施例の動作を図面を参照し説明する。

【００７１】

ユーザシステム２からユーザシステム３に送信する場合で説明する。

【００７２】

図４の概略フローチャートを参照し、ユーザシステム２は、暗号化対象ファイルに対して画像ファイルと暗号処理プログラムを使用して暗号化を行う（ステップＳ１）。

【００７３】

ユーザシステム２の送信部２１１は、暗号化されたファイル２６と画像ファイル２４－１と暗号化に使用した画像の範囲指定情報（座標情報）２５をメール等でユーザシステム３に送信する。

【００７４】

この際、図６（１）に示す様に座標情報を「暗号化する際に使用する画像ファイル」のヘッダにコメントとして挿入する例もある。

【００７５】

また、図６（２）に示す様に、座標位置の値そのものを画素値として「暗号化する際に使用する画像ファイル」に埋め込むこともできる（ステップＳ２）。

【００７６】

ユーザシステム３は、 送信されてきたファイルに対して暗号処理プログラム２２を使用して、ファイルの解読を行ない（ステップＳ３）、ファイルを開く（ステップＳ４）。

【００７７】

図５（１）のフローチャートを参照し、ステップＳ１を詳細に説明する。

【００７８】

ユーザシステム２において、暗号処理プログラム２２が起動されると、主処理部２２１が暗号化／解読の指定を取得するが、（暗号化、解読のそれぞれのアイコンを表示し、応答を入力させるが）、暗号化の指定により暗号化処理を開始する（ステップＳ１－１）。

【００７９】

主処理部２２１は、暗号化の指示を受け、暗号化対象ファイルの指定を取得し、そのファイルを取り込む（ステップＳ１－２）。

【００８０】

暗号化する際に使用する画像ファイルの指定を取得し、そのファイルを取り込む。例えば、フォルダ名が初期設定されていれば、そのフォルダの画像ファイル名を表示し、選択させ、選択されたファイルを取り込む（ステップＳ１－３）。

【００８１】

暗号化する際に使用する画像ファイルの暗号化する際に使用する範囲を生成する。範囲は矩形の左上と右下の２点の座標位置を指定する。

【００８２】

例えば図６（１）に示す様に、（ｘｍｉｎ，ｙｍｉｎ）＝（２，３）と（ｘｍａｘ，ｙｍａｘ）＝（６，７）の様に指定する。

【００８３】

ここで、（ｘｍｉｎ，ｙｍｉｎ）の値は、ランダムに生成し、（ｘｍａｘ，ｙｍａｘ）の値は初期設定されたサイズ（ｘ方向，ｙ方向にそれぞれ５画素分）で決める。

【００８４】

ランダムに生成する例としては、時刻を取得し、秒の値（バイナリで６ビット）に対し所定のビットシヤッフルを行い決めてもよい（ステップＳ１－４）。

【００８５】

次にキー作成部２２２が指定した範囲の色情報である画素の値を左上の座標から右下の座標までをメモリに格納し、これらをアルゴリズムを通して加工し、キーとする（ステップＳ１－５）。

【００８６】

データ暗号化部２２３がキーの値に対応した処理を対象ファイルのデータ等に施し暗号化する（ステップＳ１－６）。

【００８７】

このデータ暗号化処理は既存の共通鍵暗号方式の暗号化技術、例えばＤＥＳ（Ｄａｔａ Ｅｎｃｒｉｐｔｉｏｎ Ｓｔａｎｄａｒｄ）やＦＥＡＬ（Ｆａｓｔ ｄａｔａ Ｅｎｃｒｉｐｈｅｒｍｅｎｔ Ａｌｇｏｒｉｔｈｍ）等を利用して行ってもよい。

【００８８】

図５（２）のフローチャートを参照し、前記ステップ３を詳細に説明する。

ユーザシステム３で、受信部２１２が暗号化されたファイル、画像ファイル、範囲指定情報（座標情報）を受信する。

【００８９】

暗号処理プログラム２２が起動され、主処理部２２１が解読指示を受け、前記受信情報を取り込む（ステップ３－１）。

【００９０】

キー作成部２２２が画像ファイルの指定された範囲の画素値（色情報）をメモリに格納し（ステップ３－２）、これらをアルゴリズムを通して加工し、キーとする（ステップ３－３）。

