テクニカルノート

指紋照合によるリモートユーザ認証方式

若山公威[†] 出路裕介[†,☆]
冷基立[†] 岩田彰[†]

ネットワークを介した電子商取引などの情報サービスでの個人認証にバイオメトリクス情報による個人認証を行う場合，サーバで保管されているデータの盗難や管理者による不正の危険性がある．一度データが盗まれると，不正取得者は同様のアルゴリズムを利用している全サービスを利用することができてしまう．ここでは，採取機器が安く，現在最も実用化が進んでいる指紋に焦点をあて，ネットワークを介した個人認証に指紋照合を利用することを考える．そして，先ほどの問題を解決するために，指紋データをパスワードのようにサービスごとに登録情報を変えられる方式を提案する．この方式により，元の指紋データを保護した本人照合が可能となる．

A Remote User Authentication Method Using Fingerprint Matching

Kimitake Wakayama,[†] Yusuke Decchi,[†,☆] Jili Leng[†] and Akira Iwata[†]

When performing a user authentication to information service over the network using biometrics information, there is a risk of the theft by intruders or the administrators. Once the data is stolen, the thief will be able to use all services that are using the same algorithm. In this paper, we focus on fingerprint. In order to solve the problem, we propose a method that can change fingerprint registration data for every service. Using this method, we can prevent the original data abuse.

1. はじめに

人が持つ指紋や眼球の虹彩，顔の輪郭などのバイオメトリクス情報は「不人不同」,「終生不変」の特徴を持っている．この 2 大特徴は個人を特定するのに大きな利点となるため，現在，バイオメトリクス情報は PC へのログインや入退出管理など，ローカルな環境下での個人認証などに利用されている．パスワードでの認証方法においてはパスワードを忘れる場合があり，IC カードなどの所有物によりユーザを認証する場合はその所有物を紛失することがある．これらの点においては，バイオメトリクスは有効な認証方式ということができる．

しかし，ネットワーク上でバイオメトリクス情報による個人認証を利用しているサービスやアプリケーションは少ない．それは，バイオメトリクス情報の 2 大特徴の 1 つである「終生不変」が，つねに盗聴や改竄などの脅威にさらされるオープンな環境においては非常に大きな問題となるからである．バイオメトリクス情報は決して盗まれてはいけない個人情報であるため，高いセキュリティを備えた環境でなければこれらを利用するのが難しい．

ここでは，採取機器が安く，現在最も実用化が進んでいる指紋に焦点をあて，指紋をネットワークを介した電子商取引などの情報サービスでの個人認証に利用することを考える．そして，先ほどの問題を解決するために，新しい指紋照合方式を検討する．この方式では，終生不変である指紋をパスワードのように，サービスごとに登録情報を変えられるようにする．この方式により，元の指紋データを保護した本人照合が可能となる．

2. ネットワークを介した指紋照合の問題点

ネットワークを介した指紋による個人認証方式を実

† 名古屋工業大学
Nagoya Institute of Technology
☆ 現在，新日鉄ソリューションズ株式会社
Presently with NS Solutions Corporation

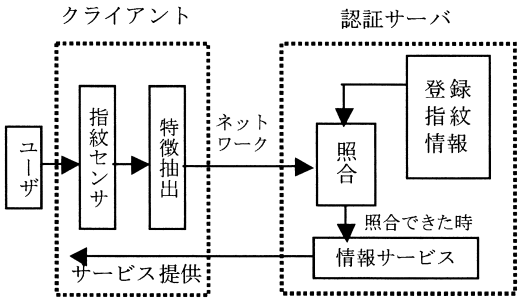


図 1 ネットワーク上での指紋照合のモデル
Fig. 1 Fingerprint verification model on a network.

