指紋を鍵とするファイル暗号化システムの開発

― あなたの指紋が鍵になる ＋ 指紋データは残しません ―

１．背景

近年、個人情報や機密情報などの重要な情報が、PC 本体や USB メモリのようなストレージの盗難、紛失や、ウィルスによってネットワーク上に流出するなど、管理上のミスにより漏洩してしまうという事件が頻繁に起こっている。対策としてファイルを暗号化していれば、ファイルを盗まれた際に中身を見られてしまう危険性はほとんど無くなるが、その際、暗号鍵をどのように管理するかがセキュリティ上重要な問題となる。

２．目的

ここで、本人と直結した生体情報である指紋を暗号化、復号化の際の鍵として用いることが出来れば、鍵が本人と直結しているので管理の必要がなく安全かつ手軽に利用できると考える。そこで本プロジェクトでは、指紋を鍵として用いるファイル暗号化システムを開発することを目的とする（図 1）。

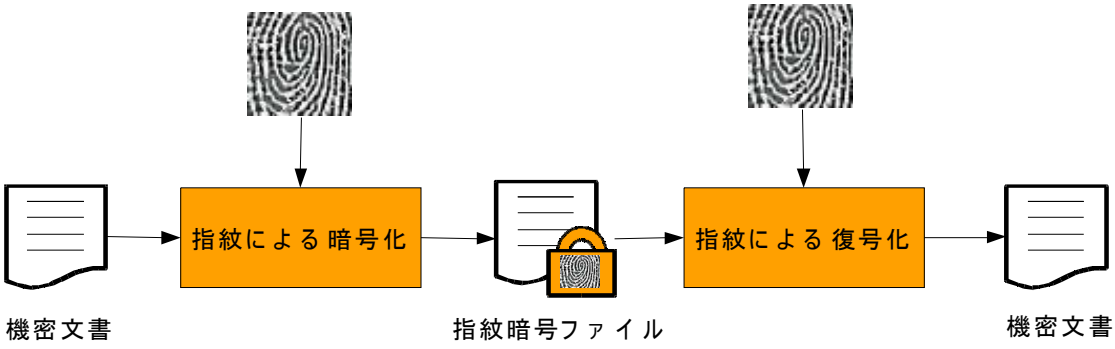

図 1 指紋暗号化による機密文書の保護

３．開発の内容

３．１．基本原理

指紋情報は、指紋センサーから取得するたびに少しずつ異なってしまうため、指紋を暗号化、復号化の鍵として用いるためには、そのばらつきに対して耐性のある手法を用いる必要がある。その手法として、バイナリデータを冗長性の高い画像に変換し、指紋画像を Double Random Phase Encoding と呼ばれる光学的な暗号化アルゴリズムの鍵として用いることにより、バイナリデータの暗号化、復号化を行うという手法が提案されている。しかし、この手法では少量のバイナリデータを暗号化する場合にも暗号化データが大きくなってしまうという問題がある。具体的には、128 bit のデータを暗号化すると 64K byte の画像ファイルとなり、そのサイズは 4096 倍になる。この手法のみでファイルを暗号化しようすると、1M byte のファイルでも、4G byte という巨大なファイルになってしまう。

本プロジェクトではこの問題を解決するために、ファイルの本体は共通鍵暗号方式を用いて暗号化し、ファイル本体の暗号化に使用した共通鍵を、指紋を鍵とする光学的な暗号化アルゴリズムによって暗号化する、2 段階の手法を用いた（図 2）。この手法により、ファイルのヘッダとして数百 K byte のデータを付加するだけで、指紋によるファイル暗号化を実現することが可能となった。