【００９１】

データ復号部２２４がキーの値に対応した逆処理を暗号化されたファイルのデータ等に施し復号する（ステップ３－４）。

【００９２】

このデータ復号処理は既存の共通鍵暗号方式の暗号化技術（ＤＥＳ、ＦＥＡＬ等）を利用して行ってもよい。

【００９３】

次に、本実施形態の第２実施例について説明する。

【００９４】

第２実施例では、ユーザシステムが暗号・解読の際に使用する画像ファイルのフォルダ２４や暗号処理プログラム２３を備えていない。

【００９５】

メモリストレージ等の持ち運び可能な媒体の中に「暗号・解読の際に使用する画像ファイル」や暗号処理プログラムを入れておき、この媒体をユーザシステムのＵＳＢインタフェースやＰＣカードスロット等に装着することにより、どこのユーザシステム上からでも暗号・解読を行うことが可能である。

【００９６】

次に、本実施形態の第３実施例について図面を参照し説明する。

【００９７】

図７は本実施形態の第３実施例の全体図である。図７に示す通り、アプリケーションサーバ（ＡＰサーバ）５はユーザネットワーク８に接続されておりユーザシステム２や３が同じソフトウェアを使用することができるように共有してあり、ファイルサーバ６やユーザシステム上の画像ファイルを使用して暗号化や解読を行う。

【００９８】

ファイルサーバ６はユーザネットワーク８に接続されておりユーザシステム２や３がファイルサーバ６の共有ディスクにアクセスできるように共有してあり、暗号・解読する際に使用する画像ファイルをフォルダ６３に格納している。

【００９９】

暗号・解読するための画像ファイルはユーザシステム２や３のローカルディスクに格納されていても暗号・解読を行うことができる。

【０１００】

図８に示す様に、ファイルサーバ６は、データ転送プログラム６１とデータ確認プログラム６２と画像ファイルのフォルダ６３を含む。

【０１０１】

図９に示す様に、ＡＰサーバ５は、データ受信プログラム５１、データ送信プログラム５３、暗号処理プログラム５２を含む。

【０１０２】

暗号処理プログラム５２は暗号処理プログラム２２と同様の構成であるが、ユーザシステム２或いは３から呼び出され実行できる。

【０１０３】

図１０に本実施例におけるユーザシステム２，３，４の構成を示す。暗号処理プログラム２２や、画像ファイルのフォルダ２４は含まなくてもよい。

【０１０４】

但し、暗号処理プログラム２２をローカルに持つ例では、暗号処理プログラム２２は通信プログラム２１から呼び出され指示とファイル等（暗号化対象ファイルと画像ファイル、暗号化されたファイルと画像ファイルと座標情報）を受け、暗号化・解読処理を行なう。そして結果を通信プログラム２１に返す。

【０１０５】

即ち、主処理部２２１が後述の暗号処理Ｉ／Ｆ部２１３とのインタフェースを持つ。

【０１０６】

通信プログラム２１の、送信部２１１は、暗号化して送信することをユーザから指示さ

れる（「暗号化して送信」アイコンが操作される）と、指示暗号処理Ｉ／Ｆ部２１３を通じ暗号処理プログラム２２，或いは５２を呼び出し、暗号化を指示する。

【０１０７】

受信部２１２Ａは、暗号化ファイル検出部２１２１で暗号化されたファイルを受信したことを検出すると、暗号処理Ｉ／Ｆ部２１３を通じ暗号処理プログラム２２，或いは５２を呼び出し、復号化を指示する。

【０１０８】

暗号化ファイル検出部２１２１は、メール本文等に所定の形式の範囲指定情報を受信するか、ヘッダのコメント欄に所定の形式の範囲指定情報を含む画像ファイルを受信すると暗号処理Ｉ／Ｆ部２１３を呼び出す。

【０１０９】

暗号処理Ｉ／Ｆ部２１３のフォルダ情報記憶２１３１には、画像ファイルのフォルダのパス名、フォルダ名、パスがファイルサーバ６の場合のユーザＩＤ、パスワードが初期設定され、アクセスする暗号処理プログラムのパス名、フォルダ名が初期設定されている。

【０１１０】

次に本実施例の動作を図面を参照し説明する。ユーザシステム２からユーザシステム３、或いは４に送信する場合で説明する。

【０１１１】

図１１のフローチャートを参照し、ユーザシステム２で、送信部２１１が「暗号化して送信」アイコンが操作されたことを受け、暗号処理Ｉ／Ｆ部２１３に暗号化対象ファイルの暗号化を指示する。

【０１１２】

暗号処理Ｉ／Ｆ部２１３は暗号化用画像ファイルがユーザシステム２にあるかをフォルダ情報記憶で判定しローカルで持っていない場合（ステップＡ１）、画像ファイルをファイルサーバ６に要求する（ステップＡ２）。

【０１１３】

データ確認プログラム６２がその要求が適切であるか確認し、確認できれば（ステップＡ３）、次にデータ転送プログラム６１が画像のファイルフォルダ６３内に格納されている画像ファイルを要求元のユーザシステム２に転送する（ステップＡ４）。