装する場合，**図 1** のような構成が考えられる[1]．あらかじめサーバ側に指紋情報を登録しておき，照合時にクライアントから指紋情報をサーバへ送信して，サーバ側で照合を行う方式である．このシステムの問題点として以下のことが考えられる．

- 送信する指紋データの盗聴，改竄
- サーバにある登録指紋情報の漏洩，改竄

ネットワーク上での情報の盗聴などは，SSL（Secure Sockets Layer）などを用いて通信メッセージを暗号化すれば防ぐことができる．しかし，サーバにある登録指紋情報の漏洩は完全には防ぐことができない．画像マッチングの場合は指紋イメージが保管されるためなおさらであるが，特徴量を用いる照合の場合も利用アルゴリズムにおいて終生不変である指紋の特徴が明らかとなってしまうため，サーバでの保管は避けたい．

3. 提案方式

前章で述べた問題点を解決するために，**図 2** のように元の指紋データから元の指紋を推測されないような新しい指紋データを作成し，これをサーバ側に登録して照合に利用することを考える．

今回は，元となる照合方式として浅井ら[2),3)]の方法を用いた．この方式は，指紋画像の中からマニューシャと呼ばれる特徴点（端点，分岐点）を検索し，その各特徴点の特徴量と互いの位置関係を求め，そのデータのマッチングによって照合を行う方式である．特徴量は各特徴点の座標と特徴方向，2 つの特徴点間を横切る指紋線の横切る数（リレーション）からなる（**図 3**）．

提案するデータ作成方式の流れは，以下のとおりである．

(1) 指紋画像から特徴点群 A を抽出し，特徴点の座標と特徴方向を求める．
(2) 特徴点群 A の座標を回転や移動することにより変化をさせ，特徴点群 A' を作成する．
(3) A' のリレーションを求めて登録指紋データとし，これを個人照合に用いる．

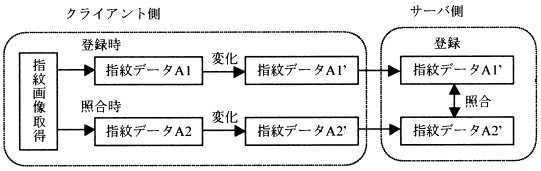


図 2 登録と照合の流れ
Fig. 2 Flow of registration and verification.

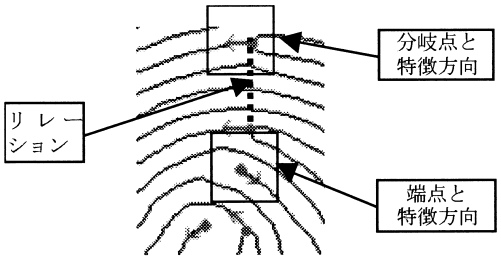


図 3 マニューシャネットワーク特徴
Fig. 3 Minutia-network feature.

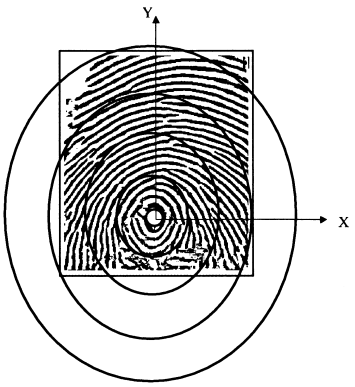


図 4 指紋画像を 4 領域に分割した例
Fig. 4 Example of dividing fingerprint image into four domains.

浅井らの指紋データ作成方式は，指紋画像に対して (1) の処理を施して (3) の処理を行っている．提案方式では新たに (2) の処理を追加する．

次に特徴点群 A' の作成方法について説明する．まず，中核点（指紋の中心点）を中心として，**図 4** のように指紋画像を距離によって 4 つの領域に分割する．領域分割を楕円にしたのは，中核点のずれが X 軸よりも Y 軸の方が大きいためである．この各領域に対してそれぞれ 0 から 9 いずれかの数字を割り当てて，(1) の処理で求めた特徴点群 A の座標と特徴方向を各領域の数字に対応して移動と回転をさせる．変化方法は次のとおりである．

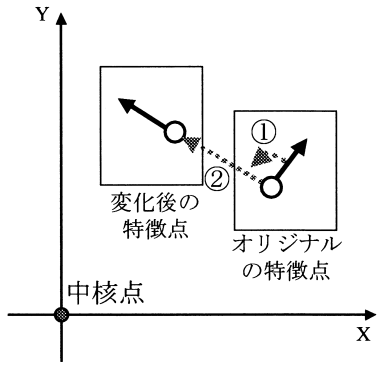


図 5 特徴点の変化
Fig. 5 Alteration of minutiae.