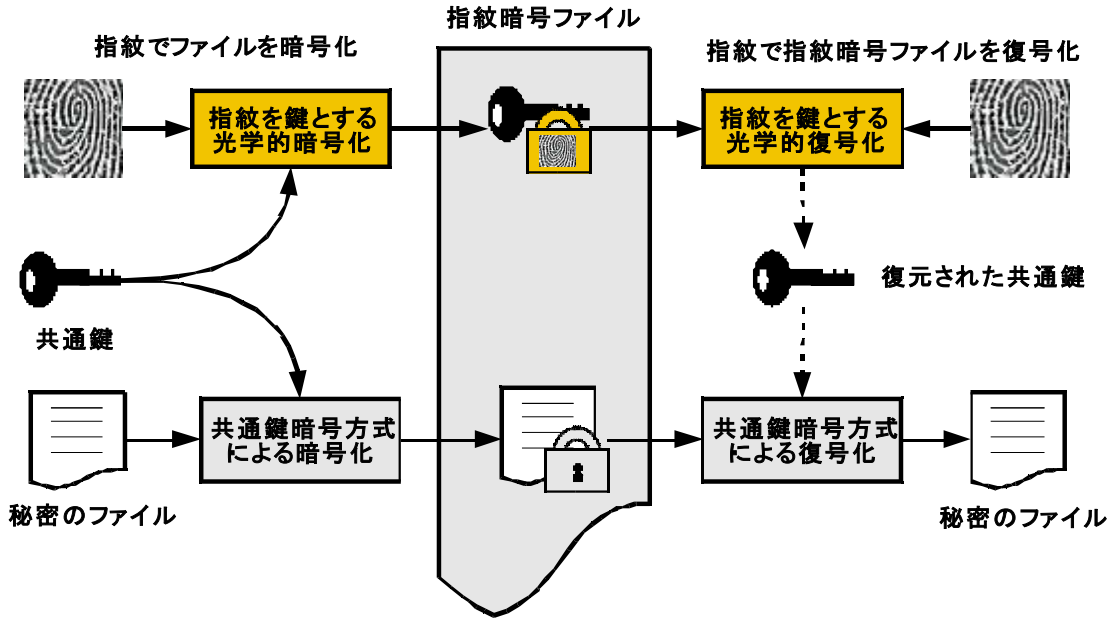

図 2 指紋を鍵とするファイル暗号化手法

３．２．実装

本プロジェクトでは、指紋センサーとして Digital Persona 社の「U.are.U」（図 3）を用い、Windows 上のアプリケーションとして実装した。また、共通鍵暗号方式としては .NET Framework で提供されている AES を利用した。GUI としては、図 4 に示すような暗号化ダイアログ、復号化ダイアログを作成した。

図 3 指紋センサー「U.are.U」
（Digital Persona 社）

アプリケーションを起動する際に、アイコンへファイルやフォルダをドラッグアンドドロップすることで暗号化ダイアログが表示される。復号化の際には、指紋で暗号化されたファイル（指紋暗号ファイル）とアプリケーションを関連付けることにより、指紋暗号ファイルのダブルクリックで復号化ダイアログが表示される。このように、圧縮解凍ソフトのような使い方で、指紋による暗号化、復号化が行えるように実装した。

図 4 左：暗号化ダイアログ、右：復号化ダイアログ

３．３．復号化精度向上のための工夫

指紋を鍵とする暗号化アルゴリズムでは、暗号化時に取得した指紋データと、復号化時に取得した指紋データの差異によってノイズが含まれる。そのため、本人の指紋で復号化した際に、復号化精度を向上させ、失敗する確率を下げるために以下のような工夫を行った。

- 共通鍵を画像に変換し、指紋で暗号化する際に誤り訂正符号を使用した。
- 位置ずれの大きな指紋画像は復号化に失敗する可能性が高いため、取得した指紋の位置ずれを検出して、位置ずれの大きさを確認できるようにした。
- 暗号化の際には、同じ指紋画像を 4 枚用いた平均画像をあらかじめ取得しておいて、その画像を用いて暗号化できるようにした。
- 複数の指紋で暗号化し、どれか 1 つの指で復号化できるようにした。

４．従来の技術（または機能）との相違

従来の指紋を用いたファイル保護システムでは、認証によって秘密情報へのアクセス権を与えるというものであった。そのため、システムはユーザーの指紋情報を安全に管理する必要があった。

本プロジェクトで開発した指紋を鍵とするファイル暗号化システムでは、復号化に必要な情報がファイル本体と本人の指以外には存在する必要がないという特徴がある。従来の指紋を用いたファイル保護システムでは、ある PC から別の PC へ保護されたデータを移動する場合には安全性を保つことが困難であったが、本システムでは認証情報をローカルに残す必要がないため、指紋を用いることの利便性を保ちつつ、暗号化したデータを別の PC へ移動する際にも安全性を確保することが可能となった。

５．期待される効果

個人情報のような外部に漏洩することが許されないデータを扱う業務で、そのデータを持ち運ぶ必要がある場合に、指紋による暗号化を行うことで、鍵管理の煩わしさなしに情報漏洩を防ぐことが可能となる。また、ネットワーク上のストレージに暗号化したデータを保存する場合にも、安全かつ手軽に、どこからでもアクセスできるようにすることが可能となる。

６．普及（または活用）の見通し

本システムを使用するためには指紋センサーが必要で、利用者に購入してもらう必要があるため、システム全体として商品化したいと考えている。

７．開発者名（所属）

田島 英朗（東京工業大学大学院 総合理工学研究科）