【０１１４】

ユーザシステム２上にあれば、ローカルの画像ファイルを取得する（ステップＡ５）。

【０１１５】

暗号処理Ｉ／Ｆ部２１３は、暗号処理プログラムがユーザシステム２にあるかをフォルダ情報記憶２１３１で判定し、ローカルで持っていない場合（ステップＡ６）、ＡＰサーバ５の暗号処理プログラムを呼出し実行する（ステップＡ７）。

【０１１６】

データ受信プログラム５１が、暗号化対象ファイルと画像ファイルと座標情報を受信し（ステップＡ８）、暗号処理プログラム５２が暗号化し（ステップＡ９）、データ送信プログラム５３が処理結果（暗号化されたファイルと、画像ファイル及び座標情報）をユーザシステム２に送信する（ステップＡ１０）。

【０１１７】

暗号処理Ｉ／Ｆ部２１３はユーザシステム２上にあれば、ローカルの暗号処理プログラムで暗号化する（ステップＡ１１）。

【０１１８】

図１２のフロチャートに移り、暗号処理Ｉ／Ｆ部２１３はユーザシステム３或いは４に暗号化されたファイルと、画像ファイル及び座標情報（或いは座標を含む画像ファイル）を送信する（ステップＡ１２）。

【０１１９】

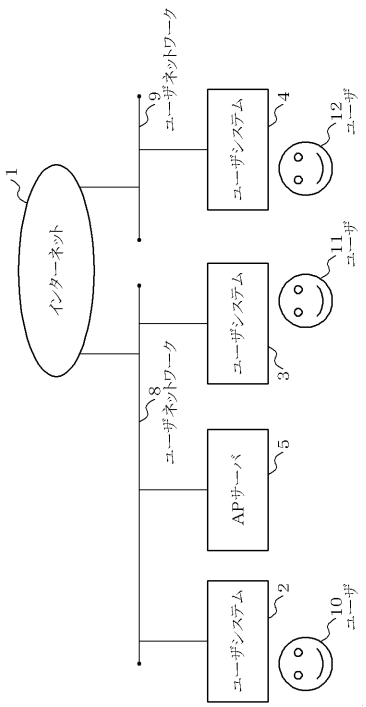
ユーザシステム３或いは４の受信部２１２Ａが範囲情報を検出し、これがＡＰサーバ５からの暗号化指示に対する返信でなければ暗号処理Ｉ／Ｆ部２１３に解読を指示する（ス

テップＡ１３）。
【０１２０】
暗号処理Ｉ／Ｆ部２１３は、解読するプログラムはローカルシステム上にあるかをフォルダ情報記憶２１３１を参照して判定し（ステップＡ１４）、なければＡＰサーバ５の暗号処理プログラムを呼び出し、暗号化されたファイルと画像ファイルと座標情報を渡す（ステップＡ１５）。
【０１２１】
データ受信プログラム５１が、暗号化されたファイルと画像ファイルと座標情報を受信し（ステップＡ１６）、暗号処理プログラム５２が解読し（ステップＡ１７）、データ送信プログラム５３が処理結果（復号されたファイル）をユーザシステム３或いは４に送信する（ステップＡ１８）。
【０１２２】
解読するプログラムはローカルシステム上にあれば、ローカルの暗号処理プログラムで解読する（ステップＡ１９）。
【０１２３】
ユーザシステム３或いは４の受信部で対象ファイルが開かれる（ステップＡ２０）。
【０１２４】
この様に、ＡＰサーバを使用することにより、ユーザシステム上に暗号処理プログラムが入っていなくても暗号化や解読を行うことができる。
【０１２５】
次に本発明の第２実施形態について図面を参照し説明する。
【０１２６】
図１３は本発明の暗号通信システムの第２実施形態の全体図である。
【０１２７】
図１３に示す通り、データベースサーバ（ＤＢサーバ）７が、ユーザネットワーク８に接続されている。
【０１２８】
このＤＢサーバ７は、ユーザシステム２、３、４からデータベース操作を行う際に認証が必要なサーバである。
【０１２９】
図１４に示すようにＤＢサーバ７は、認証プログラム７１とＤＢサーバプログラム７２とＤＢ記憶部７３とユーザ情報記憶部７４とキー作成部７５で構成されている。
【０１３０】
次に、図１５のフローチャートを参照し、本実施形態の動作を説明する。
【０１３１】
ユーザシステム２、３、４でＤＢサーバ７の操作要求が発生し（ステップＢ１）、ユーザＩＤと「認証に使用する画像ファイル」と「座標情報」をＤＢサーバ７に送信する（ステップＢ２）。
【０１３２】
認証プログラム７１がユーザシステム２、３、４から送られてきたユーザＩＤと画像ファイルと座標情報を受信し（ステップＢ３）、画像ファイルと座標情報をキー作成部７５に渡し、ここでパスワードに変換する。
【０１３３】
例えば、画像ファイルの指定範囲の画素の値を７、１２、２５、２０７、０、１９、３だとしたらそれぞれの値の桁を足して７、３、７、９、０、０、３というパスワードに変換する（ステップＢ４）。
【０１３４】
ユーザＩＤとパスワードがユーザ情報記憶部７４に登録されていればアクセス権限があると判断し（ステップＢ５）、認証した旨を要求元であるユーザシステム２、３、４に送信する（ステップＢ６）。