(1) 中核点を中心として，数字に対応して特徴点の特徴方向を回転させる．領域に割り当てられた数字を n，変更前の角度を v，変更後の角度を v' とすると，次の式で表される．

$$v' = v - (n - \alpha) \times \beta \quad (1)$$

(2) 回転させた特徴方向の向きに，特徴点の座標を距離 d 移動させる．

$$d = (abs(n - \alpha) + \gamma) \times \delta \quad (2)$$

一例を**図 5** に示す．この変化の結果，特徴点が指紋画像領域からはみ出ることがある．この場合，その特徴点と最近特徴点との隆線交差数を求めることができないため，特徴点を削除する．変化させた特徴量をサーバへ送信して登録を行う．

移動と回転に用いた 4 つの数字（それぞれ 0 から 9）は，クライアント側でのみ保管しておく．ユーザが記憶しておいてもよいし，クライアント機器でユーザ ID に対応して保管しておいてもよい．

照合時には，クライアント側で登録時と同じ数字を用いて，読み込んだ指紋イメージから最終の特徴量を計算しサーバへ送信する．サーバでは，受信した特徴量と登録してある特徴量の照合を行う．

4. 実験結果と評価

従来方式（浅井らの方式）と提案方法を実装し，比較実験を行った．登録指紋として，研究室の学生 15 人の左右の親指計 30 指を収集した．照合は，同一の 15 人の 30 指についてそれぞれ 10 回ずつ，合計 300 回行った．通常の電子商取引ではユーザ ID を指定しての照合が行われるが，ここでは方式の精度を確認するため 1 対 N の識別により行った．提案方式の場合，1 人ごとに 4 つの数字が必要となる．この数字は，登録時にランダムな値を与えて，照合時にも同様の値を用いた．式 (1)，式 (2) において，$\alpha = 5$，$\beta = 7$，$\gamma = 5$，$\delta = 3$ とした．実験結果を**表 1** に示す．

表 1 従来方式と提案方式の照合率
Table 1 Verification rate comparison between existing and proposed method.

	従来方式	提案方式
照合率（%）	93.3	73.0
他人受け入れ率（%）	1.7	0.0

提案方式では照合率が大きく落ちたものの，実現の可能性は示せたと考えられる．他人受け入れ率は向上している．これは，変形を加えたことにより，他人の指紋との違いが大きく分かるようになったものと考えられる．

提案方式の利点として，同じ指紋から数多くの登録データを作成することができるため，サービスが複数あり，そのサービスごとに認証サーバがある場合にそれぞれのサーバに別のデータを保存することができる．この結果，万一の盗難による被害の拡大を抑えることができる．また，元の指紋データをサーバに保存しておく必要がないため，自身のバイオメトリクス情報の保護にもなる．

一方，今回の方式の問題点としては以下のことがあげられる．

- 各領域で特徴点の座標を変化させるときに，特徴点の座標が画像の枠からはみ出てしまうことがある．このとき，リレーションを求めることができなくなるため，その特徴点は削除しなければいけない．もしその特徴点が重要な点であったとすれば，照合率に影響が出る．
- 指紋の中核点は座標の中心であり，重要な点である．しかし，同一ユーザの指紋にもかかわらず，中核点が大きくずれる場合があった．これが登録指紋であった場合，入力した指紋と座標系が大きく異なっているために照合できない恐れがある．安定して中核点を求める方式を検討する必要がある．
- マニューシャネットワーク特徴による照合を利用する利点として，ネットワークが変形に強いことがあげられる．しかし，提案方式では特徴方向を変化させるために，親特徴点と孫特徴点間の隆線交差数が正確に求められなくなってしまい，柔軟性が落ちてしまう．

