2007年1月23日
株式会社 日立製作所

生体情報を復元できない形に変換して登録･照合を行う生体認証技術を開発

生体情報の漏えい防止機能を強化

日立製作所システム開発研究所(所長：前田 章／以下、日立)は、このたび、生体の画像情報を事前に登録した情報と照合する生体認証システムにおいて、生体情報を復元できない形に変換して保存するとともに、復元することなく照合を行うことのできる生体認証技術を開発しました。これにより、ネットワークを介した生体認証システムを構築する際、サーバや通信路からの生体情報の漏えい防止機能を今まで以上に強化することが可能となり、安心・安全な生体認証を容易に実現できるようになります。

指紋や静脈、虹彩などの生体情報は、個人の固有情報であり、パスワードのように自由に変更することができません。このため、生体認証システムにおいては、生体情報の漏えい防止が必須となっています。また、生体情報は機微(センシティブ)な個人情報(*1)にあたる場合があり、個人情報保護の観点からも厳密な管理が要求されています。

指静脈認証ATMなどでは、高い耐タンパ性(*2)を持つICカードのチップ内で生体情報を保管・照合する方式をとることにより、生体情報の漏えいに対して高い安全性を確保しています。

一方、ICカードを利用せずに、Webシステムのログイン時など、ネットワークを介して本人確認を行う生体認証システムでは、一般に利用者の登録生体情報の集中管理、照合処理をサーバ側で行います。このようなサーバ認証型の生体認証システムでは、これまで通信やデータベースの暗号化、管理者の認証によるアクセス制限などによって、生体情報の漏えいリスクを低減し、安全性を確保してきました。しかし、より高い安全性を確保するため、近年、サーバに対しても生体情報を秘匿したまま認証を行う技術が必要であるとの認識が高まっています。

このような背景から、日立では、生体情報を秘密のパラメータを用いて変換し、元の生体情報を秘匿したままの状態で登録､照合が可能な生体認証技術の研究開発を進めてきました｡そして、今回、画像同士の比較(画像マッチング)に基づく生体認証方式に広く適用可能な技術を開発しました。

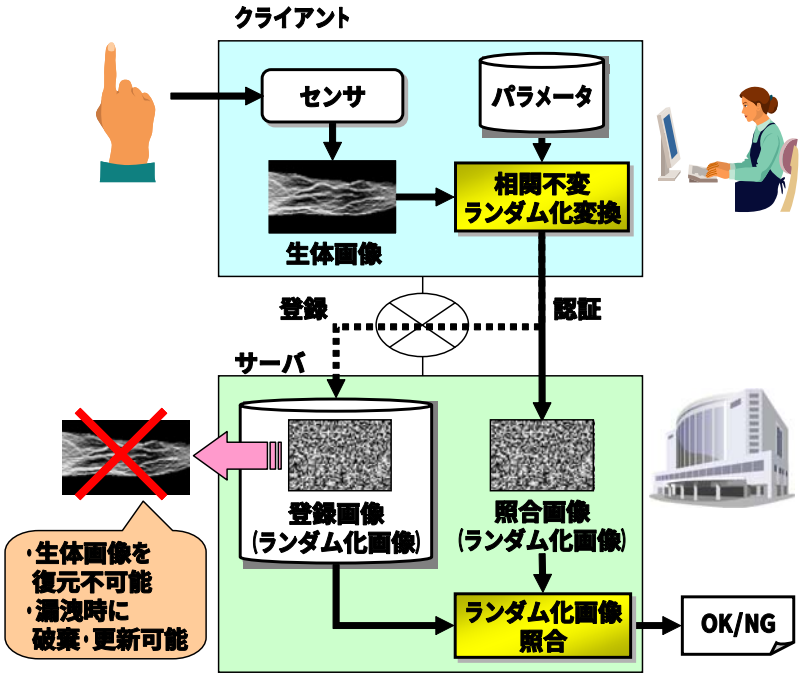
本技術を適用した、サーバ認証型の生体認証システムにおける利用者の登録、照合の流れは以下の通りです。

まず、利用者の登録時に、クライアント側でユーザの生体画像を取得、ネットワークを介してサーバに送信し、保管します。この時、サーバには生体画像を直接送信せず、ランダムに生成したパラメータ(暗号鍵に相当)を用いて変換(暗号化に相当)し、ランダム化画像(暗号文に相当)に

して送付します。サーバはこれを登録画像として保管します。また、クライアント側ではパラメータを保管し、サーバに対して秘密にしておきます。

認証時には、クライアント側で再度ユーザの生体画像を取得、保管してあるパラメータを用いて変換し、得られたランダム化画像を照合画像としてサーバに送信します。サーバは照合画像と登録画像を照合し、一致（OK)、不一致（NG）を判定します。

本技術は、指静脈認証をはじめ各種の生体認証方式に適用可能で、安心・安全なサーバ認証型の生体認証システムを容易に実現できるようになります。



サーバ認証型生体認証システムへの適用図

今回開発した技術の特長は、以下の通りです。

(1)生体画像をランダム化した状態で照合

生体情報の漏えいリスクを回避するために、生体画像を暗号化して保管する手法が考えられます。しかし、従来は、照合時に一旦復号化し、元の生体画像に戻してから照合する必要がありました。

これに対し、今回開発した技術では、数論変換(*3)とよばれる数学的な変換に基づいて、画像の変換方式(相関不変ランダム化変換)および照合方式(ランダム化画像照合)を構成することにより、元の生体画像をランダム化したままで、照合処理を行うことが可能です。ランダム化画像は一様乱数と区別がつかず、パラメータを知らずに元の生体画像を復元することはできません。このため、プライバシーとセキュリティの高いサーバ認証型生体認証システムを、今まで以上に容易に実現することができます。

(2)漏洩したランダム化画像などを破棄・更新可能

万一、ランダム化画像やパラメータが漏えいした場合も、新たにパラメータを生成してランダム化画像を作成し、登録画像とパラメータを更新することにより、漏えい情報を無効化してセキュリティを維持することができます。

なお、本内容に関して、2007 年 1 月 23 日から 26 日まで長崎県佐世保市で開催される「暗号と情報セキュリティシンポジウム（SCIS2007）」において発表する予定です。

(*1) 機微（センシティブ）な個人情報：
個人情報のなかでも特に取扱に留意すべき情報。思想、人種、保険医療情報などが該当する。金融庁より告示されている「金融分野における個人情報の保護に関するガイドライン」および「金融分野における個人情報保護に関するガイドラインの安全管理措置等についての実務指針」では、機微（センシティブ）情報に該当する生体認証情報の厳密な管理を要求している。

(*2) 耐タンパ性：
半導体チップなどの内部解析や改ざんを物理的および論理的に防衛する性能。

(*3) 数論変換：
有限体上で定義されるフーリエ変換。巡回畳み込みの性質を持ち、2 つのデータ系列の数論変換後の積が、データ系列同士の巡回畳み込みに対する数論変換に対応する。

■照会先
株式会社 日立製作所 システム開発研究所 企画室［担当:森］
〒215-0013 神奈川県川崎市麻生区王禅寺 1099 番地
電話 044-959-0325(ダイヤルイン)

以上