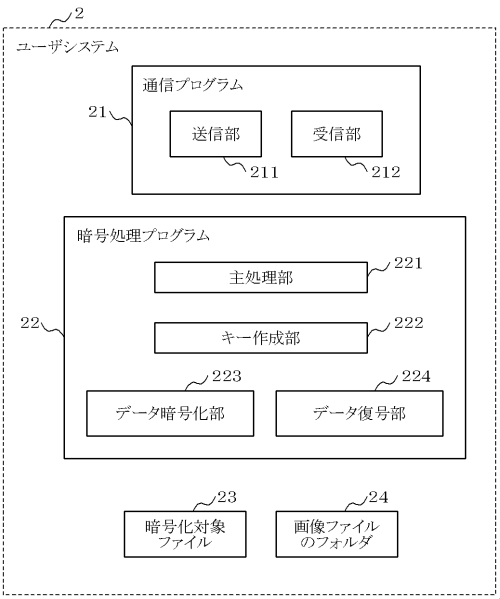
【０１３５】
認証されたならば、ユーザシステム２、３、４が操作指示を送信し（ステップＢ７）、ＤＢサーバプログラム７２が、ＤＢ記憶部７３への操作及び要求元への応答を行う（ステップＢ８）。
【０１３６】
本実施形態の別の実施例では、ＤＢサーバ７がキー作成部７５を持たないが、ＡＰサーバ５の暗号処理プログラム５２を指すフォルダ情報記憶部を持ち、認証プログラム７１が画像ファイルと座標情報を付けて暗号処理プログラム５２を呼出し、結果のパスワード（キー）を受信する。
【０１３７】
この様にして、ユーザシステムが社内のサイトや各種サーバにアクセスする際に、パスワード等の認証を求められた場合にも画像の一部の色情報をパスワード代わりに使用することができる。
【０１３８】
ユーザは今までの様な複雑で長い文字のパスワードを覚える必要がない。
【０１３９】
画像ファイルなので他の人に見られてもパスワードだと気がつかない。気がついても画像のどの部分を使用するかが分からないと解読に使えない。
【０１４０】
画像ファイルのどの部分（座標）を使用して解読を行うかが知られても暗号処理プログラム（キー作成部）を使用しないと解読できないので安全である。
【図面の簡単な説明】
【０１４１】
【図１】本発明の暗号通信システムの第１実施形態の第１実施例の全体図。
【図２】図１のユーザシステム２の構成を示したブロック図。
【図３】（１）は暗号化を行う場合の、暗号処理プログラム２２の入出力を示す図で、（２）は解読を行う場合の、暗号処理プログラム２２の入出力を示す図。
【図４】本発明の第１実施形態の第１実施例の動作を示すフローチャート。
【図５】（１）は図４のステップ１を詳細に説明するフロチャートで、（２）は図４のステップ３を詳細に説明するフロチャート。
【図６】本発明の実施形態における、範囲指定情報（座標情報）が埋め込まれた画像ファイルを示し、（１）は画像ファイルのヘッダにコメントとして挿入する例を示す図で、（２）は画像データ部に埋め込む例を示す図。
【図７】本発明の第１実施形態の第３実施例の全体図。
【図８】図７のファイルサーバ６の構成を示すブロック図。
【図９】図７のＡＰサーバ５の構成を示すブロック図。
【図１０】図７のユーザシステム２，３，４の構成を示すブロック図。
【図１１】本発明の第１実施形態の第３実施例の動作を示すフローチャート。
【図１２】本発明の第１実施形態の第３実施例の動作を示すフローチャート。
【図１３】本発明の第２実施形態の全体図。
【図１４】図１３のＤＢサーバ７の構成を示すブロック図。
【図１５】本発明の第２実施形態の動作を示すフローチャート。
【符号の説明】
【０１４２】
１　インターネット
１０、１１、１２　ユーザ
２、３、４　ユーザシステム
２１　通信プログラム
２１１　送信部
２１２、２１２Ａ　受信部