5. おわりに

提案方式のように，オリジナルの指紋データをサーバに保管しなければ，指紋データの保護と万一の盗難の被害を少なくすることができる．なお，別途他の方式によりネットワーク経路上での盗聴や改竄を防ぐ必

要がある．

今回提案した指紋照合方式と従来方式での本人認証率を比較すると，まだ実用化できるとはいえない．今後提案方式を改良することで，他人受け入れ率を下げた状態で本人照合率を上げる必要がある．

今後，インターネット上での個人認証はさらに重要な問題となるだろう．その際，バイオメトリクス情報による個人認証が有効なものとして期待できるものの，データの盗難などの危険がともなう．今回は指紋についてのみ解決方法を検討したが，様々なバイオメトリクス情報による本人照合をインターネット上で安全に利用することができれば，非対面での商取引などのサービスを享受できるようになると考えられる．

謝辞 本研究は，名古屋工業大学研究活性化経費の補助による．

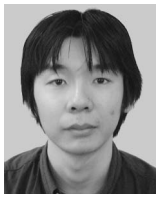
参 考 文 献

1) 内田 薫：指紋照合による本人認証，情報処理学会誌，Vol.40, No.11, pp.1078–1083 (1999).
2) 浅井 紘，星野幸夫，木地和夫：マニューシャネットワーク特徴による自動指紋照合—特徴抽出過程，電子情報通信学会論文誌，Vol.J72-D-II, No.5, pp.724–732 (1989).
3) 浅井 紘，星野幸夫，木地和夫：マニューシャネットワーク特徴による自動指紋照合—照合過程，電子情報通信学会論文誌，Vol.J72-D-II, No.5, pp.733–740 (1989).

(平成 14 年 9 月 17 日受付)
(平成 14 年 12 月 3 日採録)

若山 公威（正会員）

平成 5 年名古屋工業大学電気情報工学科卒業．平成 7 年同大学大学院博士前期課程修了．同年沖電気工業株式会社入社．平成 10 年より名古屋工業大学電気情報工学科助手．情報セキュリティに関する研究に従事．電子情報通信学会会員．



出路 裕介

平成 14 年名古屋工業大学電気情報工学科卒業．同年新日鉄ソリューションズ株式会社入社．在学中，情報セキュリティに関する研究に従事．

冷 基立

平成 7 年中国遼寧大学計算機学科卒業．同年中国国家税務局大連市分局入局．平成 11 年名古屋愛知淑徳大学留学生別科入学．平成 12 年名古屋工業大学電気情報工学科研究生．平成 13 年名古屋工業大学大学院博士前期課程入学．情報セキュリティに関する研究に従事．

岩田 彰（正会員）

昭和 48 年名古屋大学工学部電気学科卒業．昭和 50 年同大学大学院修士課程修了．同年名古屋工業大学工学部助手．昭和 57 年 4 月より昭和 58 年 10 月までドイツ連邦共和国ギーセン大学医用情報研究所客員研究員．昭和 59 年名古屋工業大学工学部情報工学科助教授．平成 5 年名古屋工業大学工学部電気情報工学科教授．平成 14 年 10 月より名古屋工業大学副学長．現在に至る．ニューラルネットワーク，生体情報処理，医療情報システム，情報セキュリティ，インターネットコンテンツ開発技術に関する研究．昭和 55 年日本 ME 学会研究奨励賞受賞．平成 4 年郵政省郵政研究所主催文字認識コンテスト奨励賞受賞．平成 5 年電子情報通信学会論文賞受賞．平成 10 年情報処理学会「Best Author 賞」受賞．工学博士．電子情報通信学会，日本 ME 学会，日本心電図学会，日本神経回路学会，日本医療情報学会各会員．IEEE Senior Member．