２１２１　暗号化ファイル検出部
２１３　暗号処理Ｉ／Ｆ部
２１３１　フォルダ情報記憶
２２　暗号処理プログラム
２２１　主処理部
２２２　キー作成部
２２３　データ暗号化部
２２４　データ復号部
２３　暗号化対象ファイル
２４　画像ファイルのフォルダ
２４－１　画像ファイル
２５　範囲指定情報（座標情報）
２６　暗号化されたファイル
５　ＡＰサーバ
５１　データ受信プログラム
５２　暗号処理プログラム
５３　データ送信プログラム
６　ファイルサーバ
６１　データ転送プログラム
６２　データ確認プログラム
６３　画像ファイルのフォルダ
７　ＤＢサーバ
７１　認証プログラム
７２　ＤＢサーバプログラム
７３　ＤＢ記憶部
７４　ユーザ情報記憶部
７５　キー作成部
８　ユーザネットワーク
９　ユーザネットワーク

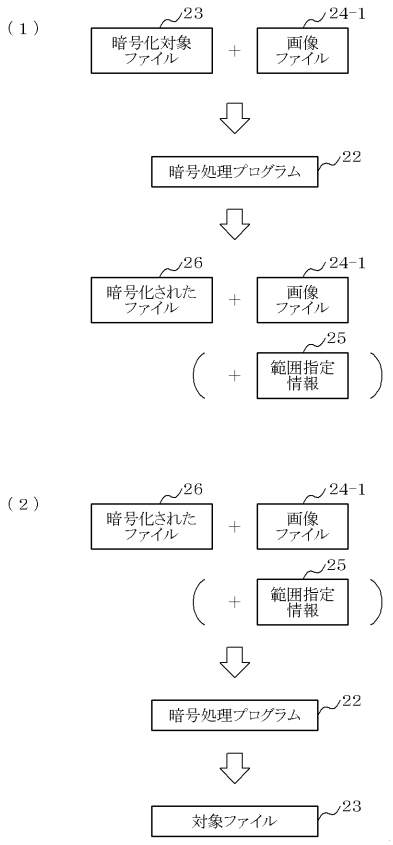
【図１】


インターネット
1
ユーザネットワーク
9
ユーザシステム
4
12
ユーザ
11
ユーザ
ユーザシステム
3
ユーザネットワーク
8
APサーバ
5
ユーザシステム
2
10
ユーザ

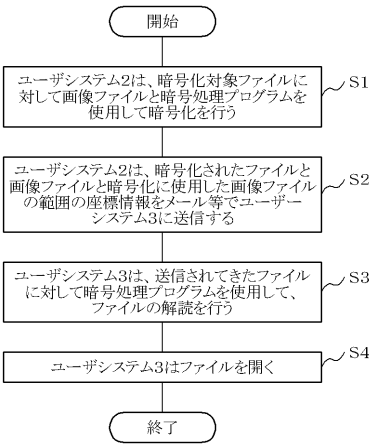
【図２】


2
ユーザシステム
通信プログラム
21
送信部
211
受信部
212
暗号処理プログラム
22
主処理部
221
キー作成部
222
223
データ暗号化部
224
データ復号部
23
暗号化対象ファイル
24
画像ファイルのフォルダ

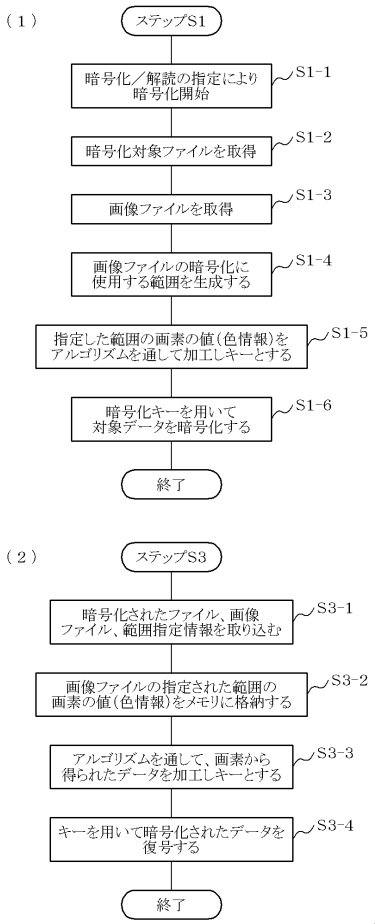
【図３】


（１）
23
暗号化対象ファイル
＋
24-1
画像ファイル
暗号処理プログラム
22
26
暗号化されたファイル
＋
24-1
画像ファイル
＋
25
範囲指定情報
（２）
26
暗号化されたファイル
＋
24-1
画像ファイル
＋
25
範囲指定情報
暗号処理プログラム
22
対象ファイル
23

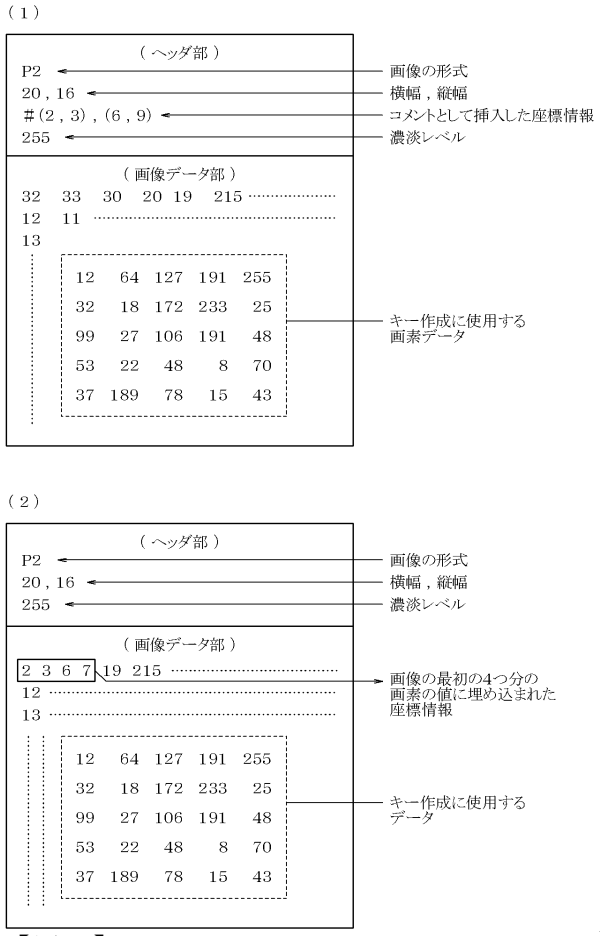
【図４】


開始
ユーザシステム2は、暗号化対象ファイルに対して画像ファイルと暗号処理プログラムを使用して暗号化を行う
S1
ユーザシステム2は、暗号化されたファイルと画像ファイルと暗号化に使用した画像ファイルの範囲の座標情報をメール等でユーザーシステム3に送信する
S2
ユーザシステム3は、送信されてきたファイルに対して暗号処理プログラムを使用して、ファイルの解読を行う
S3
ユーザシステム3はファイルを開く
S4
終了

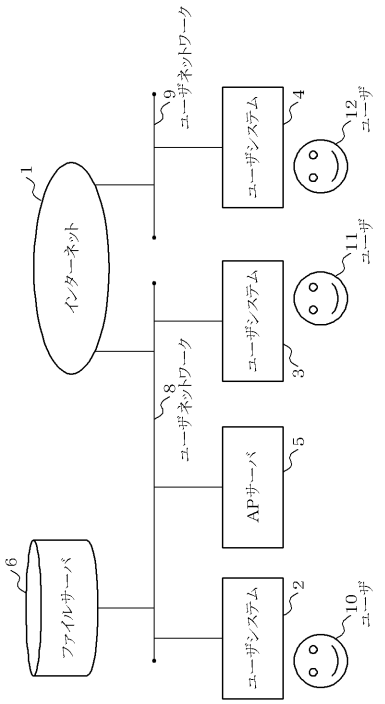
【図５】


（１）
ステップS1
暗号化／解読の指定により暗号化開始
S1-1
暗号化対象ファイルを取得
S1-2
画像ファイルを取得
S1-3
画像ファイルの暗号化に使用する範囲を生成する
S1-4
指定した範囲の画素の値（色情報）をアルゴリズムを通して加工しキーとする
S1-5
暗号化キーを用いて対象データを暗号化する
S1-6
終了
（２）
ステップS3
暗号化されたファイル、画像ファイル、範囲指定情報を取り込む
S3-1
画像ファイルの指定された範囲の画素の値（色情報）をメモリに格納する
S3-2
アルゴリズムを通して、画素から得られたデータを加工しキーとする
S3-3
キーを用いて暗号化されたデータを復号する
S3-4
終了

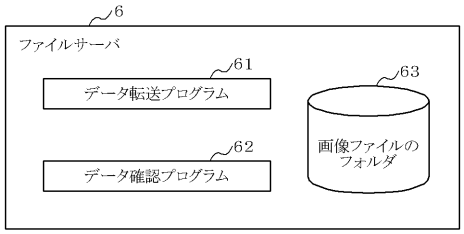
【図６】


（１）
（ヘッダ部）
P2
20，16
＃(2，3)，(6，9)
255
画像の形式
横幅，縦幅
コメントとして挿入した座標情報
濃淡レベル
（画像データ部）
32 33 30 20 19 215
12 11
13
12 64 127 191 255
32 18 172 233 25
99 27 106 191 48
53 22 48 8 70
37 189 78 15 43
キー作成に使用する画素データ
（２）
（ヘッダ部）
P2
20，16
255
画像の形式
横幅，縦幅
濃淡レベル
（画像データ部）
2 3 6 7 19 215
12
13
画像の最初の4つ分の画素の値に埋め込まれた座標情報
12 64 127 191 255
32 18 172 233 25
99 27 106 191 48
53 22 48 8 70
37 189 78 15 43
キー作成に使用するデータ

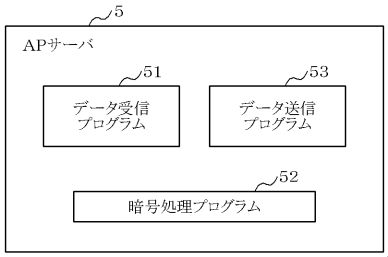
【図７】


インターネット
1
ユーザネットワーク
9
ユーザシステム
4
12
ユーザ
11
ユーザ
ユーザシステム
3
ユーザネットワーク
8
APサーバ
5
ファイルサーバ
6
ユーザシステム
2
10
ユーザ

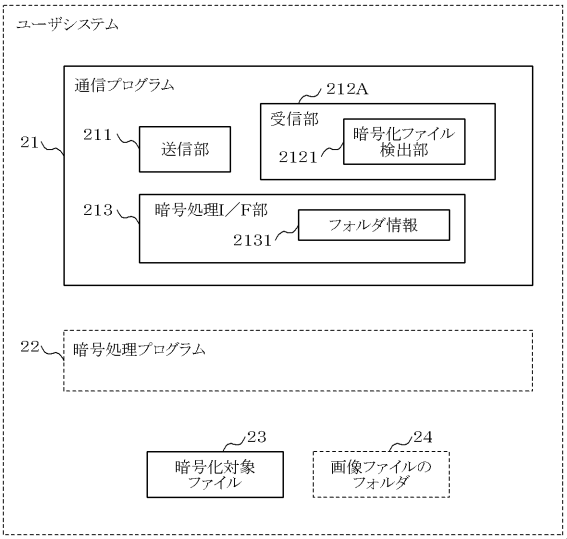
【図８】


6
ファイルサーバ
61
データ転送プログラム
62
データ確認プログラム
63
画像ファイルのフォルダ

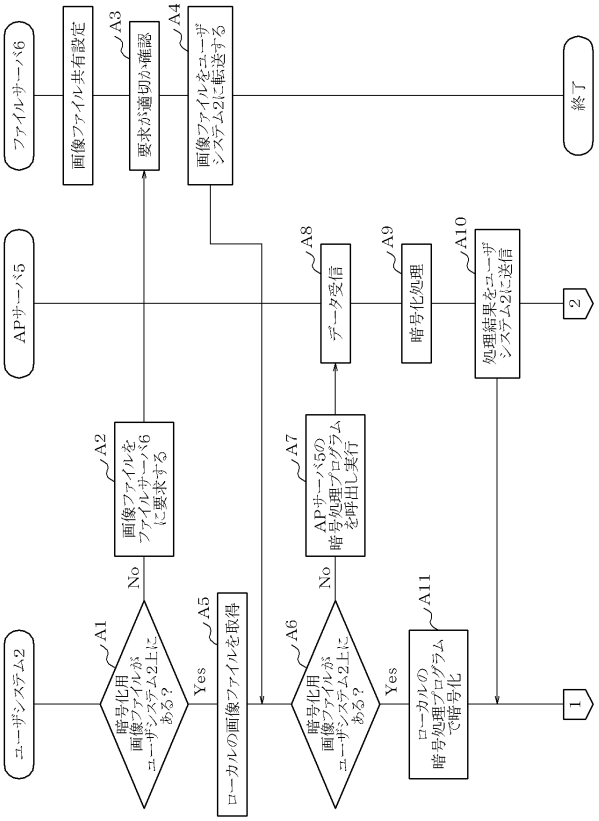
【図９】


5
APサーバ
51
データ受信プログラム
53
データ送信プログラム
52
暗号処理プログラム

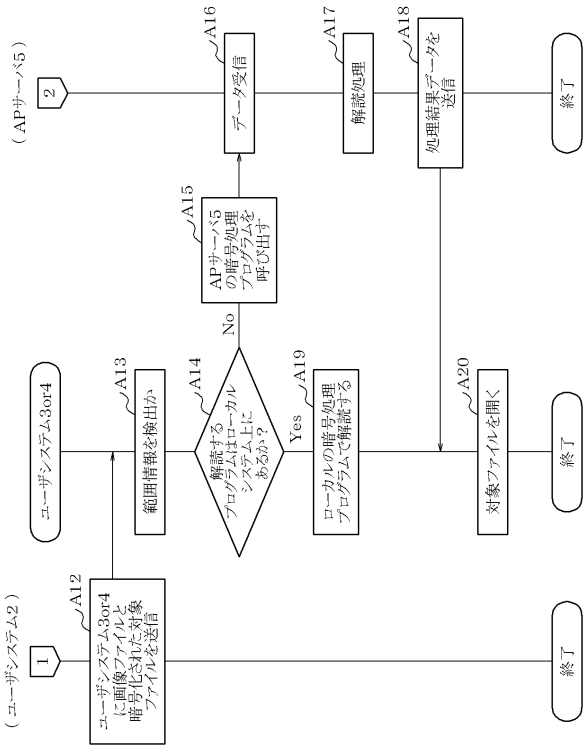
【図１０】



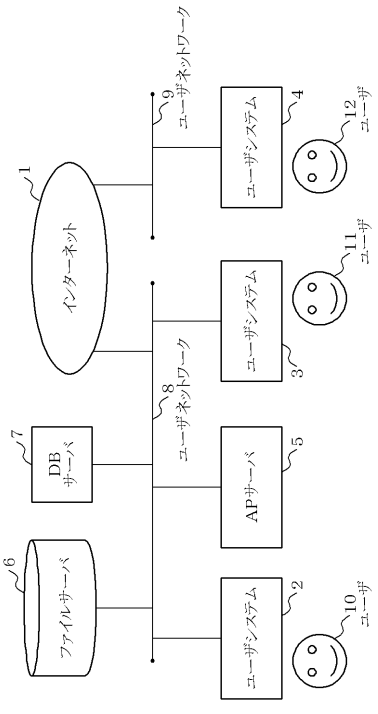
【図１１】



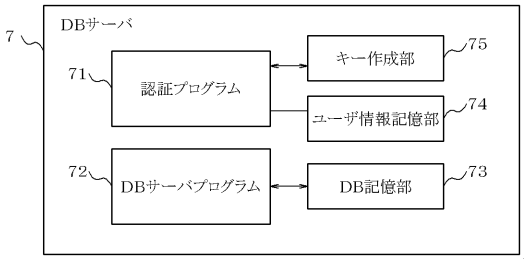
【図１２】



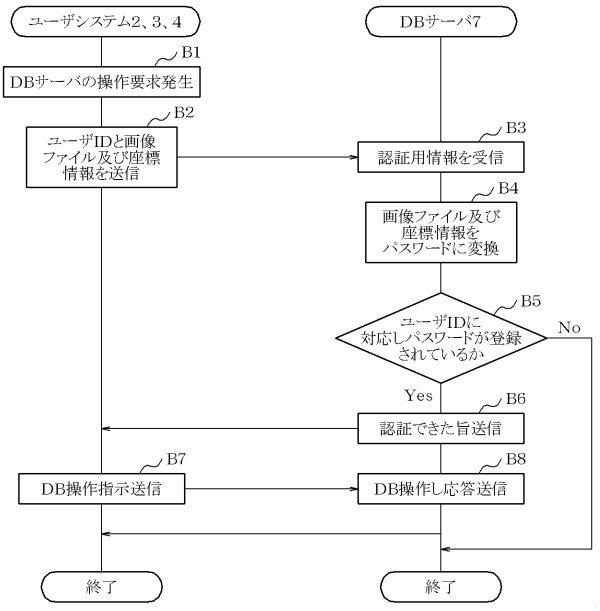
【図１３】



【図１４】


DBサーバ
7
71
認証プログラム
キー作成部
75
ユーザ情報記憶部
74
72
DBサーバプログラム
DB記憶部
73

【図１５】


ユーザシステム2、3、4
DBサーバ7
B1
DBサーバの操作要求発生
B2
ユーザIDと画像ファイル及び座標情報を送信
B3
認証用情報を受信
B4
画像ファイル及び座標情報をパスワードに変換
B5
ユーザIDに対応しパスワードが登録されているか
No
Yes
B6
認証できた旨送信
B7
DB操作指示送信
B8
DB操作し応答送信
終了
終了

フロントページの続き

(56)参考文献 特開平０９－２８４７４３（ＪＰ，Ａ）
特開平１１－０８８３２４（ＪＰ，Ａ）
特開２００５－０２６９７０（ＪＰ，Ａ）
特開２００１－２６８０６７（ＪＰ，Ａ）
国際公開第２００４／０９０８０４（WO，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／０８